



T.C.

ALTINBAŞ ÜNİVERSİTESİ

Lisansüstü Eğitim Enstitüsü

İşletme Ana Bilim Dalı / İşletme Programı

**BLOKZİNCİR TEKNOLOJİSİNİN FİNANSAL  
BİLGİ MANİPÜLASYONUNU (MUHASEBE  
HİLELERİNİ) AZALTMADA KULLANILMASI:  
İSTANBUL'DAKİ MALİ MÜŞAVİRLER ÜZERİNE  
AMPİRİK ARAŞTIRMA**

**Selmin ÇELİK**

Doktora Tezi

Danışman

Prof. Dr. Saim KILIÇ

İstanbul, 2024

**BLOKZİNCİR TEKNOLOJİSİNİN FİNANSAL BİLGİ  
MANİPÜLASYONUNU (MUHASEBE HİLELERİNİ)  
AZALTmada KULLANILMASI: İSTANBUL'DAKİ MALİ  
MÜŞAVİRLER ÜZERİNE AMPİRİK ARAŞTIRMA**

**Selmin ÇELİK**

İşletme

Doktora Tezi

ALTINBAŞ ÜNİVERSİTESİ

2024

“Selmin ÇELİK” tarafından hazırlanmış ve 24.12.2024 tarihinde sunulmuş “BLOKZİNCİR TEKNOLOJİSİNİN FİNANSAL BİLGİ MANİPÜLASYONUNU (MUHASEBE HİLELERİNİ) AZALTmada KULLANILMASI: İSTANBUL’DAKİ MALİ MÜŞAVİRLER ÜZERİNE AMPİRİK ARAŞTIRMA” başlıklı tez İşletme Anabilim Dalında Doktora Tezi olarak **oy birliği** ile kabul edilmiştir.

---

Prof. Dr. Saim KILIÇ

Danışman

Tez Savunma Sınavı Jüri Üyeleri:

|                                               |                                                                         |       |
|-----------------------------------------------|-------------------------------------------------------------------------|-------|
| Prof. Dr. Saim KILIÇ                          | İşletme Bölümü,<br>Altınbaş Üniversitesi                                | _____ |
| Prof. Dr. Ahmet Ercan GEGEZ                   | Uluslararası Ticaret ve<br>İşletmecilik Bölümü,<br>Topkapı Üniversitesi | _____ |
| Prof. Dr. Emre ALKİN                          | Ekonomi Bölümü,<br>Topkapı Üniversitesi                                 | _____ |
| Prof. Dr. Cemal İBİŞ                          | Pazarlama Bölümü,<br>Altınbaş Üniversitesi                              | _____ |
| Dr. Öğr. Üyesi Ayşegül<br>BAYRAKTAROĞLU GÜNER | Pazarlama Bölümü,<br>Altınbaş Üniversitesi                              | _____ |

Bu tezin Doktora tezi olarak bütün şartları sağladığını beyan ederim.

Bu tezdeki tüm bilgilerin akademik kurallara ve etik davranışlara uygun olarak edinildiğini ve sunulduğunu beyan ederim. Ayrıca bu kuralların ve davranışların gerektirdiği şekilde, bu çalışmada, orijinal olmayan tüm materyalleri ve sonuçları tamamen alıntı yaptığımı ve referans gösterdiğimi de beyan ederim.

Selmin ÇELİK



## İTHAF

Bu maceraya atılma sebebim ve ilhamım, babam Prof. Dr. Tuncer ÇELİK'e...

&

Bu macerayı güzelleştiren en değerli varlığım, oğlum Selim'e...



## ÖNSÖZ

“Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu (Muhasebe Hilelerini) Azaltmada Kullanılması : İstanbul’daki Mali Müşavirler Üzerine Ampirik Araştırma” konusunu ele aldığım doktora tez çalışmamın bilimsel temeller üzerine inşa edilmesine katkı sağlayan ve bu süreçte her ihtiyaç duyduğumda sabır ve anlayışla bana rehberlik eden çok kıymetli tez danışmanım Prof. Dr. Saim KILIÇ’a, değerli görüşleriyle bana yol gösteren Tez İzleme Komite üyesi hocalarım Prof. Dr. Ahmet Ercan GEGEZ’e ve Prof. Dr. Emre ALKİN’e, tez savunma jürimde yer alan hocalarım Dr. Öğr. Üyesi Ayşegül BAYRAKTAROĞLU GÜNER ile aynı zamanda TÜRMOB Genel Saymanı olan ve veri toplama sürecinde desteklerini esirgemeyen Prof. Dr. Cemal İBİŞ’e, araştırmanın veri toplama sürecine sağladıkları katkı ve desteklerinden ötürü İYMMO Başkanlığı’na ve İSMMMO Başkanı Erol DEMİREL’e ve doktora başlamama vesile olan hocam Prof. Dr. Mümin ERTÜRK’e saygı ve teşekkürlerimi sunarım.

Ayrıca bu süreçte, akademik tecrübesiyle bana alan dışı katkı sağlayan eniştem Prof. Dr. Sacit KARAMÜRSEL’e, yaşadığım her zorlukta manevi destekleriyle bana güç veren ve hayatımı kolaylaştıran sevgili ablalarım Yeşim KARAMÜRSEL’e ve Dr. Nilay ÇELİK MUHTAROĞLU’na, elinden geldiği kadar destek olan eşim Cansın GÜRDAL’a, bu sürecin tüm zorluklarını benimle yaşarken büyümüş olan ve çalışmalarım sebebiyle kendisini bir miktar ihmal etmeme sabır ve özveri gösteren can parçam oğlum Selim’e, fedakarlıklarını ve emeklerini asla karşılayamayacağım, bugün sahip olduğum benliğe ve elde ettiğim bu başarıya ulaşmamdaki en büyük payın sahipleri, her daim arkamdaki kuvvet olan biricik annem Selma ÇELİK’e ve babam Prof. Dr. Tuncer ÇELİK’e ve destek olan tüm aile bireylerime ve arkadaşlarıma hep yanımda oldukları için sonsuz teşekkürlerimi ve minnetlerimi sunar, çalışmanın tüm ilgililere yararlı olmasını dilerim.

## ÖZET

# **BLOKZİNCİR TEKNOLOJİSİNİN FİNANSAL BİLGİ MANİPÜLASYONUNU (MUHASEBE HİLELERİNİ) AZALTMADA KULLANILMASI: İSTANBUL'DAKİ MALİ MÜŞAVİRLER ÜZERİNE AMPİRİK ARAŞTIRMA**

ÇELİK, Selmin

Doktora, İşletme, Altınbaş Üniversitesi

Danışman: Prof. Dr. Saim KILIÇ

Tarih: 12/2024

Sayfa: 386

Muhasebe verilerinin kişisel çıkarlar doğrultusunda hileli kullanımı, işletmeye ve kaynakların verimsiz sarfedilmesi sebebiyle ülke ekonomisine büyük zararlar vermektedir. Finansal bilgi manipülasyonları ile mücadele etmeye yönelik ise çeşitli denetim mekanizmaları ile birlikte hile ihbar hatları, fısıltı yöntemi gibi geleneksel araçlar kullanılmaktadır. Ancak bu yöntemler, manipülasyonlar gerçekleştikten yani zarar meydana geldikten sonra tespit edilmesini sağladıklarından etkin bir mücadele yöntemi sunmamaktadırlar. Bu nedenle manipülasyonları önlemek ve yarattığı maliyetleri azaltabilmek amacıyla proaktif yöntemlere ihtiyaç duyulmaktadır. Bu kapsamda çalışmada, hile yapılmasını önlemeye yönelik alternatif bir proaktif yöntem olarak Endüstri 4.0 bileşenlerinden biri olan blokzincir teknolojisi önerilmekte ve ilgili teknolojinin, finansal bilgi manipülasyonlarının azaltılmasına yönelik uygulanabilirliğine ilişkin teorik bir çerçeve sunulmaktadır. Ayrıca çalışma ile İstanbul'da faaliyette bulunan mali müşavirlerin blokzincir teknolojisini benimseme düzeyleri, Teknoloji Kabul Modeli (TKM) ile ölçülmekte ve hile araştırmaları kapsamında, katılımcıların finansal bilgi manipülasyonu

karşılaşma sıklıkları ve blokzincir teknolojisinin finansal bilgi manipölasyonlarını önlemedeki rolüne ilişkin görüşleri ortaya konulmaktadır.

Araştırma verileri, İstanbul SMMM ve YMM Odalarına kayıtlı toplam 408 mali müşavir meslek mensubundan elde edilmiştir. Teknoloji Kabul Modeli ölçek verileri, doğrulayıcı faktör analizi, korelasyon analizi ve çoklu regresyon analizi ile test edilmiştir. Katılımcıların demografik ve mesleki özelliklerine göre farklılıkları; TKM boyutları açısından t testi ile, hile araştırmaları ölçek verileri açısından ise Mann-Whitney U ve Kruskal-Wallis testleri kullanılarak analiz edilmiştir.

Yapılan TKM analizi sonucunda; Teknoloji Kabul Modeli altı boyutlu olarak doğrulanmış ancak model değişkenlerinin, blokzincir teknolojisi kabul davranışı üzerindeki etkileri açığa çıkmamıştır. Ayrıca demografik ve mesleki özelliklere göre TKM boyutları arasında da farklılık tespit edilmemiştir. Hile araştırmaları analizi sonucunda, katılımcıların hile belirtileri ile karşılaşma sıklıklarının cinsiyetlerine, eğitim düzeylerine ve mesleki ünvanlarına göre; blokzincir teknolojisinin muhasebe hilelerini önlemedeki rolünün ise katılımcıların eğitim düzeyine göre farklılık gösterdiği tespit edilmiştir. Bu sonuçlara göre; İstanbul'daki mali müşavirlerin blokzincir teknolojisini benimseme düzeylerinde, teknolojiye dair bilgi seviyeleri belirleyici bir faktör olarak öne çıkmaktadır. Ancak bu profesyonellerin çoğu, blokzincir teknolojisi hakkında oldukça düşük bir bilgi seviyesine sahip bulunmaktadır. Blokzincir teknolojisinin finansal bilgi manipölasyonlarını önlemedeki rolüne ilişkin mali müşavirlerin olumlu görüşleri ise teknoloji hakkındaki bilgi düzeyi arttıkça etkili olmaktadır.

**Anahtar Kelimeler:** Finansal Bilgi Manipölasyonu, Muhasebe Hileleri, Blokzincir Teknolojisi, Teknoloji Kabul Modeli, Hile Araştırmaları.



## **ABSTRACT**

# **USE OF BLOKCHAIN TECHNOLOGY TO REDUCE FINANCIAL INFORMATION MANIPULATION (ACCOUNTING FRAUD): AN EMPIRICAL RESEARH ON ACCOUNTANT IN ISTANBUL**

ÇELİK, Selmin

PhD, Business Administration, Altınbaş University,

Supervisor: Prof. Dr. Saim KILIÇ

Date: 12/2024

Pages: 386

Fraudulent use of accounting data for personal gain causes great damage to the business and the national economy due to inefficient use of resources. In order to combat financial information manipulation, various audit mechanisms and traditional tools such as fraud hotline and whistleblowing are used. However, these methods do not provide an effective method of combating manipulations since they are detected after the manipulations have occurred, i.e. after the loss has occurred. Therefore, proactive methods are needed to prevent manipulations and reduce their costs. In this context, this study proposes blockchain technology, one of the components of Industry 4.0, as an alternative proactive method to prevent fraud and presents a theoretical framework for the applicability of this technology to reduce financial information manipulations. In addition, the study measures the level of adoption of blockchain technology by Certified Public Accountants (CPA) operating in Istanbul with the Technology Acceptance Model (TAM) and reveals the frequency of financial information manipulation and the views of the participants on the role of blockchain technology in preventing financial information manipulation within the scope of fraud research.

The research data were obtained from a total of 408 CPA professionals registered in Istanbul CPA Chambers. Technology Acceptance Model scale data were tested with confirmatory factor analysis, correlation analysis and multiple regression analysis. Differences in TAM dimensions according to the demographic characteristics of the participants were analyzed using the t-test, and fraud research scale data were analyzed using Mann-Whitney U and Kruskal-Wallis tests.

As a result of the TAM analysis, the Technology Acceptance Model was confirmed as six dimensions, but the effects of the model variables on blockchain technology acceptance behavior were not revealed. In addition, there was no difference between TAM dimensions according to demographic and occupational characteristics. As a result of the fraud research analysis, it was found that the frequency of the participants' encountering fraud symptoms differed according to their gender, educational level and occupational title, while the role of blockchain technology in preventing accounting fraud differed according to the educational level of the participants. According to these results, the level of knowledge about the technology stands out as a determining factor in the level of adoption of blockchain technology by CPAs in Istanbul. However, most of these professionals have a very low level of knowledge about blockchain technology. The positive views of financial advisors on the role of blockchain technology in preventing financial information manipulations become more effective as the level of knowledge about the technology increases.

**Keywords:** Financial Information Manipulation, Accounting Fraud, Blockchain Technology, Technology Acceptance Model, Fraud Investigations.

# İÇİNDEKİLER

## Sayfa

|                                                                                          |              |
|------------------------------------------------------------------------------------------|--------------|
| <b>ÖZET .....</b>                                                                        | <b>vii</b>   |
| <b>ABSTRACT .....</b>                                                                    | <b>ix</b>    |
| <b>TABLO LİSTESİ.....</b>                                                                | <b>xviii</b> |
| <b>ŞEKİL LİSTESİ .....</b>                                                               | <b>xxii</b>  |
| <b>KISALTMALAR.....</b>                                                                  | <b>xxiv</b>  |
| <b>SEMBOL LİSTESİ .....</b>                                                              | <b>xxxi</b>  |
| <b>1. GİRİŞ.....</b>                                                                     | <b>1</b>     |
| <b>2. BLOK ZİNCİR TEKNOLOJİSİ .....</b>                                                  | <b>5</b>     |
| 2.1 BLOKZİNCİR TEKNOLOJİSİNİN TANIMI .....                                               | 5            |
| 2.2 BLOKZİNCİR TEKNOLOJİSİNİN TARİHSEL SÜRECİ .....                                      | 7            |
| 2.2.1 Blokzincir Teknolojisinin Ortaya Çıkışı .....                                      | 7            |
| 2.2.2 Blokzincir Teknolojisinin Gelişimi.....                                            | 15           |
| 2.2.2.1 Blokzincir 1.0.....                                                              | 16           |
| 2.2.2.2 Blokzincir 2.0.....                                                              | 18           |
| 2.2.2.3 Blokzincir 3.0.....                                                              | 20           |
| 2.3 BLOKZİNCİR TEKNOLOJİSİNİN TEKNİK KAVRAMLARI.....                                     | 22           |
| 2.3.1 Blok.....                                                                          | 22           |
| 2.3.1.1 Merkle ağaçları (Merkle trees).....                                              | 25           |
| 2.3.1.2 Zaman damgası (Time stamp).....                                                  | 26           |
| 2.3.2 Ağ Yapıları.....                                                                   | 28           |
| 2.3.2.1 Merkezi ağlar .....                                                              | 29           |
| 2.3.2.2 Dağıtık ağlar.....                                                               | 30           |
| 2.3.2.3 Merkezi ve dağıtık ağ yapılarının karşılaştırmalı avantaj ve dezavantajları..... | 30           |
| 2.3.3 Kriptoloji : Kriptografi Yöntemleri .....                                          | 31           |
| 2.3.3.1 Simetrik şifreleme .....                                                         | 34           |
| 2.3.3.2 Asimetrik şifreleme .....                                                        | 35           |

|         |                                                                               |     |
|---------|-------------------------------------------------------------------------------|-----|
| 2.3.3.3 | Hash (Özet) tekniği .....                                                     | 37  |
| 2.3.3.4 | Steganografi tekniği .....                                                    | 40  |
| 2.3.4   | Mutabakat Algoritmaları (Consensus Algorithm) .....                           | 40  |
| 2.3.4.1 | Bizans generalleri problemi .....                                             | 41  |
| 2.3.4.2 | İş kanıtı (Proof of work -POW) .....                                          | 42  |
| 2.3.4.3 | Hisse kanıtı (Proof of stake - POS).....                                      | 70  |
| 2.3.4.4 | Pratik bizans hata toleransı (Practical Byzantine fault tolerance- PBFT)...   | 71  |
| 2.3.4.5 | Mutabakat algoritmalarının karşılaştırması.....                               | 72  |
| 2.3.5   | Kripto Cüzdan (Crypto Wallet) .....                                           | 74  |
| 2.3.6   | Akıllı Sözleşmeler (Smart Contracts) .....                                    | 78  |
| 2.4     | BLOKZİNCİR TEKNOLOJİSİNİN MİMARİSİ.....                                       | 86  |
| 2.4.1   | Blokszincir Teknolojisi Katmanları .....                                      | 86  |
| 2.4.1.1 | Altyapı katmanı (Infrastructure layer) .....                                  | 87  |
| 2.4.1.2 | Veri katmanı (Data layer).....                                                | 87  |
| 2.4.1.3 | Ağ katmanı (Network layer) .....                                              | 88  |
| 2.4.1.4 | Mutabakat katmanı (Consensus layer) .....                                     | 89  |
| 2.4.1.5 | Sözleşme katmanı (Contract layer) .....                                       | 89  |
| 2.4.1.6 | Hizmet katmanı (Service layer) ve Uygulama katmanı (Application layer)        | 90  |
| 2.4.2   | Blokszincir Teknolojisinin İşleyişi.....                                      | 91  |
| 2.5     | BLOKZİNCİR TEKNOLOJİSİNİN ÖZELLİKLERİ .....                                   | 95  |
| 2.5.1   | Merkeziyetsizlik (Decentralized).....                                         | 96  |
| 2.5.2   | Şeffaflık ve İzlenebilirlik (Transparency and Traceability).....              | 97  |
| 2.5.3   | Gizlilik ve Anonimlik (Privacy and Anonymity) .....                           | 97  |
| 2.5.4   | Güvenlik ve Bütünlük (Security and Integrity) .....                           | 98  |
| 2.5.5   | Değişmezlik ve Dayanıklılık (Immutability and Tamper Resistant) .....         | 98  |
| 2.5.6   | Denetlenebilirlik ve İnkâr Edilemezlik (Auditability and Undeniability) ..... | 99  |
| 2.5.7   | Otonom Sistem (Autonomous System) .....                                       | 99  |
| 2.6     | BLOKZİNCİR TÜRLERİ .....                                                      | 100 |

|           |                                                                     |            |
|-----------|---------------------------------------------------------------------|------------|
| 2.6.1     | Genel (Public) Blokzincir .....                                     | 100        |
| 2.6.2     | Özel (Private) Blokzincir .....                                     | 101        |
| 2.6.3     | Konsorsiyum (Consortium) Blokzincir.....                            | 101        |
| 2.6.4     | Karma (Hybrid) Blokzincir.....                                      | 101        |
| 2.6.5     | Blokzincir Türlerinin Karşılaştırması .....                         | 102        |
| 2.7       | BLOKZİNCİR PLATFORMLARI.....                                        | 102        |
| 2.8       | BLOKZİNCİR TEKNOLOJİSİNİN KULLANIM ALANLARI .....                   | 105        |
| 2.9       | BLOKZİNCİR TEKNOLOJİSİNİN AVANTAJ VE DEZAVANTAJLARI .....           | 111        |
| <b>3.</b> | <b>FİNANSAL BİLGİ MANİPÜLASYONU (MUHASEBE HİLELERİ).....</b>        | <b>116</b> |
| 3.1       | FİNANSAL BİLGİ VE MANİPÜLASYONU .....                               | 116        |
| 3.1.1     | Finansal Bilgi .....                                                | 116        |
| 3.1.2     | Finansal Bilgi Manipülasyonunun Tanımı.....                         | 119        |
| 3.2       | FİNANSAL BİLGİ MANİPÜLASYONU YAPILMASININ NEDENLERİ.....            | 120        |
| 3.2.1     | Teşvik veya Baskı .....                                             | 121        |
| 3.2.2     | Fırsat .....                                                        | 121        |
| 3.2.3     | Haklı Gösterme (Rasyonelleştirme).....                              | 122        |
| 3.2.4     | Yetenek .....                                                       | 122        |
| 3.3       | FİNANSAL BİLGİ MANİPÜLASYONU TÜRLERİ .....                          | 125        |
| 3.3.1     | Varlıkların Kötüye Kullanılması (Çalışan Hileleri).....             | 127        |
| 3.3.2     | Yolsuzluk .....                                                     | 128        |
| 3.3.3     | Finansal Tablo Hileleri (Yönetim Hileleri).....                     | 128        |
| 3.4       | FİNANSAL BİLGİ MANİPÜLASYONUNUN AMAÇLARI .....                      | 129        |
| 3.5       | FİNANSAL BİLGİ MANİPÜLASYONU YÖNTEMLERİ .....                       | 131        |
| 3.5.1     | Kazanç Yönetimi (Earnings Management).....                          | 132        |
| 3.5.2     | Karın İstikrarlı Hale Getirilmesi (Income Smoothing).....           | 133        |
| 3.5.3     | Büyük Temizlik Muhasebesi (Big Bath Accounting).....                | 134        |
| 3.5.4     | Agresif Muhasebe (Aggressive Accounting).....                       | 134        |
| 3.5.5     | Yaratıcı Muhasebe Uygulamaları (Creative Accounting Practices)..... | 135        |

|         |                                                                                                   |            |
|---------|---------------------------------------------------------------------------------------------------|------------|
| 3.5.6   | Hileli Finansal Raporlama (Fraudulent Financial Reporting) .....                                  | 137        |
| 3.6     | FİNANSAL BİLGİ MANİPÜLASYONUNUN TESPİT EDİLMESİNDE VE<br>ÖNLENMESİNDE UYGULANAN YAKLAŞIMLAR ..... | 137        |
| 3.6.1   | Reaktif Yaklaşımlar .....                                                                         | 141        |
| 3.6.1.1 | İç kontrol .....                                                                                  | 141        |
| 3.6.1.2 | İç denetim.....                                                                                   | 143        |
| 3.6.1.3 | Bağımsız denetim.....                                                                             | 144        |
| 3.6.1.4 | Çapraz denetim tekniği .....                                                                      | 145        |
| 3.6.1.5 | Kırmızı bayraklar .....                                                                           | 146        |
| 3.6.1.6 | Hile ihbar hatları .....                                                                          | 147        |
| 3.6.1.7 | Fısıltı yöntemi (Bilgi ifşası -Whistleblowing) .....                                              | 148        |
| 3.6.2   | Proaktif Yaklaşımlar .....                                                                        | 150        |
| 3.6.2.1 | Analitik inceleme teknikleri (Mali analiz) .....                                                  | 150        |
| 3.6.2.2 | İstatistiki yöntemler.....                                                                        | 152        |
| 3.6.2.3 | Dijital analiz teknikleri : Benford Kanunu.....                                                   | 154        |
| 3.6.2.4 | Bilgisayar destekli denetim teknikleri : Sürekli denetim .....                                    | 157        |
| 3.6.2.5 | Veri madenciliği analiz teknikleri.....                                                           | 159        |
| 3.6.2.6 | Kurumsal yönetim (Corporate governance).....                                                      | 164        |
| 3.6.2.7 | Adli muhasebe (Forensic accounting).....                                                          | 166        |
| 4.      | <b>BLOKZİNCİR TEKNOLOJİSİNİN FİNANSAL BİLGİ MANİPÜLASYONUNU<br/>AZALTMADA KULLANILMASI .....</b>  | <b>169</b> |
| 4.1     | BLOKZİNCİR TABANLI MUHASEBE.....                                                                  | 170        |
| 4.1.1   | Küresel Kayıt Defteri (World Wide Ledger - WWL).....                                              | 174        |
| 4.1.2   | Üç Taraflı Kayıt Sistemi (Triple-Entry Accounting – TEA) .....                                    | 175        |
| 4.1.3   | Günlük İşlemlerin Değiştirilemez ve Otomatik Kaydı .....                                          | 182        |
| 4.1.4   | Gerçek Zamanlı ve Otomatik Finansal Tablo Sunumu.....                                             | 185        |
| 4.1.5   | Dinamik Analiz ve Etkin Karar Alma Süreci .....                                                   | 187        |
| 4.2     | BLOKZİNCİR TABANLI DENETİM.....                                                                   | 189        |
| 4.2.1   | Gerçek Zamanlı Sürekli Denetim .....                                                              | 190        |

|           |                                                                                                                               |            |
|-----------|-------------------------------------------------------------------------------------------------------------------------------|------------|
| 4.2.2     | Otomatik Doğrulanabilir Kanıt Üretme .....                                                                                    | 191        |
| 4.2.3     | Tüm İşlemlerin Denetimi .....                                                                                                 | 192        |
| 4.2.4     | Denetim Risklerinin Azalması .....                                                                                            | 192        |
| 4.2.5     | Tasdik Hizmetlerinin Kolaylaşması ve Otomatik Vergi Denetimi .....                                                            | 194        |
| 4.3       | BLOKZİNCİR TEKNOLOJİSİNİN FİNANSAL BİLGİ MANİPÜLASYONU UYGULAMALARINA ETKİSİ .....                                            | 197        |
| 4.3.1     | Finansal Bilgi Manipülasyonlarını Azaltmaya Yönelik Avantajları .....                                                         | 197        |
| 4.3.2     | Finansal Bilgi Manipülasyonlarına Yönelik Yeni Tehdit ve Riskler.....                                                         | 202        |
| 4.4       | BLOKZİNCİR TEKNOLOJİSİNE GEÇİŞİN SEKTÖRE ETKİLERİ.....                                                                        | 205        |
| 4.4.1     | İşletmelere Etkisi .....                                                                                                      | 206        |
| 4.4.2     | Meslek Profesyonellerine Etkisi .....                                                                                         | 208        |
| 4.4.3     | Kamuya Etkisi.....                                                                                                            | 209        |
| <b>5.</b> | <b>ARAŞTIRMANIN KURAMSAL ÇERÇEVESİ .....</b>                                                                                  | <b>211</b> |
| 5.1       | ARAŞTIRMANIN KONUSU .....                                                                                                     | 211        |
| 5.2       | ARAŞTIRMANIN AMACI VE ÖNEMİ .....                                                                                             | 211        |
| 5.3       | ARAŞTIRMANIN VARSAYIM VE SINIRLARI .....                                                                                      | 212        |
| 5.3.1     | Araştırmanın Varsayımları.....                                                                                                | 212        |
| 5.3.2     | Araştırmanın Sınırları .....                                                                                                  | 213        |
| 5.4       | ARAŞTIRMA SORULARI.....                                                                                                       | 214        |
| 5.5       | ARAŞTIRMANIN LİTERATÜRE SAĞLADIĞI KATKI.....                                                                                  | 215        |
| 5.5.1     | Teknolojinin Benimsenmesinde Kullanılan Modeller .....                                                                        | 216        |
| 5.5.2     | Teknoloji Kabul Modeli (Technology Acceptance Model – TAM/TKM).....                                                           | 222        |
| 5.5.3     | Teknoloji Kabul Modeli ve Blokzincir ile ilgili Çalışmalar .....                                                              | 224        |
| <b>6.</b> | <b>ARAŞTIRMANIN YÖNTEMİ .....</b>                                                                                             | <b>230</b> |
| 6.1       | ARAŞTIRMANIN MODELİ VE HİPOTEZLERİ .....                                                                                      | 230        |
| 6.1.1     | Araştırmanın Hipotezleri .....                                                                                                | 230        |
| 6.1.1.1   | Teknoloji Kabul Modeli hipotezleri.....                                                                                       | 230        |
| 6.1.1.2   | Demografik ve mesleki özelliklere göre Teknoloji Kabul Modeli boyutlarının farklılık analizine yönelik ölçek hipotezleri..... | 232        |

|         |                                                                                                                                                             |            |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 6.1.1.3 | ACFE hile arařtırmaları ölçeęi hipotezleri .....                                                                                                            | 233        |
| 6.1.1.4 | İřgüden Kılıç & Anadolu (2018) tarafından hazırlanan muhasebe hilelerinin önlenmesinde kullanılan araçlara yönelik makalede kullanılan ölçek hipotezleri... | 234        |
| 6.1.2   | Arařtırmanın Modeli .....                                                                                                                                   | 234        |
| 6.2     | ARAřTIRMA EVRENİ VE ÖRNEKLEM PLANI .....                                                                                                                    | 236        |
| 6.3     | ARAřTIRMADA KULLANILAN VERİ TOPLAMA YÖNTEMLERİ .....                                                                                                        | 238        |
| 6.3.1   | Döküman İnceleme .....                                                                                                                                      | 238        |
| 6.3.2   | Anket .....                                                                                                                                                 | 239        |
| 6.3.2.1 | Anket formunun yapısı .....                                                                                                                                 | 239        |
| 6.3.2.2 | Anketin uygulanması .....                                                                                                                                   | 241        |
| 6.4     | ARAřTIRMADA KULLANILAN VERİ ANALİZ YÖNTEMLERİ .....                                                                                                         | 242        |
| 6.4.1   | Parametrik Testler .....                                                                                                                                    | 243        |
| 6.4.1.1 | Doęrulamayı faktör analizi (DFA) .....                                                                                                                      | 243        |
| 6.4.1.2 | Korelasyon analizi .....                                                                                                                                    | 248        |
| 6.4.1.3 | Çoklu regresyon analizi .....                                                                                                                               | 249        |
| 6.4.1.4 | T testi .....                                                                                                                                               | 250        |
| 6.4.2   | Parametrik Olmayan Testler .....                                                                                                                            | 250        |
| 6.4.2.1 | Mann-Whitney U testi .....                                                                                                                                  | 250        |
| 6.4.2.2 | Kruskal-Wallis testi .....                                                                                                                                  | 251        |
| 7.      | <b>ARAřTIRMANIN BULGULARI VE YORUM .....</b>                                                                                                                | <b>252</b> |
| 7.1     | DEMOGRAFİK BULGULAR .....                                                                                                                                   | 252        |
| 7.2     | TEKNOLOJİK ÜRÜN KULLANIMINA AİT BULGULAR .....                                                                                                              | 254        |
| 7.3     | TEKNOLOJİ KABUL MODELİNE AİT BULGULAR .....                                                                                                                 | 258        |
| 7.3.1   | Güvenilirlik Analizine Ait Bulgular .....                                                                                                                   | 258        |
| 7.3.2   | Normallik Testi ve Tanımlayıcı İstatistik Bulguları .....                                                                                                   | 258        |
| 7.3.3   | Doęrulamayı Faktör Analizine Ait Bulgular .....                                                                                                             | 260        |
| 7.3.4   | Korelasyon Analizine Ait Bulgular .....                                                                                                                     | 263        |
| 7.3.5   | Teknoloji Kabul Modeli Hipotezlerinin Test Edilmesi ve Sonuçları .....                                                                                      | 265        |
| 7.3.5.1 | Standart çoklu regresyon analizine ait bulgular .....                                                                                                       | 266        |



|           |                                                                                                                                                                                                                    |            |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 7.3.5.2   | TKM hipotezlerinin sonuçları .....                                                                                                                                                                                 | 274        |
| 7.3.6     | Demografik Özelliklere Göre TKM Boyutlarına Yönelik Farklılıkların Test Edilmesi ve Sonuçları .....                                                                                                                | 275        |
| 7.3.6.1   | T testine ait bulgular.....                                                                                                                                                                                        | 276        |
| 7.3.6.2   | TKM farklılık hipotezlerinin sonuçları .....                                                                                                                                                                       | 284        |
| 7.4       | HİLE ARAŞTIRMALARI ÖLÇEĞİNE AİT BULGULAR.....                                                                                                                                                                      | 285        |
| 7.4.1     | Güvenilirlik Analizine Ait Bulgular .....                                                                                                                                                                          | 286        |
| 7.4.2     | Normallik Testi ve Tanımlayıcı İstatistik Bulguları .....                                                                                                                                                          | 286        |
| 7.4.3     | Demografik ve Mesleki Özelliklere Göre Hile Belirtileri ile Karşılaşma Sıklıklarına Yönelik Farklılıkların Test Edilmesi ve Sonuçları.....                                                                         | 287        |
| 7.4.3.1   | Mann-Whitney U testine ait bulgular.....                                                                                                                                                                           | 287        |
| 7.4.3.2   | Kruskal-Wallis testine ait bulgular.....                                                                                                                                                                           | 292        |
| 7.4.3.3   | Hile araştırmaları hipotezlerinin sonuçları-1 .....                                                                                                                                                                | 298        |
| 7.4.4     | Demografik ve Mesleki Özelliklere Göre Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonlarını Önlemedeki Rolüne İlişkin Mali Müşavirlerin Görüşlerine Yönelik Farklılıkların Test Edilmesi ve Sonuçları ..... | 300        |
| 7.4.4.1   | Mann-Whitney U testine ait bulgular.....                                                                                                                                                                           | 301        |
| 7.4.4.2   | Kruskal-Wallis testine ait bulgular.....                                                                                                                                                                           | 305        |
| 7.4.4.3   | Hile araştırmaları hipotezlerinin sonuçları-2 .....                                                                                                                                                                | 312        |
| <b>8.</b> | <b>SONUÇ VE ÖNERİLER .....</b>                                                                                                                                                                                     | <b>314</b> |
| 8.1       | TEORİK ÇIKARIMLAR .....                                                                                                                                                                                            | 319        |
| 8.2       | PRATİK ÇIKARIMLAR.....                                                                                                                                                                                             | 321        |
| 8.3       | ÖNERİLER.....                                                                                                                                                                                                      | 322        |
| 8.4       | AKADEMİSYENLERE ÖNERİLER .....                                                                                                                                                                                     | 322        |
|           | <b>REFERANSLAR .....</b>                                                                                                                                                                                           | <b>324</b> |
|           | <b>EK A .....</b>                                                                                                                                                                                                  | <b>355</b> |
|           | <b>EK B.....</b>                                                                                                                                                                                                   | <b>358</b> |

## TABLO LİSTESİ

### Sayfa

|                                                                                                 |     |
|-------------------------------------------------------------------------------------------------|-----|
| Tablo 2.1: Blokzincir Tanımları. ....                                                           | 6   |
| Tablo 2.2: Blokzincir Teknolojisini Şekillendiren Teknolojik İlerlemeler. ....                  | 13  |
| Tablo 2.3: Blokzincir Teknolojisinde 2009-2014 Yılları Arasında Yaşanan Gelişmeler. ..          | 17  |
| Tablo 2.4: Blokzincir Teknolojisinde 2014-2020 Yılları Arasında Yaşanan Gelişmeler. ..          | 19  |
| Tablo 2.5: Blokzincir Teknolojisinde 2020 Sonrası Yaşanan Gelişmeler. ....                      | 21  |
| Tablo 2.6: Mutabakat Algoritmalarının Karşılaştırılması. ....                                   | 73  |
| Tablo 2.7: Kripto Cüzdanlar. ....                                                               | 78  |
| Tablo 2.8: Blokzincir Türlerinin Karşılaştırılması. ....                                        | 102 |
| Tablo 2.9: En Yüksek Piyasa Değerine Sahip Blokzincir Platformları. ....                        | 103 |
| Tablo 2.10: Blokzincir Platformlarının Karşılaştırması. ....                                    | 104 |
| Tablo 2.11: Blokzincir Teknolojisinin Uygulama Alanları. ....                                   | 107 |
| Tablo 3.1: KPMG Raporuna Göre Hile Nedenleri. ....                                              | 124 |
| Tablo 3.2: KPMG Raporuna Göre Hile Motivasyonları. ....                                         | 125 |
| Tablo 3.3: KPMG Raporuna Göre Suistimal Türleri. ....                                           | 125 |
| Tablo 3.4: PwC Raporuna Göre Finansal ve Ekonomik Suçlar ve Hileler. ....                       | 126 |
| Tablo 3.5: Yıllar İtibarıyla Türlerine Göre Suistimal Gerçekleşme Oranları ve Maliyetleri. .... | 138 |
| Tablo 3.6: KPMG ve ACFE Raporlarına Göre Suistimal Tespit Yöntemleri ve Vaka Oranları. ....     | 140 |
| Tablo 3.7: ACFE 2024 Raporuna Göre Kırmızı Bayrak Belirteçleri. ....                            | 146 |

|                                                                                                                                                |     |
|------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Tablo 3.8: ACFE 2024 Raporuna Göre İhbarcıların İlk Raporlama Birimleri.....                                                                   | 149 |
| Tablo 3.9: Finansal Bilgi Manipülasyonu Tespitinde Kullanılan İstatistiki Modeller. ....                                                       | 152 |
| Tablo 3.10: Benford Kanunu’na Göre Rakamların Görülme Sıklığı. ....                                                                            | 155 |
| Tablo 3.11: Geleneksel ve Sürekli Denetimin Karşılaştırılması- 1. ....                                                                         | 159 |
| Tablo 3.12: Geleneksel ve Sürekli Denetimin Karşılaştırılması- 2. ....                                                                         | 159 |
| Tablo 4.1: Üç Taraflı Kayıt Sisteminin Gelişimine Katkı Sağlayan Önemli Çalışmalar..                                                           | 178 |
| Tablo 5.1: Teknolojinin Benimsenmesinde Kullanılan Modeller. ....                                                                              | 218 |
| Tablo 5.2: Blokzincir Teknolojisi Kabulünün Teknoloji Kabul Modeli (TKM) ile Ölçülmesi<br>Konusunda Yapılan Yayınlar ve Çalışma Alanları. .... | 225 |
| Tablo 6.1: Araştırmada Kullanılan Analiz Yöntemleri. ....                                                                                      | 243 |
| Tablo 6.2: DFA Uyum İndeksleri ve Eşik Değerleri.....                                                                                          | 244 |
| Tablo 7.1: Katılımcıların Demografik Bilgilerine Göre Dağılımları. ....                                                                        | 254 |
| Tablo 7.2: Katılımcıların Teknolojik Ürün Kullanım Sıklığına Göre Dağılımları.....                                                             | 256 |
| Tablo 7.3: TKM Ölçeğine İlişkin Normallik Testi ve Tanımlayıcı İstatistik Bulguları....                                                        | 259 |
| Tablo 7.4: TKM Doğrulayıcı Faktör Analizi Uyum İyiliği Değerleri.....                                                                          | 260 |
| Tablo 7.5: TKM Doğrulayıcı Faktör Analizi Regresyon Ağırlıkları.....                                                                           | 261 |
| Tablo 7.6: Ölçek Boyutları İtibarıyla Güvenilirlik Analizi Sonuçları.....                                                                      | 263 |
| Tablo 7.7: TKM Ölçeği Korelasyon Analizi. ....                                                                                                 | 264 |
| Tablo 7.8: TKM Standart Çoklu Regresyon Analizi (Tutum). ....                                                                                  | 267 |
| Tablo 7.9: TKM Standart Çoklu Regresyon Analizi (Niyet). ....                                                                                  | 269 |
| Tablo 7.10: TKM Standart Çoklu Regresyon Analizi (Davranış).....                                                                               | 271 |
| Tablo 7.11: TKM Hipotez Sonuç Tablosu. ....                                                                                                    | 274 |

|                                                                                                                                                                           |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Tablo 7.12: Katılımcıların TKM Boyutları Açısından Cinsiyetlerine Göre Farklılıkları..                                                                                    | 277 |
| Tablo 7.13: Katılımcıların TKM Boyutları Açısından Mesleki Ünvanlarına Göre Farklılıkları. ....                                                                           | 281 |
| Tablo 7.14: TKM Farklılık Hipotezlerinin Sonuçları.....                                                                                                                   | 284 |
| Tablo 7.15: Hile Araştırmaları Ölçeğine İlişkin Normallik Testi ve Tanımlayıcı İstatistik Bulguları. ....                                                                 | 286 |
| Tablo 7.16 Katılımcıların Hile Belirtileri ile Karşılaşma Sıklıkları Açısından Cinsiyetlerine Göre Farklılıkları. ....                                                    | 288 |
| Tablo 7.17: Katılımcıların Hile Belirtileri ile Karşılaşma Sıklıkları Açısından Mesleki Ünvanlarına Göre Farklılıkları. ....                                              | 290 |
| Tablo 7.18: Katılımcıların Hile Belirtileri ile Karşılaşma Sıklıkları Açısından Çalışma Şekillerine Göre Farklılıkları.....                                               | 291 |
| Tablo 7.19: Katılımcıların Hile Belirtileri ile Karşılaşma Sıklıkları Açısından Eğitim Düzeylerine Göre Farklılıkları.....                                                | 293 |
| Tablo 7.20: Katılımcıların Hile Belirtileri ile Karşılaşma Sıklıkları Açısından Mesleki Tecrübelerine Göre Farklılıkları.....                                             | 295 |
| Tablo 7.21: Katılımcıların Hile Belirtileri ile Karşılaşma Sıklıkları Açısından Mükellef Sayılarına Göre Farklılıkları.....                                               | 297 |
| Tablo 7.22: Hile Araştırmaları Hipotezleri Sonuç Tablosu-1. ....                                                                                                          | 299 |
| Tablo 7.23: Cinsiyet, Ünvan ve Eğitim Düzeyi Gruplarına Göre Farklılık Analizi Sonuçları. ....                                                                            | 299 |
| Tablo 7.24: Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Cinsiyetlerine Göre Farklılıkları.....  | 302 |
| Tablo 7.25: Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Mesleki Ünvanlarına Göre Farklılıkları. | 303 |

|                                                                                                                                                                                         |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Tablo 7.26: Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Çalışma Şekillerine Göre Farklılıkları...             | 304 |
| Tablo 7.27: Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Eğitim Düzeylerine Göre Farklılıkları...              | 305 |
| Tablo 7.28: Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Mesleki Tecrübelerine Göre Farklılıkları. ....        | 307 |
| Tablo 7.29: Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Mükellef Sayılarına Göre Farklılıkları. .             | 309 |
| Tablo 7.30: Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Blokzincir Bilgi Düzeylerine Göre Farklılıkları. .... | 311 |
| Tablo 7.31: Hile Araştırmaları Hipotezleri Sonuç Tablosu-2. ....                                                                                                                        | 313 |

## ŞEKİL LİSTESİ

|                                                                         | <u>Sayfa</u> |
|-------------------------------------------------------------------------|--------------|
| Şekil 2.1: Bitcoin Genesis Bloğu.....                                   | 11           |
| Şekil 2.2: İlk Bitcoin Transferi.....                                   | 12           |
| Şekil 2.3: Blokzincir Teknolojisinin Evreleri.....                      | 16           |
| Şekil 2.4: Blok Yapısı.....                                             | 22           |
| Şekil 2.5: Merkle Kök Hash Değerin Oluşturulması.....                   | 24           |
| Şekil 2.6: Blok Dizisi Örneği. ....                                     | 24           |
| Şekil 2.7: Merkle'in Dijital İmza Sağlama Yöntemi.....                  | 25           |
| Şekil 2.8: Ağ Yapıları.....                                             | 29           |
| Şekil 2.9: Kriptografi Yöntemleri ve En Yaygın Algoritma Örnekleri..... | 33           |
| Şekil 2.10: Anahtarlı Kriptografi Süreci.....                           | 34           |
| Şekil 2.11: SHA-256 Fonksiyon Özeti.....                                | 39           |
| Şekil 2.12: İş Kanıtı Bulmacası.....                                    | 48           |
| Şekil 2.13: Madencilik ile Hash Üretme.....                             | 48           |
| Şekil 2.14: Çatallanma Türleri.....                                     | 51           |
| Şekil 2.15: Blokzincirin Çatallanması.....                              | 52           |
| Şekil 2.16: Yumuşak Çatallanma ve Sert Çatallanma.....                  | 54           |
| Şekil 2.17: Paranın Sınıflandırması.....                                | 55           |
| Şekil 2.18: İş Kanıtı Mutabakat Algoritması.....                        | 65           |
| Şekil 2.19: PoW Madenciliğinin Evrimi.....                              | 68           |
| Şekil 2.20: Kripto Cüzdan Türleri.....                                  | 76           |

|                                                                                                  |     |
|--------------------------------------------------------------------------------------------------|-----|
| Şekil 2.21: Blokzincir Teknolojisi Mimari Katmanları.....                                        | 86  |
| Şekil 2.22: Blokzincir Türleri.....                                                              | 100 |
| Şekil 2.23: Türkiye’de Bilinen Blokzincir Platformları. ....                                     | 103 |
| Şekil 2.24: Blokzincir Teknolojisinin Kullanılabileceği Çeşitli Sektörler ve Alanlar. ....       | 106 |
| Şekil 3.1: Finansal Bilginin Sınıflandırılması. ....                                             | 117 |
| Şekil 3.2: Finansal Bilgi Manipülasyonu Yöntemleri. ....                                         | 131 |
| Şekil 3.3: Finansal Bilgi Manipülasyonunun Tespitinde ve Önlenmesinde Uygulanan Yaklaşımlar..... | 139 |
| Şekil 3.4: Veri Madenciliği Modelleri.....                                                       | 161 |
| Şekil 3.5: Hile Tespitinde Karar Ağacı Uygulama Örneği.....                                      | 162 |
| Şekil 3.6: Yapay Sinir Ağlarının Modellemesi. ....                                               | 164 |
| Şekil 4.1: Üç Taraflı Kayıt Yönteminin Basit Örneği. ....                                        | 180 |
| Şekil 5.1: Orijinal Teknoloji Kabul Modeli. ....                                                 | 223 |
| Şekil 5.2: Yaygın Kullanılan Teknoloji Kabul Modeli. ....                                        | 223 |
| Şekil 6.1: TKM Araştırma Modeli-1. ....                                                          | 235 |
| Şekil 6.2: TKM Araştırma Modeli-2. ....                                                          | 235 |
| Şekil 6.3: Hile Araştırmaları Ölçeği Araştırma Modeli. ....                                      | 236 |
| Şekil 7.1: Teknoloji Kabul Modelinin Doğrulayıcı Faktör Analizi Diyagramı. ....                  | 262 |

## KISALTMALAR

|         |                                                                                                              |
|---------|--------------------------------------------------------------------------------------------------------------|
| A.Ş.    | : Anonim Şirket                                                                                              |
| AAA     | : American Accounting Association (Amerikan Muhasebe Derneği)                                                |
| ABD     | : Amerika Birleşik Devletleri                                                                                |
| ACFE    | : Association of Certified Fraud Examiners (Sertifikalı Suistimal İnceleme Uzmanları Derneği)                |
| AES     | : Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)                                                |
| AF      | : Algılanan Fayda                                                                                            |
| AGFI    | : Adjustment Goodness of Fit Index (Düzeltilmiş Uyum İyiliği İndeksi)                                        |
| AI      | : Artificial Intelligence (Yapay Zekâ)                                                                       |
| AICPA   | : American Institute of Certified Public Accountants (Amerikan Serbest Muhasebeci Mali Müşavirler Enstitüsü) |
| AKK     | : Algılanan Kullanım Kolaylığı                                                                               |
| Altcoin | : Alternative Coin (Alternatif kriptopara)                                                                   |
| ARPAnet | : Advanced Research Projects Agency Network (İleri Araştırma Projeleri Ajansı Ağı)                           |
| ASIC    | : Application-Specific Integrated Circuit (Uygulamaya Özgü Entegre Devre)                                    |
| ATM     | : Automated Teller Machine (Otomatik Vezne Makinesi)                                                         |
| BCH     | : Bitcoin Cash                                                                                               |
| BCT     | : Blockchain Technology (Blokzincir Teknolojisi)                                                             |
| BDS     | : Bağımsız Denetim Standardı                                                                                 |
| BFT     | : Byzantine Fault Tolerance (Bizans Hata Toleransı)                                                          |
| BIST    | : Borsa İstanbul                                                                                             |
| Bknz    | : Bakınız                                                                                                    |



|       |                                                                                                 |
|-------|-------------------------------------------------------------------------------------------------|
| BNB   | : Binance Coin                                                                                  |
| BTC   | : Bitcoin                                                                                       |
| C.R.  | : Critical Ratio (Kritik Oran)                                                                  |
| CAATs | : Computer Assisted Audit Techniques (Bilgisayar Destekli Denetim Teknikleri)                   |
| CFE   | : Certified Fraud Examiner (Suistimal İnceleme Uzmanlığı) - SİU                                 |
| CFI   | : Comparative Fit Index (Karşılaştırmalı Uyum İndeksi)                                          |
| CICA  | : The Canadian Institute of Chartered Accountants (Kanada Yeminli Mali Müşavirler Enstitüsü)    |
| COSO  | : Committee of Sponsoring Organisations (Sponsor Kuruluşlar Komitesi)                           |
| CPA   | : Certified Public Accountant (Sertifikalı Kamu Muhasebecisi / Serbest Muhasebeci Mali Müşavir) |
| CPU   | : Central Processing Unit (Merkezi İşlem Birimi)                                                |
| DACs  | : Decentralized Autonomous Communities (Merkeziyetsiz Otonom Topluluklar)                       |
| DAG   | : Directed Acyclic Graph (Yönlendirilmiş Döngüsüz Grafik)                                       |
| DAO   | : Decentralized Autonomous Organization (Merkeziyetsiz Otonom Organizasyon)                     |
| DApps | : Decentralized Applications (Merkeziyetsiz Uygulamalar)                                        |
| DASs  | : Decentralized Autonomous Systems (Merkeziyetsiz Otonom Sistemler)                             |
| DEA   | : Double-Entry Accounting (Çift Taraflı Kayıt Sistemi)                                          |
| Defi  | : Decentralized Finance (Merkeziyetsiz Finans Uygulamaları)                                     |
| DES   | : Data Encryption Standard (Veri Şifreleme Standardı)                                           |
| DFA   | : Doğrulayıcı Faktör Analizi                                                                    |
| DH    | : Diffie-Helman                                                                                 |
| DLT   | : Distributed Ledger Technology (Dağıtık Defter Teknolojisi)                                    |
| DOI   | : Diffusion of Innovation Theory (Yenilik Yayılım Teorisi)                                      |

|       |                                                                                      |
|-------|--------------------------------------------------------------------------------------|
| DoS   | : Denial of Service (Hizmet Reddi)                                                   |
| DSA   | : Digital Signature Algorithm (Dijital İmza Algoritması)                             |
| DVR   | : Davranış                                                                           |
| ECDSA | : Elliptic Curve Digital Signature Algorithm (Eliptik Eğri Dijital İmza Algoritması) |
| e-CNY | : Dijital Yuan                                                                       |
| EDI   | : Electronic Data Interchange (Elektronik Veri Değişimi)                             |
| ENG   | : Engel                                                                              |
| ERP   | : Enterprise Resource Planning (Kurumsal Kaynak Planlama)                            |
| ETF   | : Exchange-Traded Fund (Borsa Yatırım Fonu)                                          |
| ETH   | : Ether                                                                              |
| EVM   | : Ethereum Virtual Machine (Ethereum Sanal Makinesi)                                 |
| EY    | : Earnst & Young (Muhasebe-Denetim Danışmanlık Firması)                              |
| FBI   | : Federal Bureau of Investigation (Federal Soruşturma Bürosu)                        |
| FEI   | : Financial Executives International (Uluslararası Finans Yöneticileri Derneği)      |
| FPGA  | : Field Programmable Gate Arrays (Alan Programlanabilir Kapı Dizisi)                 |
| GAAP  | : Generally Accepted Accounting Principles                                           |
| GB    | : Gigabyte                                                                           |
| GFI   | : Goodness of Fit Index (Uyum İyiliği İndeksi)                                       |
| GKGMİ | : Genel Kabul Görmüş Muhasebe İlkeleri                                               |
| GPU   | : Graphics Processing Unit (Grafik İşlemci Birimi)                                   |
| HTTP  | : Hypertext Transfer Protocol (Hiper Metin Transfer Protokolü)                       |
| IBAN  | : International Bank Account Number (Uluslararası Banka Hesap Numarası)              |

|           |                                                                                   |
|-----------|-----------------------------------------------------------------------------------|
| IBM       | : International Business Machines (Uluslararası İş Makineleri)                    |
| IIA       | : The Institute of Internal Auditors (İç Denetçiler Enstitüsü)                    |
| IIoT      | : Industrial Internet of Things (Endüstriyel Nesnelerin İnterneti)                |
| IMA       | : Institute of Management Accountants (Yönetim Muhasebecileri Enstitüsü)          |
| Inc.      | : Incorporated (Anonim Şirket)                                                    |
| IOS       | : iPhone Operating System (Iphone İşletim Sistemi)                                |
| IoT       | : Internet of Things (Nesnelerin İnterneti)                                       |
| ISP (ISS) | : Internet Service Provider (İnternet Servis Sağlayıcısı)                         |
| İSMMMO    | : İstanbul Serbest Muhasebeci Mali Müşavirler Odası                               |
| İYMMO     | : İstanbul Yeminli Mali Müşavirler Odası                                          |
| KDV       | : Katma Değer Vergisi                                                             |
| KGK       | : Kamu Gözetim Kurumu                                                             |
| KPMG      | : Klynveld- Peat - Marwick - Goerdeler (Muhasebe-Denetim Danışmanlık Firması)     |
| KS        | : Kolmogorov-Smirnov                                                              |
| K-W       | : Kruskal-Wallis                                                                  |
| LTC       | : Litecoin                                                                        |
| MB        | : Megabyte                                                                        |
| MD5       | : Message Digest Algorithm 5 (Mesaj Özeti Algoritması 5)                          |
| MSUGT     | : Muhasebe Sistemi Uygulama Genel Tebliği                                         |
| M-W       | : Mann-Whitney U                                                                  |
| NASDAQ    | : National Association of Securities Dealers (Ulusal Menkul Kıymetler Satıcıları) |
| NFI       | : Normed Fit Index (Ölçeklendirilmiş Uyum İndeksi)                                |

|        |                                                                                             |
|--------|---------------------------------------------------------------------------------------------|
| NFS    | : Network File System (Ağ Dosya Sistemi)                                                    |
| NFT    | : Non-Fungible Token (Değiştirilemez Jeton)                                                 |
| NHST   | : Null Hypothesis Significance Test (Sıfır Hipotezi Anlamlılık Testi)                       |
| NİY    | : Niyet                                                                                     |
| NMC    | : Namecoin                                                                                  |
| NNFI   | : Non Normed Fit Index (Ölçeklendirilmemiş Uyum İndeksi)                                    |
| Nonce  | : Number Used Only Once (Tek Kullanımlık Sayı)                                              |
| NSA    | : National Security Agency (Ulusal Güvenlik Ajansı)                                         |
| NSFnet | : National Science Foundation Network (Ulusal Bilim Vakfı Ağı)                              |
| P2P    | : Peer to Peer (Eşten Eşe)                                                                  |
| PBFT   | : Practical Byzantine Fault Tolerance (Pratik Bizans Hata Toleransı)                        |
| PGP    | : Pretty Good Privacy (Oldukça İyi Gizlilik)                                                |
| PoA    | : Proof of Authority (Otorite Kanıtı)                                                       |
| POS    | : Point Of Sale (Ödeme Noktası)                                                             |
| PoS    | : Proof of Stake (Pay Kanıtı)                                                               |
| PoW    | : Proof of Work (İş Kanıtı)                                                                 |
| PPC    | : Peercoin /Peer to Peer Coin/ PP Coin                                                      |
| PWC    | : Price Waterhouse Coopers (Muhasebe-Denetim Danışmanlık Firması)                           |
| QR     | : Quick Response (Çabuk Tepki)                                                              |
| RC2    | : Rivest Cipher 2 (Rivest Şifresi 2)                                                        |
| RMR    | : Root Mean Square Residual (Kök Artık Kareler Ortalaması)                                  |
| RMSEA  | : Root Mean Square Error of Approximation (Yaklaşık Hataların Kök Artık Kareler Ortalaması) |

|        |                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------|
| RPoW   | : Reusable Proofs of Work (Yeniden Kullanılabilir İş Kanıtı)                                    |
| RSA    | : Rivest-Shamir-Adleman                                                                         |
| S.E.   | : Standart Error (Standart Hata)                                                                |
| SAS    | : Statements on Auditing Standards                                                              |
| SEA    | : Single-Entry Accounting (Tek Taraflı Kayıt Sistemi)                                           |
| SEC    | : Securities and Exchange Commission (Amerika Menkul Kıymetler ve Borsa Komisyonu)              |
| SegWit | : Segregated Witness (Ayrılmış Tanık)                                                           |
| SHA    | : Secure Hash Algorithm (Güvenli Hash Algoritması)                                              |
| SiU    | : Suistimal İnceleme Uzmanlığı                                                                  |
| SMMM   | : Serbest Muhasebeci Mali Müşavir                                                               |
| SOX    | : Sarbanes-Oxley Act (Sarbanes-Oxley Yasası)                                                    |
| SPK    | : Sermaye Piyasası Kurulu                                                                       |
| SRMR   | : Standardized Root Mean Square Residual<br>(Standartlaştırılmış Kök Artık Kareler Ortalaması)  |
| Std.   | : Standart                                                                                      |
| TAM    | : Technology Acceptance Model (Teknoloji Kabul Modeli)                                          |
| TCP/IP | : Transmission Control Protocol/Internet Protocol (İletim Denetim Protokolü/İnternet Protokolü) |
| TDK    | : Türk Dil Kurumu                                                                               |
| TEA    | : Triple-Entry Accounting (Üç Taraflı Kayıt Sistemi)                                            |
| Teksa  | : Tek Kullanımlık Sayı                                                                          |
| TKM    | : Teknoloji Kabul Modeli                                                                        |
| TL     | : Türk lirası                                                                                   |
| TLI    | : Trucker-Lewis Index (Trucker-Lewis İndeksi)                                                   |

|        |                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------|
| TMS    | : Türkiye Muhasebe Standartları                                                                       |
| TOE    | : Technology – Organization - Environment<br>(Teknoloji – Organizasyon – Çevre Modeli)                |
| TPB    | : Theory of Planned Behavior (Planlı Davranış Teorisi)                                                |
| TRA    | : Theory of Reasoned Action (Sebepli Davranış Teorisi)                                                |
| TTF    | : Task Technology Fit (İş-Teknoloji Uygunluk Modeli)                                                  |
| TTP    | : Trusted Third Party (Güvenilir Üçüncü Taraf)                                                        |
| TUT    | : Tutum                                                                                               |
| TÜRMOB | : Türkiye Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali<br>Müşavirler Odaları Birliği            |
| TÜSİAD | : Türk Sanayicileri ve İş İnsanları Derneği                                                           |
| UFRS   | : Uluslararası Finansal Raporlama Standartları                                                        |
| USB    | : Universal Serial Bus (Evrensel Seri Veriyolu)                                                       |
| USD    | : United States Dollar (Amerikan doları)                                                              |
| USİUD  | : Uluslararası Suistimal İnceleme Uzmanları Derneği                                                   |
| UTADIS | : Utilities Additives Discriminantes (Çok Kriterli Karar Analizi )                                    |
| UTAUT  | : Unified Technology Acceptance and Use Theory (Birleştirilmiş<br>Teknoloji Kabul ve Kullanım Modeli) |
| v.b    | : Ve bunun gibi                                                                                       |
| VIF    | : Variance Inflation Factor (Varyans Şişirme Faktörü)                                                 |
| WAN    | : Wide Area Network (Geniş Alan Ağı)                                                                  |
| WOS    | : Web Of Science                                                                                      |
| WWL    | : World Wide Ledger (Küresel Kayıt Defteri)                                                           |
| www    | : World Wide Web (Dünya Çapında Ağ)                                                                   |
| YEM    | : Yapısal Eşitlik Modeli                                                                              |

## SEMBOL LİSTESİ

|                |                                 |
|----------------|---------------------------------|
| $\square$      | : Bitcoin                       |
| $\beta$        | : Beta Katsayısı                |
| df             | : Serbestlik Derecesi           |
| F              | : Genel Anlamlılık Değeri       |
| H              | : Hipotez                       |
| H <sub>0</sub> | : Sıfır Hipotezi                |
| H <sub>1</sub> | : Alternatif Hipotez            |
| n              | : Number (Sayı)                 |
| p              | : Probability (Olasılık değeri) |
| r              | : Korelasyon Katsayısı          |
| R <sup>2</sup> | : Determinasyon Katsayısı       |
| \$             | : Dolar                         |
| $\chi^2$       | : Ki-kare                       |

## 1. GİRİŞ

Finansal bilgi manipölasyonu bir diğör adıyla muhasebe hileleri; işletme yönetiminin veya çalışanlarının, haksız veya yasal olmayan bir yarar sağlamak amacıyla işletme varlıklarını kötüye kullanmaları, işletmenin mali durumunu ve performansını olduğundan farklı göstermeye yönelik finansal raporlama sürecinde yanıltıcı bilgi sunmaları veya yasa dışı ve etik dışı faaliyetlerde bulunmaları şeklindeki kasıtlı aldatıcı davranışlarını ifade etmektedir. Enron, WorldCom, Global Crossing, Parmalat, Tyco International, Xerox, Toshiba vb. gibi örneklerine rastladığımız büyük muhasebe skandalları göstermektedir ki finansal bilgi manipölasyonları dünya genelinde pek çok ülkede ve farklı dönemlerde sürekli tekrarlayan bir olgudur ve ciddi ekonomik zararlara yol açmaktadır. Bu kapsamda ilgili ekonomik zararların boyutunu ortaya koyabilmek amacıyla Association of Certified Fraud Examiners (ACFE), iki yılda bir dünya genelinde farklı ülkeleri kapsayan bir hile araştırması yapmaktadır. Son yayımlanan “Occupational Fraud 2024: A Report To The Nations” raporunda ise dünya üzerinde 138 ülkede gerçekleşen 1.921 adet vaka incelendiğinde, 3,1 milyon \$’dan fazla kaybın meydana geldiği tespit edilmiştir (ACFE, 2024, s.4). Bu sonuç; ACFE’nin geçmiş yıllardaki rapor sonuçlarına benzer şekilde, işletmelerin, gelirlerinin yaklaşık %5’ini muhasebe hilesi sonucu kaybettiklerini göstermektedir (ACFE, 2024, s.4; ACFE, 2022, s.4; ACFE, 2020, s.9). Ancak bu zararlardan yalnızca işletme paydaşlarının etkilendiği düşünölmemelidir. İşletme gelirlerinin %5’i gibi yüksek bir oranın kaybedilmesi aynı zamanda kaynakların etkin dağılımını engellemekte ve makroekonomik düzeyde tüm toplumun refahını da olumsuz yönde etkilemektedir.

Bu açıdan değörlendirildiğinde, söz konusu kayıplarla mücadele büyük önem taşımaktadır. Finansal bilgi manipölasyonunun tespit edilmesine ve önlenmesine yönelik olarak öncelikle finansal işlem ve raporların denetlenmesi yoluyla çözüm sağlanmaya çalışılmaktadır. Bu kapsamda iç kontrol, iç denetim, bağımsız denetim gibi denetim araçları kullanılmaktadır. Bununla birlikte denetime rağmen muhasebe hata ve hileleri önlenememekte, hile ihbar hatları ve fısıltı yöntemi gibi araçlar ile ortaya çıkarılabilmektedir. Ancak bu yöntemler, manipölasyonlar gerçekleştikten yani zarar meydana geldikten sonra tespit edilmesini sağlayan geleneksel yaklaşımlardır. Manipölasyonların işletmelere ve ekonomiye yükledikleri maliyetin düşürölebilmesi için hile yapılmasını önlemeye yönelik proaktif araçlara ihtiyaç duyulmaktadır. Bu bağlamda kurumsal yönetim, adli muhasebe, analitik



inceleme (mali analiz), istatistiki yöntemler, dijital analiz teknikleri (Benford kanunu), veri madenciliği analiz teknikleri (karar ağaçları, yapay sinir ağları vb. gibi) ve bilgisayar destekli denetim teknikleri (sürekli denetim) gibi alternatif araçlar muhasebe hilelerini tespit etme amacıyla kullanılarak sisteme dahil edilmektedir.

Bununla birlikte, teknolojik ilerlemeler, finansal bilgi manipölasyonlarını tespit etme ve önleme konusunda yenilikçi araçların ortaya çıkmasına olanak tanımaktadır. Nitekim Endüstri 4.0'ı tetikleyen ve gelecekteki sanayi üretimini şekillendirecek başlıca teknolojiler arasındaki, üretim bandında kullanılan robotik sistemler, üretimi yöneten yapay zeka, tüketim verileriyle desteklenen büyük veri, yazılım ve donanımların birbirleriyle iletişimini sağlayan nesnelerin interneti, veri depolama birimi olarak bulut bilişim ve sistemin merkeziyetsiz ve otomatik yürütülebilmesini sağlayan blokzincir teknolojisi, akıllı fabrikaların oluşturulmasında kullanılabilecektir. Akıllı fabrikalar ile hedeflenen ise fiziksel dünyanın sanal bir kopyası oluşturularak, karar alma süreçlerinin merkeziyetsiz ve otomatik bir şekilde yürütüldüğü bir sistem yaratmaktır. Teknolojik gelişmelerin doğrultusunda işletmelerin akıllanması ise muhasebe ve denetim süreçlerinde kaçınılmaz bir dönüşümü beraberinde getirmektedir. Bu dönüşüm aynı zamanda finansal bilgi manipölasyonuna olanak tanıyan fırsatlar ile tespit ve önleme yaklaşımları üzerinde de etkili olmaktadır. Bu bağlamda dijital dönüşümün Endüstri 4.0 teknoloji bileşenleri itibarıyla muhasebe ve denetim süreçlerine dolaylı olarak da muhasebe hilelerine etkileri, araştırmacılar tarafından literatürde sıklıkla ele alınmaktadır. Ancak bu bileşenlerden blokzincir teknolojisinin, finansal bilgi manipölasyonlarını azaltmada kullanılmasına yönelik yeterli çalışma bulunmamaktadır. Ayrıca blokzincir teknolojisinin; merkeziyetsiz, şeffaf, izlenebilir, güvenilir, değişmez, kurcalamaya dayanıklı, denetlenebilir, inkar edilemez ve otonom yapısı sebebiyle taşıdığı finansal bilgi manipölasyonlarını azaltmada kullanılabilecek etkili bir araç olma potansiyeli de konunun araştırılmasını önemli kılmaktadır.

Özetle, blokzincir teknolojisinin sunduğu potansiyel ve literatürdeki boşluk nedeniyle bu tez çalışmasında, finansal bilgi manipölasyonunu azaltmada kullanılabilecek yeni bir yaklaşım olarak blokzincir teknolojisinin uygulanabilirliği tartışılmıştır. Diğer yandan bu süreci yönetmede aktif rol oynayan mali müşavirler arasından İstanbul'daki meslek mensuplarının blokzincir teknolojisini benimseme düzeyleri, Teknoloji Kabul Modeli kapsamında araştırılmıştır. Ek olarak ilgili mali müşavirlerin finansal bilgi manipölasyonu ile karşılaşma

sıklıkları ve muhasebe hilelerinin önlenmesinde blokzincir teknolojisinin rolü hakkındaki görüşleri değerlendirilmiştir.

Bu kapsamda çalışma giriş ve sonuç bölümleri dışında altı bölümden oluşmaktadır. İlk üç bölümde, araştırma konusuna ilişkin literatür taramaları yapılarak kavramsal çerçeve ortaya konulmuş; son üç bölümde ise ampirik araştırmanın metodolojisi ve bulgularına ilişkin kapsamlı bir değerlendirme yapılmıştır.

Çalışmanın ikinci bölümünde, blokzincir teknolojisi kavramsal hatlarıyla incelenmiştir. Bu kapsamda blokzincir teknolojisi; tanımı, tarihsel gelişim süreci, teknik unsurları, mimarisi, işleyişi, özellikleri ve türleri itibarıyla detaylı bir şekilde açıklanmıştır. Ardından da en çok bilinen dört blokzincir platformu karşılaştırmalı olarak tanımlanmış, blokzincir teknolojisinin çeşitli kullanım alanları örneklendirilmiş ve teknolojinin genel kullanımına yönelik avantaj ve dezavantajları özetlenmiştir.

Üçüncü bölümde, çalışmanın diğer bir kavramı finansal bilgi manipülasyonuna (muhasebe hileleri) ilişkin kavramsal yapı ele alınmıştır. İlgili çerçevede finansal bilgi ve finansal bilgi manipülasyonu kavramları tanımlanmış, finansal bilgi manipülasyonu nedenleri, türleri, amaçları ve yöntemlerine ilişkin açıklamalar yapılmıştır. Sonrasında ise finansal bilgi manipülasyonlarının tespit edilmesinde ve önlenmesinde uygulanan yaklaşımlar, reaktif ve proaktif sınıflandırmaları altında kısaca incelenmiştir.

Dördüncü bölümde, blokzincir teknolojisinin finansal bilgi manipülasyonunu azaltmadaki potansiyeli üzerine teorik bir çerçeve sunulmuştur. Bu çerçevede muhasebe ve denetim süreçlerinde blokzincir teknolojisinin uygulanabilirliği ortaya konulmuştur. Ardından genel itibarıyla blokzincir teknolojisinin finansal bilgi manipülasyonunu engellemeye yönelik avantajları ve bu teknolojinin kullanımının yarattığı tehdit ve riskler özetlenmiştir. Sonrasında ise blokzincir teknolojisi tabanlı uygulamaların, muhasebe ve denetim sektörüne olası etkileri değerlendirilmiştir.

Beşinci bölümde, araştırmanın kuramsal çerçevesi; araştırmanın konusu, amacı, önemi, varsayımları, sınırları ve soruları itibarıyla tanımlanmış ve literatüre sağladığı katkı, blokzincir teknolojisinin benimsenmesine ilişkin Teknoloji Kabul Modeli kullanılarak yapılan araştırmalar açısından değerlendirilmiştir.

Altıncı bölümde, araştırmanın yöntemi açıklanmıştır. Bu kapsamda kullanılan ölçeklere bağlı olarak oluşturulan, araştırma modeline, hipotezlerine, araştırma evrenine, örneklem planına, veri toplama yöntemlerine ve araştırmada kullanılan veri analiz yöntemlerine ilişkin açıklamalara yer verilmiştir.

Yedinci bölümde ise araştırmada uygulanan veri analiz yöntemlerinin sonuçlarına ilişkin bulgular ve ilgili bulgulara dair yorumlar sunulmuştur. Bulgular; katılımcıların demografik bilgileri, katılımcıların teknolojik ürün kullanma sıklıkları, Teknoloji Kabul Modeli'ne yönelik gerçekleştirilen doğrulayıcı faktör, ilişki ve farklılık analizleri ve son olarak Hile Araştırmaları Ölçeği'ne ilişkin meslek mensuplarının hile ile karşılaşma sıklıkları ve hilelerin önlenmesinde blokzincirin rolüne dair görüşlerine yönelik farklılık analizleri itibarıyla sınıflandırılarak açıklanmış ve yorumlanmıştır.

Son olarak sonuç bölümünde, araştırmaya ilişkin sonuçlar özetlenmiş ve önerilerde bulunulmuştur.

## 2. BLOK ZİNCİR TEKNOLOJİSİ

Çalışmanın bu bölümünde, blokzincir teknolojisinin kavramsal çerçevesi ortaya konulmaktadır. Bu kapsamda ilk olarak blokzincir teknolojisi tanımlanarak, gelişim sürecine etki eden çalışmalar ve olaylar itibarıyla tarihsel gelişim süreci incelenmektedir. Ardından teknolojiyi oluşturan teknik unsurlar detaylandırılmakta ve teknolojinin mimarisi ve işleyişi açıklanmaktadır. Akabinde blokzincir teknolojisi, özellikleri ve türleri itibarıyla sınıflandırılmaktadır. Takiben, en çok bilinen dört blokzincir platformu Bitcoin, Ethereum, Ripple ve Hyperledger, karşılaştırmalı olarak tanımlanmakta ve blokzincir teknolojisinin çeşitli kullanım alanlarına örnekler verilmektedir. Son olarak ise blokzincir teknolojisinin genel kullanımına yönelik avantaj ve dezavantajları özetlenmektedir.

### 2.1 BLOKZİNCİR TEKNOLOJİSİNİN TANIMI

Blokzincir kavramı; Satoshi Nakamoto rumuzlu anonim bir kişi veya grup tarafından 2008 yılında yayımlanan “Bitcoin: A Peer-to-Peer Electronic Cash System (Bitcoin: Eşler Arası Elektronik Nakit Sistemi)” isimli makalede ilk kez bahsedilen ilk kripto para Bitcoin (Nakamoto, 2008) ile öne çıktığından yaygın olarak kripto para tanımı yerine kullanılmaktadır. Ancak blokzincir, Bitcoin’in İnternet üzerinden işlem gördüğü platformun dayandığı temel teknolojidir (Swan, 2015, s.1). Dolayısıyla uygulaması vasıtasıyla kendisini gösteren blokzincir teknolojisi aslında çok farklı amaçlarla kullanılabilecek teknolojik bir yeniliktir (Dursun, 2020, s.10).

Literatürde blokzincir kavramına ilişkin ilk çalışma olarak Nakamoto (2008)’nin söz konusu makalesi gösterilmekle birlikte ilgili çalışmada blokzincir (blockchain) terimine rastlanmamaktadır. Diğer yandan elektronik parayı, dijital imzalar zinciri şeklinde tanımlayarak her bir para transfer işleminin (blok) bir imza (düğüm) ile kendinden önceki ve sonraki işleme bağlandığı (zincirlendiği) bir ağ sisteminden bahsedilmektedir (Nakamoto, 2008). Söz konusu ağ sisteminin bu yapısı dolayısıyla da ilgili teknoloji uluslararası yazında çoğunlukla blokzincir terimi ile kabul görmüştür. Her ne kadar terimsel açıdan fikir birliğine varılmış olsa da blokzincir teknolojisinin literatürdeki açıklamalarına baktığımızda standart bir tanıma ulaşamamaktadır. Bunun yanında yazarlar blokzincir teknolojisinin farklı özelliklerine vurgu yaparak sistemi açıklamaya çalışmışlardır. Buna göre aşağıdaki Tablo 2.1’de bazı kaynaklara göre yapılan blokzincir tanımlamaları verilmiştir:

**Tablo 2.1: Blokzincir Tanımları.**

| YAZAR                                                       | TANIM                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Swan (2015)                                                 | Blok zinciri, tüm varlıkların kaydedildiği dev bir elektronik tablo üzerine işlem yapabilecek küresel ölçekteki tüm tarafların sahip olduğu bir muhasebe sistemidir.                                                                                                                                                                                                 |
| Buterin (2015)                                              | Blokzincir, herkesin program yükleyebileceği, programların kendi kendine yürütülebileceği, her programın mevcut ve önceki tüm durumlarının her zaman kamuya açık olacağı ve zincir üzerinde çalışan programların tam olarak blokzinciri protokolünün belirttiği şekilde yürütüleceğine yönelik güçlü bir kripto ekonomik güvence taşıdığı sihirli bir bilgisayardır. |
| Yli-Hummo vd. (2016)                                        | Blokzincir; kendisine katılan düğümler tarafından onaylanan ve sürekli büyüyen bir veri kayıtları listesini tutan, işlemlerin ve verilerin hiçbir üçüncü tarafın kontrolünde olmadığı merkezi olmayan, dağıtılmış bir veri tabanı çözümüdür.                                                                                                                         |
| Peters vd. (2016)                                           | Blokzincir; işlem maliyetlerini azaltmayı, finansal araçlara olan ihtiyacı tamamen ortadan kaldırmayı ve çevrimiçi ödemeler için bir elektronik para biçimi olmayı hedefleyen bitcoin gibi kripto para birimlerinin tanıttığı temel yeniliktir.                                                                                                                      |
| Crosby vd. (2016)                                           | Blokzincir; tüm işlem ve dijital olayların sistemdeki katılımcılar arasında paylaşıldığı, her bir işlemin katılımcıların mutabakatı ile doğrulandığı, kesin ve silinemeyen kayıtların olduğu bir genel defterdir.                                                                                                                                                    |
| Lansiti & Lakhani (2017)                                    | Blokzincir; dijital koda gömülü olan sözleşme verilerinin silinmeye ve değiştirilmeye karşı korunarak şeffaf ve paylaşılan veri tabanlarında saklandığı dağıtık bir defterdir.                                                                                                                                                                                       |
| Zheng Z. vd. (2017)                                         | Blokzinciri teknolojisi; ademi merkeziyetçilik, kalıcılık, anonimlik ve denetlenebilirlik gibi özelliklere sahip olan ve bu özellikleri ile maliyet tasarrufu sağlayarak verimliliği artıran, kullanıcı güvenliği ve defter tutarlılığı için asimetrik kriptografi ve dağıtılmış mutabakat algoritmaları uygulayan halka açık bir defterdir.                         |
| Deloitte & TUSİAD (2018)                                    | Blokzincir; birden fazla tarafın kendi aralarında mutabakata vardıkları, işlemi farklı veri tabanları üzerinde kaydederek değiştirilememesini garanti altına aldıkları bir veri saklama yaklaşımıdır.                                                                                                                                                                |
| Zheng, W. vd. (2019)                                        | Blokzinciri, tamamen kalıcı ve doğrulanabilir verilerin ve işlemlerin herhangi bir üçüncü tarafın kontrolü altında olmadan kaydedildiği bir dağıtılmış defterdir.                                                                                                                                                                                                    |
| Blockchain Türkiye Platformu Teknoloji Çalışma Grubu (2019) | Merkezi olmayan dijital kayıt defteri kavramının özel bir türü olan blokzincir, kayıtların peer-to-peer (P2P) ağ içerisindeki bilgisayarlarda eş kopyalar şeklinde ve eş güdüm ile onaylanıp saklanmasını sağlayarak, bu kayıtların değiştirilemezliklerini garanti altına alan bir teknolojidir.                                                                    |
| BİLGEM UEKAE ENSTİTÜSÜ (2020)                               | Blokzincir teknolojisi, güvenilir işlem yapan küresel bir bilgisayardır. Bilgisayarın en temel bileşenlerinden hafıza kısmı; kayıt defteri olarak adlandırılan zincir şeklinde birbirine kriptografik tekniklerle bağlanan veri kümelerini, işlemci kısmı ise akıllı kontratlar olarak adlandırılan değiştirilemeyen güvenilir bir kod parçasını ifade etmektedir.   |
| TÜBİTAK                                                     | Blokzincir teknolojisi; dijital paraları, varlıkları ve emtiaları besleyen, mutabakatla güncellenen, dağıtılmış bir veri tabanı veya paylaşılmış kayıt (muhasebe) defteridir.                                                                                                                                                                                        |

Literatür taraması neticesinde blokzincir teknolojisinin temelde bilişim, muhasebe ve denetim ve finans olmak üzere üç sektör üzerinden tanımlandığını görmekteyiz. Bu tanımlamaları özetlediğimizde blokzincir; bilişim sektörü açısından, tüm dijital işlemlerin merkezi olmayan ve değiştirilemez bir veri tabanında saklanmasını sağlayan bir şifreleme teknolojisidir. Muhasebe ve denetim sektörü açısından; kaydetme fonksiyonun tüm ağ katılımcıları tarafından gerçekleştirilebildiği, değiştirilemez ve silinemez nitelikteki verilerin herkesin erişimi ile saklandığı ve tüm işlemlerin doğrulanarak denetlenebildiği bir elektronik kayıt defteridir. Ve son olarak finans sektörü açısından ise dijital değişim aracı olarak kullanılan kripto para birimlerinin dayanağı olan teknolojidir.

## **2.2 BLOKZİNCİR TEKNOLOJİSİNİN TARİHSEL SÜRECİ**

### **2.2.1 Blokzincir Teknolojisinin Ortaya Çıkışı**

Blokzincir teknolojisi her ne kadar teknolojik bir yenilik olarak görülse de aslında felsefi bir ideolojiye dayanmaktadır. Bu teknolojinin temelini oluşturan, bilgi güvenliği ve kişisel gizliliğin kriptografik yöntemlerle sağlandığı merkeziyetsiz yapı, “Cypherpunk ” hareketinin felsefesinden doğmuştur.

Cypherpunk hareketi; 1980’lerin sonlarına doğru ortaya çıkan, toplumsal ve politik değişim aracı olarak gizliliği artıran teknolojilerin ve güçlü kriptografinin kullanılması gerekliliği ile kişisel gizlilik ve özgürlüğü savunan aktivist bir hareketi ifade etmektedir (<https://bitcoinwiki.org/wiki/cypherpunk>). Bu felsefi hareketin gelişmesinde ise özellikle birkaç çalışma etkili olmuştur. Bunlar (<https://bilgiplatformu.btcturk.com/bitcoin/cypherpunk-manifesto-nedir/>):

- a. Whitfield Diffie ve Martin Hellman tarafından 1976 yılında yayınlanan “New Directions in Cryptography” (Kriptografide Yeni Yönler) isimli makalede önerdikleri açık anahtarlı kriptografi<sup>1</sup> yöntemi,
- b. David Chaum’un 1985 yılında yayınladığı “Security without Identification: Transaction Systems to Make Big Brother Obsolete (Kimlik Olmadan Güvenlik: Karlı Bilgisayarlarla Büyük Birader’i İşlevsiz Hale Getirmek) adlı makalede önerilen

---

<sup>1</sup> “Asimetrik şifreleme” hakkında detaylı bilgi için bkz. s. 35.

mahremiyeti koruma odaklı güçlü ve güvenilir şifreleme sistemleriyle desteklenen bir işlem yaklaşımı,

- c. David Chaum'un 1989 yılında kör imza teknolojisine dayalı ve kişisel gizliliği koruyarak çevrimiçi ödemelerin izlenememesini sağlayan elektronik ödeme şirketi Digicash'i kurması,
- d. John Gilmore'un 1991 yılında yayınladığı "Privacy, Technology, and the Open Society (Gizlilik, Teknoloji ve Açık Topluluk)" makalesinde önerdiği (1. Bilgisayarlar, Özgürlük ve Gizlilik Konferansında) kanunlar yerine matematik ve fizik ile mahremiyetin sağlandığı bir toplum düşüncesi.

Eylül 1992'de Timothy C. May (Tim May), Eric Hughes ve John Gilmore'un düzenli olarak her ay San Francisco'da Gilmore'un şirketi Cygnus Solutions'da bir araya gelerek çalışmalarını ve fikirlerini paylaştıkları küçük bir grup kurmalarıyla Cypherpunk hareketi başlamıştır. Bu toplantılardan birinde, Jude Milhon'un mizahi olarak "cyberpunk" kelimesinden türeterek "Cypherpunks" olarak adlandırmasıyla kavram benimsenmiştir. Bu toplantılar sırasında; anonimlik, kriptografi, matematik, bilgisayar bilimi gibi konuların felsefesi ve siyaseti üzerine derin tartışmaların yapıldığı "Kriptografi Posta Listesi (The Cryptography Mailing List)"nin de temelleri atılmıştır (<https://bilgiplatformu.btcturk.com/bitcoin/cypherpunk-manifesto-nedir/>). Bir diğer adı "Şifrepunk Posta Listesi (Cypherpunks Mailing List)" olan bu e-posta grubu üyelerinin siyasi ideolojileri (anarko-kapitalist, liberteryen, sosyalist) ise farklılık göstermektedir. Buna rağmen üyelerinin tamamı; bireysel özgürlüğü ve otonomiye destekleyen, mahremiyet odaklı yeni bir ekonomik takas sistemi kurma ve finansal kurumların gücünü sınırlama hedefinde buluşmuşlardır (Yılmaz, 2022, s.412). Diğer yandan bu farklı bakış açılarından, blokzincir teknolojisine dönüşecek etkileşimi sağlayan iki vizyon öne çıkmıştır: Kripto Anarşistler ve Şifrepunklar.

Timothy C. May, hem cypherpunk hareketinin öncüsü (Jarvis, 2022, s.319) hem de kripto anarşistlerin temsilcisidir. 1988 yılında yazdığı "Kripto Anarşist Manifestosu (The Crypto Anarchist Manifesto)"nu, ilk kez Eylül 1992'de cypherpunk hareketinin oluşumunda dile getirmiş ve Kasım 1992'de kriptografi posta listesinde paylaşarak geniş kitlelere ilan etmiştir (<https://eksiseyler.com/tim-mayin-kripto-para-teknolojisini-1988de-gordugu-metin-kripto->

anarsist-manifestosu). May (1988), manifestosunda; açık anahtarlı şifreleme, sıfır bilgi etkileşimli kanıt sistemleri, kimlik doğrulama vb. gibi teknolojilerin gelişimiyle tarafların anonim iletişim kurmasına, alışveriş-iş yapmasına ve elektronik sözleşme imzalamasına olanak sağlayabilecek teorik altyapının oluşturulması dolayısıyla, teknolojinin artık “sosyal ve ekonomik devrim” için gerekli seviyeye ulaştığını ve gelecekteki on yılın getireceği yeterli ek hız ile bu devrimin ekonomik olarak uygulanabilir hale geleceğini, bunun da istense bile durdurulamayacağını öne sürmektedir. “Tıpkı matbaanın icadının orta çağ loncalarının gücünü azaltması ve toplumsal güç yapısını değiştirmesi gibi” (May, 1988), May de kriptografinin, ticaretin ve yönetimin doğasını değiştireceğine inanmaktadır (Jarvis, 2022, s.319). Sonuç olarak kripto anarşistler, özgürlüğün hem bilgi paylaşımında hem de piyasalarda sağlanması gerektiğini ve bunun da ancak kriptografik teknoloji aracılığıyla devlet otoritesi olmayan bir sistem ile gerçekleştirilebileceğini savunmaktadırlar (Yılmaz, 2022, s.412).

Şifrepunkların temsilcisi ise cypherpunks hareketinin kurucularından Eric Hughes’tir. Hughes, Mart 1993’te yayınladığı “Şifrepunk Manifestosu (A Cypherpunk Manifest)”nda; kendilerini, açık bir toplumda gizli olmayan ancak bireylerin isteklerine bağlı olarak kimliklerini ifşa etme gücü olan “mahremiyeti” sağlayacak kriptografiye dayanan sistemlerin, “kod yazarı” olarak tanımlamıştır. Bu manifestoya göre; kurumlar ve devletler, bireylerin bilgilerinden fayda sağlamaktadırlar ancak bilgi paylaşımına ilişkin kontrolün bireyin kendisine ait olması gerekmektedir. Bu mahremiyetin sağlanması ise şifreleme, dijital imzalar, anonim posta iletim sistemleri ve elektronik para teknolojilerini içeren anonim sistemlerle mümkün olabilmektedir. Diğer yandan bu sistemlerin oluşturulması ile kalınmaması ve toplumun geneline yayılarak sosyal sözleşmenin bir parçası haline gelmesi gerekliliğini de savunmaktadırlar (Hughes, 1993).

İki vizyonu birlikte değerlendirdiğimizde ise kripto-anarşistler, devlet otoritesinden bağımsız özgür bir toplum oluşturma hedefinde; şifrepunklar ise birey kimlikleri ve işlem gizliliğini sağlamak için merkeziyetsiz ağlar kurma yolunda benzer bir altyapı üzerinde çalışmışlardır. (Yılmaz, 2022, s.412).

Dolayısıyla kendisini cypherpunks olarak tanımlayan veya tanımlamayan bilgisayar güvenliği uzmanları, akademisyenler ve ilgili profesyoneller kriptografi ve bilgisayar güvenliği alanında bilgi paylaşımında bulunma ve tartışmaları takip etme gerekçesiyle



“<https://www.metzdowd.com>” internet adresi aracılığıyla “The Cryptography Mailing List (Kriptografi Posta Listesi)”e ya da kısaca “Cypherpunks”<sup>a2</sup> abone olmuşlardır. Üye sayıları yıllar itibarıyla giderek artarken etkileşim düzeyleri de artmıştır. Nitekim blokzincir ağının gelişmesine katkı sağlayan teknolojileri geliştiren birçok profesyonelin (Adam Back, Nick Szabo, Hal Finney gibi) cypherpunks olduğu bilinmektedir ve yakın gelecekte ulaşılabilecek teknolojik düzey ile sosyal, ekonomik ve siyasi atmosferi 20 yıl öncesinden öngörmüşler ve buna yönelik harekete geçmişlerdir.

İronik bir şekilde, 2008'deki küresel finansal krizin patlak verdiği dönemde, yatırım bankalarının iflasıyla birlikte ekonomik çalkantılar yaşanırken, başka bir köşede teknolojik bir devrimin tohumları atılmıştır. Tüm bu kriz sürecinin yaşandığı sıralarda 31 Ekim 2008 tarihinde “Bitcoin P2P e-cash paper (Bitcoin P2P e-nakit makalesi)” konulu bir e-mail Satoshi Nakamoto rumuzlu anonim bir adresten The Cryptography Mailing List grubuna gönderilmiştir. Nakamoto bu e-postada “*tamamen eşler arası, güvenilir bir üçüncü tarafın olmadığı yeni bir elektronik para sistemi üzerinde çalıştığını*” ilan etmiş ve Bitcoin White Paper (Teknik Doküman)’ının tam metnine erişilmesi için <https://bitcoin.org/bitcoin.pdf> bağlantısını vermiştir<sup>3</sup>. Böylece “*eşten eşe (peer to peer - P2P) bir ağ ile çift harcamanın önlendiği, güvenilir üçüncü tarafların olmadığı, katılımcıların anonim oldukları, hashcash benzeri iş kanıtı ile yeni coinlerin üretilebildiği bir e-nakit ödeme sistemi*” olan Bitcoin (Nakamoto, 2008b) ve altında yatan blokzincir teknolojisi ilk kez teorik olarak ortaya konmuştur.

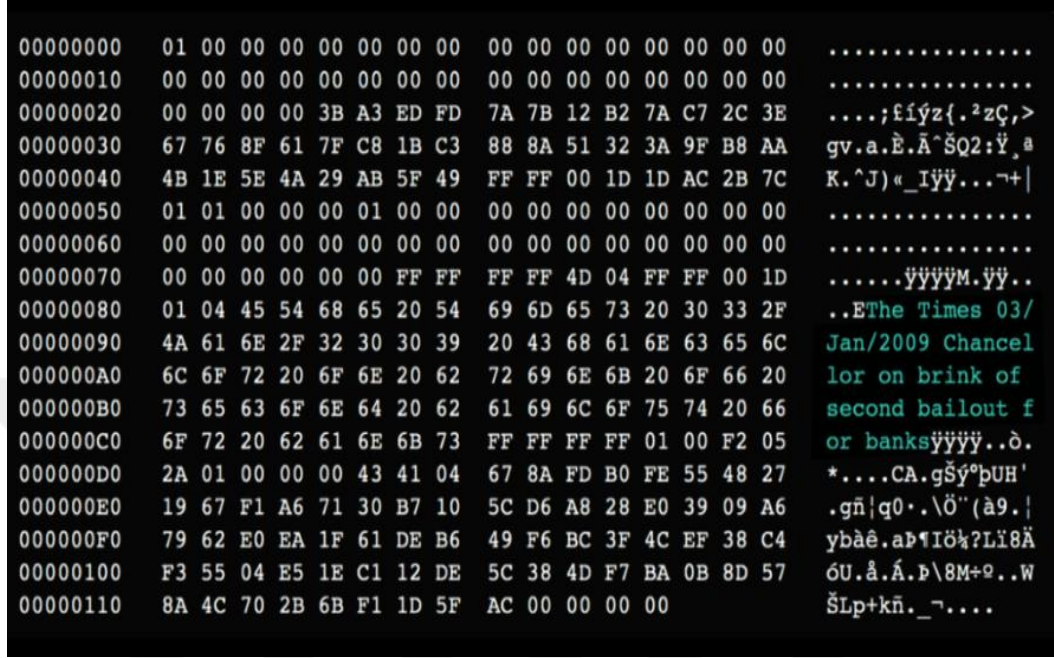
Ardından 2 ay gibi bir süre sonrasında 3 Ocak 2009 tarihinde Nakamoto, Bitcoin ağı üzerinde blok madenciliğini başlatmış ve harcanamaz 50 BTC ödüllü ilk bitcoin bloğu Genesis’i oluşturmuştur (Şekil 2.1). Diğer yandan; blok içindeki veri satırları arasına, sebebini hiç açıklamadığı bir mesaj yazmıştır: “*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks (Şansölye bankalar için ikinci kurtarma paketinin eşiğinde).*” Bu mesaj 3 Ocak 2009 tarihindeki The Times Gazetesi’nin manşetidir. 3 Ocak tarihi, bitcoinin doğuş günü kabul edilmekte ve her yıl “Genesis Blok Günü” olarak harcanamaz

---

<sup>2</sup> Cypherpunks terimi, geniş anlamda bilgisayar güvenliği ve bireysel özgürlükleri savunan aktivistleri tanımladığı kadar Kriptografi Posta Listesi üyeleri ifadesini kısaca söylemek için de kullanılmaktadır.

<sup>3</sup> Söz konusu e-postaya ulaşmak için bkz. <https://satoshi.nakamotoinstitute.org/emails/cryptography/1/>.

50 BTC'nin bulunduğu "1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa" Genesis adresine<sup>4</sup> bitcoin gönderilmektedir (<https://bilgiplatformu.btcturk.com/blokzinciri/genesis-block-nedir/>).



Şekil 2.1: Bitcoin Genesis Bloğu.

[<https://digicentralized.com/genesis-block-nedir/>]

11 Ocak 2009'da Hal Finney Twitter'da "Running Bitcoin (Bitcoin çalıştırmak)" ifadesi içeren bir gönderi paylaşmıştır, bu gönderi bitcoin hakkında atılan ilk tweet olmuştur.

Ve hemen ertesi gün 12 Ocak 2009 tarihinde Nakamoto, blokzincirinin 170 no.lu bloğunda ilk bitcoin test transferini gerçekleştirerek cüzdanındaki 50 BTC'nin, 10 BTC'sini Finney'e göndermiş kalan 40 BTC'yi ise başka bir hesaba devretmiştir (Şekil.2.2) (<https://bilgiplatformu.btcturk.com/bitcoin/ilk-bitcoin-transferi/>). Bu transfer, Bitcoin'in gerçek kullanımını ve işlem yapılabilirliğini gösteren ilk örnek olmuştur.

<sup>4</sup> Genesis adresine erişim için bkznz.

<https://www.blockchain.com/explorer/addresses/btc/1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa>.



Şekil 2.2: İlk Bitcoin Transferi.

[<https://bilgiplatformu.btcturk.com/bitcoin/ilk-bitcoin-transferi/>]

Bu gelişmenin 1 ay üzerine Nakamoto, 11 Şubat 2009 tarihinde P2P Foundation (Eşler Arası Vakfı)'da, P2P para birimi Bitcoin'in açık kaynaklı uygulamasının gerçekten çalıştığına dair ilk duyuruyu yapmış ve Bitcoin v0.1'i "http://www.bitcoin.org" internet adresi üzerinden kullanıma sunmuştur (Nakamoto, 2009).

Nakamoto (2009), bu duyuruyu yaparken ise şu ifadelere yer vermiş:

*"Geleneksel para biriminin temel sorunu, sistemin işlemesi için gereken "güven" unsurudur. Merkez bankasına, paranın değerini düşürmeyeceği konusunda güvenilmelidir, ancak itibari para birimlerinin tarihi bu güvenin ihlal edilmesiyle doludur. Bankalara, paramızı tutacakları ve elektronik olarak transfer edecekleri konusunda güvenilmelidir, ancak onlar paranın çok az bir kısmını rezervlerinde tutmakta, kalanı ise kredi balonu dalgaları halinde ödünç vermektedirler. Gizliliğimiz konusunda da onlara güvenmeliyiz, kimlik hırsızlarının hesaplarımızı boşaltmasını engelleyecekleri hususunda da onlara güvenmeliyiz."*

ve sistemi yaratma gerekçesini, enflasyon ve merkez bankalarının aşırılık eğilimlerine dayandırmıştır (Golumbia, 2016, s.21).

Sonuç olarak blokzincir teknolojisinin temel özelliklerinden gizlilik, anonimlik ve merkeziyetsizlik unsurlarının sağlanmasına yönelik çok sayıda akademik ve pratik teknolojik gelişme yaşanmıştır. Bu gelişmelerin arasında, Nakamoto'nun teknik dokümanda atıfta bulunduğu ve blokzincir teknolojisiyle doğrudan ilişkili olanlar: (i) Ralph Merkle'nin hash ağaçları (1979), (ii) David Chaum'un kör imzaları (1982), (iii) Adam Back'in hashcash

proof of work sistemi (1997), (iv) Wei Dai'nin b-money şeması (1998), (v) Nick Szabo'nun bitgold konsepti (1999) ve (vi) Hal Finney'in yeniden kullanılabilir proof of work sistemi (2004)'dir (Dupont, 2014, s.9). Söz konusu gelişmeler, bu çalışmada kavramlar üzerinden detaylı bir şekilde ele alınacak olup temel bir çerçeve olması adına blokzincir teknolojisinin ortaya çıkışına etki eden internet ve kriptografi üzerine çeşitli çalışmalar ve gelişmeler kronolojik olarak Tablo 2.2'de özetlenmiştir.

**Tablo 2.2:** Blokzincir Teknolojisini Şekillendiren Teknolojik İlerlemeler.

| Yıl  | Yazar                                    | Çalışmanın/Konunun Orijinal Başlığı                                    | Çalışma/Gelişme İçeriği                                                                                            | Sayfa No <sup>5</sup> |
|------|------------------------------------------|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|-----------------------|
| 1961 | Leonard Kleinrock                        | Information Flow in Large Communication Networks                       | Paket anahtarlama teorisi geliştirildi.                                                                            | -                     |
| 1964 | Paul Baran                               | On Distributed Communication                                           | Dağıtık iletişim ağlarının kullanımı ve bu ağların nasıl oluşturulabileceği tanımlandı.                            | 30                    |
| 1969 | ABD Savunma Bakanlığı                    | Distributed Communication Network: ARPAnet                             | İlk ARPAnet (Advanced Research Projects Agency Network) düğümleri kuruldu ve paket anahtarlama ağına temel atıldı. | -                     |
| 1972 | ABD Savunma Bakanlığı                    | Electronic Mail (E-mail)                                               | İlk e-posta haberleşmesi ARPAnet'te kullanıldı.                                                                    | -                     |
| 1974 | Robert Khan                              | Protocol for Inter-Network Packet Communication                        | TCP/IP standart ağ protokolü tasarlandı.                                                                           | -                     |
| 1974 | Vinton Cerf & Robert Khan                | Packet Radio Network Access Protocol                                   | TCP/IP standardı geliştirildi ve internetin gelişimine katkı sağladı.                                              | -                     |
| 1976 | Whitfield Diffie & Martin Hellman        | New Directions in Cryptography                                         | Açık anahtarlı kripto sistem kavramı geliştirildi.                                                                 | 35                    |
| 1978 | Ron Rivest, Adi Shamir & Leonard Adleman | A Method for Obtaining Digital Signatures and Public-Key Cryptosystems | Kriptografik şifreleme yöntemi RSA geliştirildi.                                                                   | -                     |
| 1979 | Ralph C. Merkle                          | Method for Digital Signature Authentication                            | Merkle ağacı kavramının patenti alındı.                                                                            | 25                    |
| 1982 | David Chaum                              | Blind Signatures for Untraceable Payments                              | Merkezi yapıya dayalı, dijital imzalı, takip edilemeyen elektronik para (e-cash) kavramı geliştirildi              | 57                    |
| 1983 | ABD Savunma Bakanlığı                    | Communication Control Protocol                                         | TCP/IP (IPv4) internet protokolü ARPAnet'te kullanılmaya başlandı.                                                 | -                     |

<sup>5</sup> Tablo 2.2'deki "Sayfa No" başlığında belirtilen numaralar, ilgili konuların bu çalışma içerisindeki detaylarına ulaşılacak sayfa numaralarıdır.

**Tablo 2.2:** Blokzincir Teknolojisini Şekillendiren Teknolojik İlerlemeler (Devam).

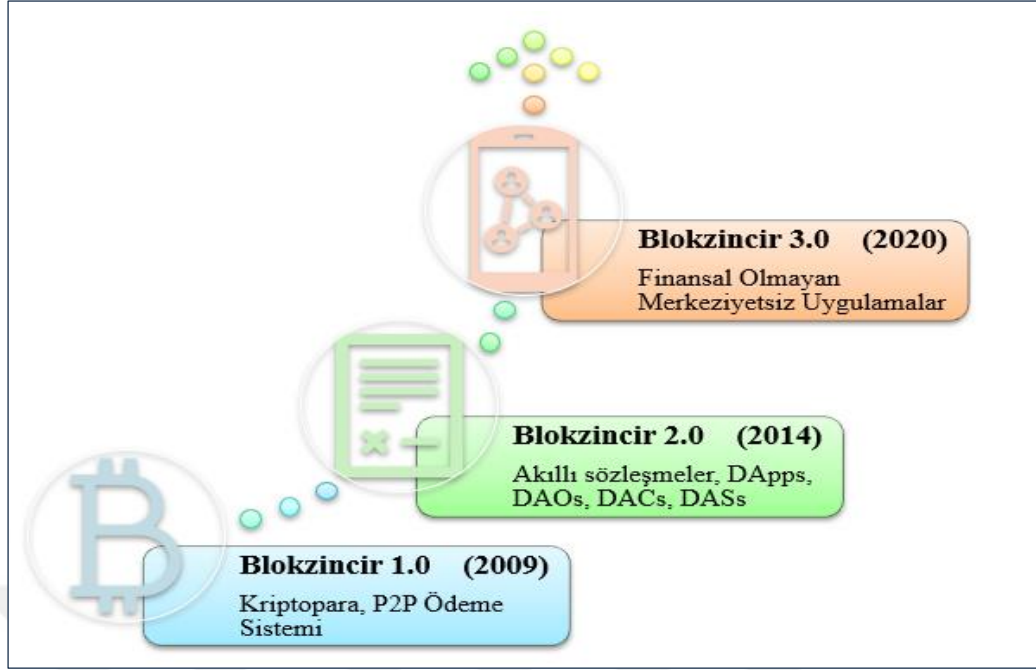
| Yıl  | Yazar                                        | Çalışmanın/Konunun Orijinal Başlığı                                           | Çalışma/Gelişme İçeriği                                                                                                                                                                                     | Sayfa No |
|------|----------------------------------------------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| 1985 | David Chaum                                  | Security Without Identification: Making Big Brother Obsolete with Smart Cards | Akıllı kart teknolojisi ile kimlik tespiti olmadan güvenliğin ve gizliliğin sağlanması önerisi getirildi.                                                                                                   | -        |
| 1985 | Neal Koblitz                                 | Elliptic Curve Cryptosystems                                                  | Elipitik eğri kriptografi teorisi geliştirildi.                                                                                                                                                             | -        |
| 1987 | Ralph C. Merkle                              | Digital Signature Based on Traditional Encryption Function                    | Merkle ağacı kavramının çalışma prensibini resmi olarak tanımladı.                                                                                                                                          | 25       |
| 1989 | Tim Berners-Lee                              | World Wide Web (www)                                                          | İlk web tarayıcısı World Wide Web (www) geliştirildi ve modern internetin temelleri atıldı.                                                                                                                 | -        |
| 1989 | David Chaum                                  | Digicash                                                                      | Dijital imza teknolojisine dayalı ve çevrimiçi ödemelerin izlenememesini sağlayan elektronik ödeme şirketi Digicash kuruldu.                                                                                | 57       |
| 1989 | The World                                    | Commercial Internet Service Provider (ISP)                                    | İlk ticari hizmet sağlayan, İnternet Servis Sağlayıcısı (ISS) The World faaliyete geçti.                                                                                                                    | -        |
| 1991 | Tim Berners-Lee                              | World Wide Web (www)                                                          | World Wide Web (www) kullanıcılara açıldı.                                                                                                                                                                  | -        |
| 1991 | NSFnet                                       | Commercial Internet                                                           | NSFnet (National Science Foundation Network), ticari internet kullanımını serbest bıraktı ve internet yaygınlaşmaya başladı.                                                                                | -        |
| 1991 | Stuart Haber & W. Scott Stornetta            | How to Timestamp a Digital Document                                           | Dijital belgelerin bütünlüğünü ve doğruluğunu sağlamak için her belgenin oluşturulan hash değerine zaman damgası eklenmesi ve bu belgelerin birbirine kronolojik olarak bağlandığı bir sistem geliştirildi. | 26       |
| 1991 | Phil Zimmermann                              | Pretty Good Privacy (PGP)                                                     | Veri iletişimde gizlilik ve kullanıcı kimlik doğrulaması sağlayan açık anahtarlı şifreleme ve dijital imzala yazılımı PGP geliştirildi.                                                                     | -        |
| 1991 | John Gilmore                                 | Privacy, Technology, and Open Society                                         | Kanunlar yerine matematik ve fizik ile mahremiyetin sağlandığı toplum önerisi getirildi.                                                                                                                    | -        |
| 1992 | Timothy C. (Tim) May                         | Crypto Anarchist Manifesto                                                    | Kripto Anarşist Manifestosu yayınlandı.                                                                                                                                                                     | 8        |
| 1993 | Eric Hughes                                  | Cyberpunk Manifesto                                                           | Cyberpunk Manifestosu yayınlandı.                                                                                                                                                                           | 9        |
| 1993 | Cynthia Dwork & Moni Noar                    | Pricing via Processing, or Combatting Junk Mail                               | Spam e-postaları önlemek için iş kanıtı üretme fikri geliştirildi.                                                                                                                                          | 43       |
| 1996 | Ross J. Anderson                             | Eternity Service                                                              | Uzun süreli saklanabilen dağıtık veri depolama sistemi kavramından söz edildi.                                                                                                                              | -        |
| 1996 | Douglas Jackson, Barry Downey & Reid Jackson | E-gold                                                                        | Altın rezervlerine dayanan dijital para e-gold kuruldu.                                                                                                                                                     | -        |

**Tablo 2.2:** Blokzincir Teknolojisini Şekillendiren Teknolojik İlerlemeler (Devam).

| Yıl  | Yazar                            | Çalışmanın/Konunun Orijinal Başlığı                                   | Çalışma/Gelişme İçeriği                                                                                                                        | Sayfa No |
|------|----------------------------------|-----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| 1997 | Adam Back                        | Hashcash                                                              | Spam e-postaları ve DoS saldırılarını önlemek için hash bulmacası çözerek iş kanıtı üretilmesi sonucu token dağıtılan bir protokol tanımlandı. | 44       |
| 1998 | Wei Dai                          | B-money                                                               | Merkeziyetsiz elektronik ödeme sistemi b-money tanıtıldı.                                                                                      | 60       |
| 1999 | Markus Jakobsson & Ari Juels     | Proofs of Work and Bread Pudding Protocols                            | Dwork & Noar'ın iş kanıtı protokolü resmi olarak tanımlandı.                                                                                   | 43       |
| 2001 | ABD Ulusal Güvenlik Ajansı (NSA) | SHA-256 Function                                                      | SHA ailesinde daha güçlü bir kriptografik hash fonksiyonu geliştirildi.                                                                        | 39       |
| 2001 | MIT                              | Chord: Scalable Peer-to-Peer Lookup Service for Internet Applications | Dağıtılmış hash tablosu sistemi Chord geliştirildi.                                                                                            | -        |
| 2001 | Bram Cohen                       | Bittorent                                                             | P2P dosya paylaşım yazılımı BitTorrent geliştirildi.                                                                                           | -        |
| 2004 | Harold Thomas (Hal) Finney       | Reusable Proofs of Work and Storage Obligations                       | Yeniden Kullanılabilir İş Kanıtı (RPoW) mutabakat algoritması geliştirildi.                                                                    | -        |
| 2005 | Nick Szabo                       | Bitgold                                                               | Merkeziyetsiz enflasyondan arınmış sanal para geliştirildi.                                                                                    | 60       |
| 2008 | Satoshi Nakamoto                 | Bitcoin: Peer-to-Peer Electronic Payment System                       | Bitcoin teknik dökümanı yayınlandı.                                                                                                            | -        |

## 2.2.2 Blokzincir Teknolojisinin Gelişimi

Blokzincir teknolojisi, Bitcoin sanal para ve ödeme sisteminin geliştirilmesiyle ortaya çıkmış ve 2008 yılından itibaren farklı evrelerden geçerek sürekli olarak gelişmiştir. Bu evrim süreci literatürde, Şekil 2.3'te de gösterildiği üzere üç kategoriye ayrılmakta ve bölüm alt başlıklarında detaylı bir şekilde ele alınmaktadır.



Şekil 2.3: Blokzincir Teknolojisinin Evreleri.

#### 2.2.2.1 Blokzincir 1.0

Birinci nesil blokzincir, “kripto para birimi” evresi olarak adlandırılmakta ve P2P ödeme sistemlerinin kullanılarak para transferleri ile ödemelerin gerçekleştirildiği, kripto para birimi ticaretinin yapılmaya başlandığı, bitcoinin dolayısıyla kripto paraların iskeleti olarak öne çıktığı evredir. Bu süreçte, ilk İnternet para birimi uygulaması bitcoinin tanıtılmasının yanı sıra blokzincir teknolojisine dayanan alternatif kripto paralar (Namecoin, Litecoin, Peercoin gibi) da ortaya çıkmıştır. Diğer yandan bazı ülkelerin (Birleşik Krallık) para birimi olarak tanıdığı; bazılarının (Avrupa Bankacılık Otoritesi, İsviçre, Polonya, Kanada ve Amerika Birleşik Devletleri gibi) mevcut yapılarına uydurmaya çalıştığı, bazılarının (Bangladeş, Ekvador, İzlanda gibi) ise, yasadışı faaliyetlerle ilişkilendirilerek engellediği ancak her şeye rağmen kripto paralara ilginin giderek arttığı bir süreçtir (Swan, 2015, s.7).

Bu yeni teknolojinin ilk gelişme evresi olan 2009-2014 arası dönemde blokzincir teknolojisi ile ilgili ilk kez yaşanan bazı önemli gelişmeler Tablo 2.3’te özetlenmiştir.



**Tablo 2.3:** Blokzincir Teknolojisinde 2009-2014 Yılları Arasında Yaşanan Gelişmeler.

| Yıl           | Gelişme İçeriği                                                                                                                                                                                |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5 Ekim 2009   | İlk bitcoin kuru, New Liberty Standart isimli borsada 1 \$ = 1.309,03 BTC'den işlem gördü.                                                                                                     |
| 22 Mayıs 2010 | İlk gerçek bitcoin alışverişi, Bitcoin geliştiricisi Laszlo Hanyecz tarafından pizza karşılığı 10.000 BTC ödemesi ile gerçekleşti. Bu gün, "Bitcoin Pizza Günü" olarak her yıl kutlanmaktadır. |
| Temmuz 2010   | İlk bitcoin borsası, Mt. Gox faaliyete geçti.                                                                                                                                                  |
| Ağustos 2010  | Bitcoin'in toplam piyasa değeri 1 milyon USD'yi geçti. (1 BTC = 0,5 USD)                                                                                                                       |
| Ekim 2010     | İlk Bitcoin ticaret platformu TradeHill ve Bitcoin Market, bitcoin fiyat belirleme sorunlarına çözüm olarak kuruldu.                                                                           |
| 6 Şubat 2011  | Bitcoin ile anonim alışverişler yapılabilmesini sağlayan ilk darknet pazarı Silk Road açıldı.                                                                                                  |
| 9 Şubat 2011  | İlk bitcoin kur eşitlemesi gerçekleşti. (1 BTC = 1 ABD USD)                                                                                                                                    |
| Nisan 2011    | Bitcoin'den sonraki ve DNS üzerinde merkezi olmayan alan adı kayıtları yapılmasını sağlayan ilk kripto para, Namecoin (NMC) ortaya çıkmıştır.                                                  |
| 26 Nisan 2011 | Satoshi Nakamoto'nun son iletişim tarihidir. Bu tarihten sonra ortadan kayboldu.                                                                                                               |
| Haziran 2011  | Wikileaks, ABD hükümeti tarafından finansal yaptırımlarla karşı karşıya kaldığı için Bitcoin ile bağış kabul etmeye başladı.                                                                   |
| Ağustos 2011  | Bitcoin fiyatı ilk kez 10 USD'yi geçti ve ardından kısa sürede 31 USD'yi aştı.                                                                                                                 |
| Ekim 2011     | Scrypt madencilik algoritmasını kullanan altcoin, Litecoin (LTC) ortaya çıkmıştır.                                                                                                             |
| Aralık 2011   | Bitcoin fiyatı 2 USD'ye kadar düştü, bu dönemde önemli fiyat dalgalanmaları yaşandı.                                                                                                           |
| Mayıs 2012    | İlk kripto para birimlerine yönelik dergi, Bitcoin Magazine yayınlandı. Çevrimiçi ücretsiz olan dergi, 9 \$'dan satışa sunuldu.                                                                |
| Mayıs 2012    | İlk Bitcoin konferansı, Bitcoin 2012 Conference, Prag'da düzenlendi.                                                                                                                           |
| Ağustos 2012  | Enerji ve sürdürülebilirlik odaklı Peercoin (PPC) altcoini ortaya çıktı.                                                                                                                       |
| Eylül 2012    | Altcoin Ripple (XRP), bankalararası transferi hızlandırmak amacıyla ortaya çıktı.                                                                                                              |
| Kasım 2012    | Bitcoin Foundation kuruldu; Bitcoin'in geliştirilmesini, standardizasyonunu ve yaygınlaştırılmasını amaçladı.                                                                                  |
| 28 Kasım 2012 | İlk bitcoin ödül yarılması gerçekleşerek 50 BTC'den 25 BTC'ye düşürüldü.                                                                                                                       |
| Mart 2013     | Bitcoin'in toplam piyasa değeri 1 milyar USD'yi geçti.                                                                                                                                         |
| Nisan 2013    | Kıbrıs banka krizi bitcoine ilgiyi artırdı.                                                                                                                                                    |
| Nisan 2013    | Bitcoin fiyatı, ilk kez 100 USD'yi geçti.                                                                                                                                                      |
| Haziran 2013  | Çin'de Bitcoin'e olan ilgi arttı, Çin borsaları (BTCC, Huobi, OKCoin) kuruldu.                                                                                                                 |
| Ekim 2013     | Silk Road kapatıldı. Bu durum Bitcoin'in yasa dışı faaliyetlerde kullanımı konusundaki endişeleri artırdı.                                                                                     |
| Ekim 2013     | İlk Bitcoin ATM'si, Kanada -Vancouver'daki Waves adlı kafede halka açılmıştır.                                                                                                                 |
| Kasım 2013    | Bitcoin fiyatı, 1.000 USD'yi aşarak tarihi zirvesini gördü.                                                                                                                                    |
| Aralık 2013   | Çin Merkez Bankası, bitcoin ile işlem yapılmasını yasakladı. Bu gelişmenin ardından bitcoin fiyatı düşüşe geçti.                                                                               |



### 2.2.2.2 Blokzincir 2.0

İkinci nesil blokzincir, “akıllı sözleşme” evresi olarak adlandırılmaktadır. Bu evre; blokzincir teknolojisini kullanarak merkeziyetsiz para transferi yapmanın ötesinde, akıllı sözleşmeler ile diğer varlık türlerinin (mülkiyet hakları, patentler, dijital varlıklar, hisse senetleri, tahviller, vadeli işlemler, krediler gibi) transferini mümkün kılan bir değer biriminin yaratıldığı, böylece piyasaların merkeziyetsizleştirilerek, geleneksel aracılardan işlevsizleştirildiği bir süreci ifade etmektedir (Swan, 2015, s.9).

Aslında Nakamoto, bitcoin tasarımı yaparken tüm bu süreçleri destekleyecek şekilde tasarımı yapmıştır (Swan, 2015, s.9). Ancak TCP/IP internet protokolünün gelişim evresine benzer bir şekilde (Lansiti vd., 2017, s.5), blokzincir 1.0’ın verimsizliği ve ağır ölçeklenebilirlik konusundaki yetersizliği yeni bir versiyonunun geliştirilmesi ihtiyacını doğurmuştur (Guleria vd., 2022, s.786). Bu süreç, Kasım 2013’te bitcoin geliştiricilerinden Vitalik Buterin’in akıllı sözleşme<sup>6</sup> yazılımını destekleyen Ethereum blokzincirinin White Paper’ını yayınlaması ile başlamış ve 2015 yılında Ethereum blokzincirinin kullanıma açılmasıyla, Merkeziyetsiz Uygulamaların (DApps), Merkeziyetsiz Otonom Organizasyonların (DAO), Merkeziyetsiz Otonom Şirketlerin (DAC) ve Merkeziyetsiz Otonom Toplulukların (DAS) oluşturulmasına olanak sağlayarak blokzincir teknolojisinin “küresel bir bilgi işlem sistemi” (Cheng vd; 2018, s.1047; Çaşkurlu vd., 2021, s.103) haline gelmesinin yolunu açmıştır.

Bu süre zarfında küresel teknoloji devleri blokzincir teknolojisine dikkatleri çekmeye çalışmışlardır. Ayrıca ilk gelişme evresinde başlayan kripto para start up’larının başarıya ulaşması, yatırımcıların verdikleri desteklerini artırmalarını ve bu durum da devletin blokzincir teknolojisine ilgisinin yoğunlaşmasını sağlamıştır. Dolayısıyla yasa koyucular uyumluluk sürecine aktif katılımında bulunarak hem teknolojiye ilgilinin hem de yatırımın daha da artmasının önünü açmıştır (Peters vd., 2015, s.141). Diğer yandan bu dönemde hem Bitcoin hem de Ethereum blokzincirlerinde ilk kez gerçekleşen sert çatallanmalar<sup>7</sup> ve çeşitli hack saldırıları dolayısıyla sistemin güvenilirliği de sorgulanmıştır.

---

<sup>6</sup> “Akıllı sözleşmeler” hakkında detaylı bilgi için bkz. s.78.

<sup>7</sup> “Çatallanma” hakkında detaylı bilgi için bkz. s.50.

Bu kapsamda 2014-2020 arası dönemde Bitcoin ve Ethereum blokzincirleri ile ilgili yaşanan bazı önemli gelişmeler Tablo 2.4'te özetlenmiştir.

**Tablo 2.4:** Blokzincir Teknolojisinde 2014-2020 Yılları Arasında Yaşanan Gelişmeler.

| Yıl                          | Gelişme İçeriği                                                                                                               |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Kasım 2013</b>            | Vitalik Buterin, Ethereum White Paper'ını yayınladı.                                                                          |
| <b>23 Ocak 2014</b>          | Vitalik Buterin, North American Bitcoin Konferansı'nda Ethereum blokzincirini tanıttı.                                        |
| <b>Şubat 2014</b>            | Mt. Gox borsası iflas etti ve bitcoin fiyatlarında düşüş yaşandı.                                                             |
| <b>Nisan 2014</b>            | Ethereum Foundation faaliyete geçti.                                                                                          |
| <b>Temmuz - Ağustos 2014</b> | Ethereum'un geliştirilmesi için ihtiyaç duyulan maddi kaynak, kitle fonlaması finansman yöntemiyle çevrimiçi olarak toplandı. |
| <b>Ağustos 2014</b>          | Bitcoin blokzincirinin blok büyüklüğü 20 GB'a ulaştı.                                                                         |
| <b>Eylül 2014</b>            | BitLicense düzenleme önerisi New York Eyaleti tarafından duyuruldu.                                                           |
| <b>Aralık 2014</b>           | Microsoft, Bitcoin'i ödeme yöntemi olarak kabul ettiğini duyurdu.                                                             |
| <b>Mart 2015</b>             | İkinci Silk Road operasyonu gerçekleştirildi.                                                                                 |
| <b>Nisan 2015</b>            | Bitcoin blokzincirinin blok büyüklüğü 30 GB'a ulaştı.                                                                         |
| <b>Haziran 2015</b>          | Yunanistan krizi, bitcoin talebini artırdı.                                                                                   |
| <b>Temmuz 2015</b>           | Ethereum'un ilk deneysel ağı Olympic başlatıldı.                                                                              |
| <b>30 Temmuz 2015</b>        | Ethereum ağı canlı hale geldi ve ilk sürümü Frontier yayınlandı.                                                              |
| <b>30 Temmuz 2015</b>        | 11,9 milyon sanal para karşılığı ön madencilik ile blokzincir faaliyete geçmiştir.                                            |
| <b>7 Ağustos 2015</b>        | İlk ether kuru, 1 BTC = 2,77 USD'den işlem gördü.                                                                             |
| <b>Ocak 2016</b>             | Ethereum blokzincirinde saniyede 25 işlem yapılabilir hale gelmiştir.                                                         |
| <b>Mart 2016</b>             | Bitcoin blokzincirinin blok büyüklüğü 50 GB'a ulaştı.                                                                         |
| <b>14 Mart 2016</b>          | Ethereum blokzincirinin ikinci sürümü Homestead yayınlandı.                                                                   |
| <b>17 Haziran 2016</b>       | DAO hack saldırısı sonrası, DAO çatalı gerçekleşti. Ethereum'a güven azaldı.                                                  |
| <b>9 Temmuz 2016</b>         | İkinci bitcoin ödül yarılması gerçekleşerek 25 BTC'den 12.5 BTC'ye düşürüldü.                                                 |
| <b>20 Temmuz 2016</b>        | Orijinal Ethereum ağında sert çattanma gerçekleşmesi ile Ethereum Classic ağı faaliyete geçti.                                |
| <b>Ağustos 2016</b>          | Bitfinex borsası, hack saldırısına uğradı.                                                                                    |
| <b>Eylül 2016</b>            | Büyük dijital para birimi borsaları DAO token'ını listeden çıkardı.                                                           |
| <b>Ekim 2016</b>             | Çin hükümeti, bitcoin borsalarına yönelik regülasyonlar getirdi.                                                              |
| <b>19 Aralık 2016</b>        | Ethereum işlem hacmi günde 1 milyonu aştı.                                                                                    |
| <b>Nisan 2017</b>            | Japonya, Ödeme Hizmetleri Yasası ile bitcoin'i ilk yasalaştıran ülke oldu.                                                    |

**Tablo 2.4:** Blokzincir Teknolojisinde 2014-2020 Yılları Arasında Yaşanan Gelişmeler (Devam).

| Yıl             | Gelişme İçeriği                                                                                                                                        |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 Ağustos 2017  | SegWit güncellemesi aktive edildi.                                                                                                                     |
| 16 Ekim 2017    | Metropolis hard fork'unun ilk aşaması olarak Ethereum'un ilk büyük güncellemesi Byzantium gerçekleşti.                                                 |
| Kasım 2017      | Bitcoin fiyatı 10.000 \$'ı aştı.                                                                                                                       |
| Aralık 2017     | Ethereum blokzinciri üzerinde çalışan ilk merkeziyetsiz finans uygulaması (Defi) MakerDAO hayata geçirildi. Dai stabil kripto parası piyasaya sürüldü. |
| Ocak 2018       | Ethereum fiyatı 1.000 \$'ı geçti.                                                                                                                      |
| Mayıs 2018      | SEC, Ripple Labs blokzincir şirketine menkul kıymet satışı ile ilgili dava açtı.                                                                       |
| Temmuz 2018     | Amerika Menkul Kıymetler Borsası SEC, bitcoin ETF başvurularını reddetti.                                                                              |
| 15 Aralık 2018  | Bitcoin Cash, sert çatallanma ile Bitcoin SV ve Bitcoin ABC olarak bölündü.                                                                            |
| 28 Şubat 2019   | Metropolis sert çatallının ikinci aşaması Constantinople gerçekleşti.                                                                                  |
| 22 Haziran 2020 | Facebook, Libra adında kendi kripto para birimini duyurdu.                                                                                             |
| Temmuz 2020     | Twitter hesapları hacklendi ve bitcoin dolandırıcılığı yapıldı.                                                                                        |
| 16 Aralık 2020  | Bitcoin fiyatı 20.000 \$'ı aşarak en yüksek seviyesine ulaştı.                                                                                         |

### 2.2.2.3 Blokzincir 3.0

Üçüncü nesil blokzincir ise, “dijital toplum” evresi olarak adlandırılmaktadır ve sadece para, ekonomi ve piyasaların merkeziyetsizleştirilmesi ile sınırlı kalmayıp tüm endüstrilerin dolayısıyla toplumun merkeziyetsizleştirilmesini hedeflemektedir. Bu süreç; yönetim, sağlık, bilim, kültür, sanat, eğitim, iletişim, ulaşım, denetim gibi finansal olmayan birçok alanı kapsayan, blokzincir teknolojisine dayalı merkezi olmayan uygulamaların hayata geçirildiği ve bu teknolojinin toplum geneline yayıldığı bir dönemi ifade etmektedir. Dijital kimlik, tedarik zinciri, merkezi olmayan borsa, merkezi olmayan finans (Defi), oy verme ve seçim, gayrimenkul, sağlık kayıtları, sigorta ve tazminat, enerji yönetim sistemleri gibi uygulama örnekleri bu gelişmenin ürünleridir.

Diğer yandan yüksek enerji tüketimi, ölçeklenebilirlik zorlukları ve farklı blokzincir ağları arasındaki uyumsuzluk gibi önceki nesil blokzincirlerinin kısıtlamalarını aşarak sürdürülebilirlik ve uyumluluk sağlama hedefi taşımaktadır. Bu doğrultuda farklı mutabakat yöntemleri ve merkeziyetsiz sistemler geliştirilmektedir.

Gelişim süreci halen devam etmekte olan blokzincir 3.0, blokzincir teknolojisine dayanan büyük veri, nesnelerin/endüstriyel nesnelerin interneti (IoT/IIoT), yapay zekâ (AI) gibi Endüstri 4.0 bileşenleri ve Web 3.0 teknolojilerinin birleşimiyle akıllı toplum yaratılmasına yönelik çözümler vadetmektedir. Bu vaatler de birçok endüstrinin blokzincir teknolojisini benimseyerek büyük yatırımlarda bulunmasını ve yeni iş modellerinin geliştirilmesini sağlayacaktır (Çetin vd., 2019, s.141).

Ayrıca bazı devletler, başlangıçta temkinli davrandıkları, sonrasında uyumlaştırma çabalarında bulundukları blokzincir teknolojisini, bu son evrim ile birlikte ekonomik sistem içine dahil ederek vergi ve bazı kamu gelirlerini tahsil etme ve kontrol etme aracı olarak kullanacağı; hatta %10'luk bir nüfusun ekonomik yaşantısını bu teknolojiye dayandırmasının bile mümkün olacağı bir aşamaya gelmek üzeredir (Çetin vd., 2019, s.141). Diğer yandan bazı ülkeler için tam tersinin söz konusu olduğu bir dönüşüm sürecini da yansıtabilir.

Bu süreci daha iyi anlamak adına, 2020 sonrası dönemde blokzincir teknolojisi ile ilgili yaşanan bazı önemli gelişmeler Tablo 2.5'te özetlenmiştir.

**Tablo 2.5:** Blokzincir Teknolojisinde 2020 Sonrası Yaşanan Gelişmeler.

| Yıl                   | Gelişme İçeriği                                                                                                                           |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Nisan 2020</b>     | Japonya, kripto para birimlerini yasal ödeme aracı olarak tanıdı.                                                                         |
| <b>11 Mayıs 2020</b>  | Üçüncü bitcoin ödül yarılması gerçekleşerek 12.5 BTC'den 6.25 BTC'ye düşürüldü.                                                           |
| <b>Eylül 2020</b>     | Çin'in dijital para birimi, dijital yuanın (e-CNY) çalışmalarına başlandı.                                                                |
| <b>Ekim 2020</b>      | PayPal, ABD'deki kullanıcılarına kripto para alım-satım hizmeti sunmaya başladı.                                                          |
| <b>Mart 2021</b>      | NFT (Değiştirilemez Jeton) kavramı ortaya çıktı. Birçok sanat eseri ve dijital içerik NFT olarak blokzincir üzerine kaydedilerek satıldı. |
| <b>14 Nisan 2021</b>  | Coinbase, NASDAQ borsasında halka arz edildi. Bu olay, kripto paranın kurumsal olarak kabul edildiğini gösteren önemli bir gelişmedir.    |
| <b>12 Mayıs 2021</b>  | Ether döviz kuru en yüksek fiyatına erişerek 4.878 \$'dan işlem gördü.                                                                    |
| <b>8 Haziran 2021</b> | İlk kez bir ülke, El Salvador, bitcoini yasal para birimi olarak kabul etti.                                                              |
| <b>Temmuz 2021</b>    | Ethereum, 2.0 güncellemesinin bir parçası olan Beacon Chain'i başlattı. Böylece PoS mutabakat mekanizmasına geçişin ilk adımı atıldı.     |
| <b>Eylül 2021</b>     | Çin, kripto para ticaretini ve madenciliği yasaklayan bir düzenleme getirdi.                                                              |
| <b>Kasım 2021</b>     | Blokzincir teknolojisine dayanan Metaverse projeleri geliştirilmeye başlandı.                                                             |
| <b>Aralık 2021</b>    | Merkeziyetsiz internet Web 3.0'de blokzincir teknoloji kullanımı gündeme geldi.                                                           |

**Tablo 2.5:** Blokzincir Teknolojisinde 2020 Sonrası Yaşanan Gelişmeler (Devam).

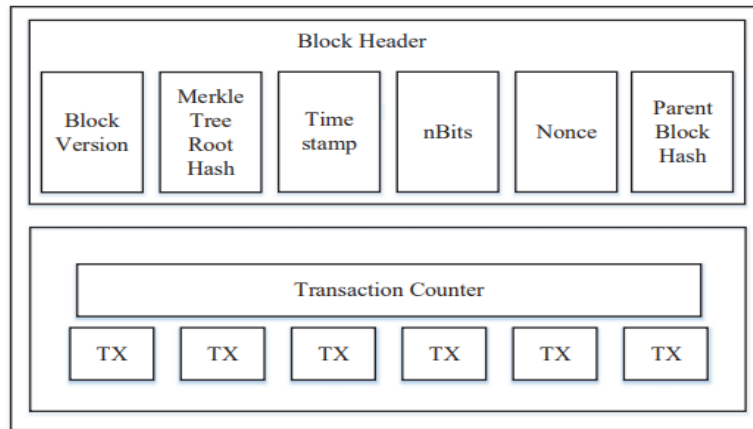
| Yıl           | Gelişme İçeriği                                                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Haziran 2022  | Güney Kore hükümeti, Dijital Varlık Komitesi kurdu ve Dijital Varlıklar Temel Yasası'nın yürürlüğe girmesi için çalışmalar yapmaya başladı.     |
| Haziran 2022  | İlk istikrarlı para birimlerine yönelik yasal çerçeve Japonya'da Fon Uzlaştırma Kanunu ile oluşturuldu.                                         |
| Eylül 2022    | ABD'de kripto paralara yönelik ilk düzenleyici yasa taslağı çıkarıldı. Ancak henüz yasalaşmadı.                                                 |
| Aralık 2022   | Türkiye'de blokzincir tabanlı Merkez Bankası dijital para birimi Dijital Türk lirası ile ilk ödeme gerçekleştirildi.                            |
| 15 Eylül 2022 | Ethereum, Merge güncellemesini yaparak PoS mutabakat algoritmasına geçti.                                                                       |
| Ekim 2023     | SEC, kripto para birimi piyasasına yönelik daha sıkı düzenlemelerde bulunacağını açıkladı.                                                      |
| Ocak 2024     | Ethereum, 2.0 güncellemesinin ikinci aşaması Shard Chains'i başlattı. Böylece ölçeklenebilirlik ve performans açısından önemli bir adım atıldı. |

## 2.3 BLOKZİNCİR TEKNOLOJİSİNİN TEKNİK KAVRAMLARI

Blokzincir teknolojisinin çalışma prensibinin bir bütün olarak anlaşılabilir olması için öncelikle içerdiği teknik kavramların; tanımları, türleri, önemli alt kavramları, gelişimleri ve uygulama biçimleri dikkate alınarak açıklanması gerekmektedir. Bu bağlamda; Blok, Ağ Yapıları, Kriptoloji, Mutabakat Algoritmaları, Kripto Cüzdan ve Akıllı Sözleşmeler kavramları bu bölümde detaylı bir şekilde ele alınmıştır.

### 2.3.1 Blok

Blok, belirli bir süre içerisinde gerçekleştirilen işlemlere ait her bir işlem ve onay kayıtlarının saklandığı şifrelenmiş veri kümesidir (Blockchain Türkiye Platformu, 2019, s.13).



**Şekil 2.4:** Blok Yapısı.

[Zheng, Z. vd., 2017, s.558]

Bir blok; Şekil 2.4'te gösterildiği üzere “Blok Başlığı (Block Header)” ve “Blok Gövdesi (Block Body)” olmak üzere iki ana yapıdan oluşmaktadır. Blok başlığında, bloğa özel temel bilgiler yer almaktadır. Bunlar (Zheng, Z. vd., 2018, s.355):

- a. Blok Sürümü (Block Version): İzlenecek blok doğrulama kurallarının hangisi olduğunu gösterir.
- b. Merkle Kök<sup>8</sup> Hash<sup>9</sup> Değeri (Merkle Tree Root Hash): Bloкта yer alan tüm işlemlere ait hash değeridir.
- c. Zaman Damgası (Time Stamp): İşlemin gerçekleştiği tarih (yıl, ay, gün) ve saat (saat, dakika, saniye) şeklinde zaman bilgisini ifade eder. Verinin hash'e girebilmesi için o anda var olması gerektiğini kanıtlar (Nakamoto, 2008, s.2).
- d. nBits: Geçerli bir blok hash değerinin, hedef değer eşiğidir.
- e. Nonce<sup>10</sup>: “Number Used Only Once (sadece bir kez kullanılan sayı)” ifadesinin kısaltmasıdır. Bir fonksiyonun çıktısını değiştirmeye yarayan tek bir işlemde yalnızca bir kez kullanılabilen (Monrat vd., 2019, s.117139), genel itibarıyla 0 rakamı ile başlayan ve her bir hash değer hesaplaması için artan 32 bitlik (4 byte) bir rastgele sayı dizisidir. <https://www.btcturk.com/bilgi-platformu/kriptopara-dunyasinda-nonce-ne-anlama-gelir/>
- f. Üst Blok Hash Değeri (Parent Block Hash): Bir önceki bloğa işaret eden 256 bitlik bir hash değeridir.
- g. Blok gövdesi ise işlem sayacı (transaction counter) görevi görmekte ve bloкта saklanan tüm işlemleri içermektedir. Her bir işlemin boyutuna bağlı olarak da bir bloğun içerebileceği maksimum işlem sayısı değişkenlik göstermektedir (Zheng, Z. vd., 2018, s.355).

Yukarıda yapılan tanımlama itibarıyla bloкта yer alan işlemlerin tümünün hash çıktısına “Merkle Kök Hash Değeri” denilmektedir. Şekil 2.5'te gösterildiği üzere; işlemler öncelikle

---

<sup>8</sup> “Merkle kökü” hakkında detaylı bilgi için bkz. s.25.

<sup>9</sup> “Hash” kelimesi, Türkçe'ye “Kriptografik Özet veya kısaca özet” ifadesi ile çevrilmiştir. Ancak yaygın olarak kaynak dildeki teknik ifadesi kullanıldığından bu çalışmada da “Hash” terimi üzerinden kullanılmıştır.

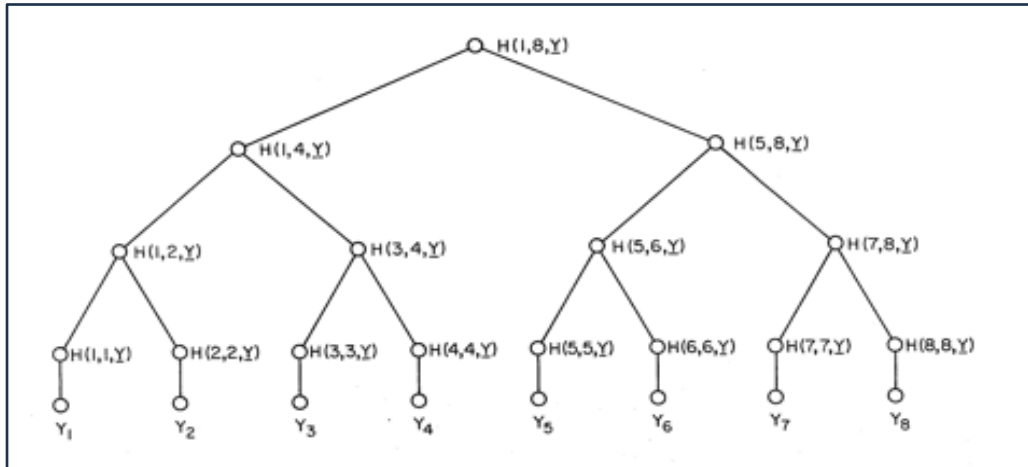
<sup>10</sup> “Nonce” kelimesi, Türkçe'ye “Tek Kullanımlık Sayı” ifadesinin kısaltması olarak “Teksa” şeklinde çevrilmiştir. Ancak yaygın olarak kaynak dildeki teknik ifadesi kullanıldığından bu çalışmada da “nonce” terimi üzerinden kullanılmıştır.



### 2.3.1.1 Merkle ağaçları (Merkle trees)

1979 yılında Ralph C. Merkle tarafından “Dijital İmza Sağlama Yöntemi” olarak Şekil 2.7’de gösterilen haliyle patenti alınan “Hash Ağacı” veya mucidinin adıyla anıldığı haliyle “Merkle Ağacı”; büyük veri kümelerinin bütünlüğünü, hızlı ve güvenilir bir şekilde doğrulayan bir veri yapısıdır.

Merkle, patenti aldıktan sonra 1987 yılında “A Digital Signature Based on a Conventional Encryption Function (Geleneksel Şifreleme Fonksiyonuna Dayalı Dijital İmza)” isimli makalesi ile hash ağacı kavramının çalışma prensibini açıklamıştır. Buna göre; sistemde, tek seferlik imzalardan oluşan sonsuz bir ağaç kullanılmaktadır. En basit haliyle; ağacın ikili olduğu varsayımı altında, bu sonsuz ağacın kökü sadece açık dosyaya yerleştirilerek doğrulanmaktadır. Ağacın her bir düğümü üç işlevi yerine getirmektedir: i) sol alt düğümün kimliğini doğrulama, ii) sağ alt düğümün kimliğini doğrulama ve iii) tek bir mesajı imzalama. Ağaçta sonsuz sayıda düğüm olduğundan, sonsuz sayıda mesaj imzalanabilmektedir. Bu üç işlevi yerine getirmek için her düğümün üç imzası olmalıdır: bir tane “sol” imza, bir tane “sağ” imza ve bir tane “mesaj” imzası. Sol imza, sol alt düğümü; sağ imza, sağ alt düğümü imzalamak için kullanılırken; mesaj imzası, bir kullanıcı mesajını imzalamak için kullanılmaktadır. Belirli bir imza için ise tüm değerlere (Y’lere) tek yönlü bir hash fonksiyonu uygulanmaktadır (Merkle, 1987, s.373).



Şekil 2.7: Merkle’in Dijital İmza Sağlama Yöntemi.

[<https://worldwide.espacenet.com/patent/search/family/022107098/publication/US4309569A?q=ap%3DUS7236379A>]



Bu yapıda; elimizde bulunan her bir veri, ağacın yapraklarıdır ve her bir yaprak teker teker hash fonksiyonundan geçirilerek verilerin hash değerleri bulunmaktadır. Bu hashlenmiş yaprak olmayan düğümler ağacın en alt dalını oluşturmaktadır. Ardından yaprak olmayan düğümler ikili çiftler halinde gruplandırılmakta ve her bir gruptaki iki düğümün hash değerleri toplanarak tek bir düğüm hash değeri yaratılmaktadır. Bu veri yapıları ile de ağacın bir üst dalı oluşturulmuş olmaktadır. Üstteki düğümler de tekrar çiftler halinde gruplandırılmakta ve bunların hash değerleri yine ağacın bir üst dalında saklanmaktadır. Bu işlem, tek bir dal/düğüm kalana kadar yani ağacın köküne ulaşılan kadar yapılmaya devam edilmektedir. Dolayısıyla bir düşmanın, yaprakların yani verilerin herhangi birinde bir değişiklik yapmaya kalkması halinde, bu değişiklik ağacın köküne kadar yayılmaktadır. Kök hash değere müdahale edilmesi de mümkün olmadığından, olması gereken değer ile kök değerinin eşleşmemesi veri bütünlüğünde bozulmanın tespit edilmesini sağlamaktadır (Narayanan vd., 2016, s.34).

Böylece Merkle ağaçları ve köklerinin; değişmezlik, manipülasyona karşı dayanıklılık, depolama ihtiyacının azaltılması, büyük veri kümelerinin etkin doğrulanması, blokzincirlerde bütünlük sağlama ve merkezi olmayan sistemlerde çapraz doğrulama açılarından olumlu katkıları bulunmaktadır. Sağladığı bu faydalar doğrultusunda Merkle ağaçları; dağıtık sistemler, blokzincir güvenliği, hash tabanlı kriptografi, dosya sistemleri, veri tabanı yönetimi, sürüm kontrol sistemleri ve merkezi olmayan uygulamalar dahil olmak üzere çeşitli alanlarda uygulama alanı bulmaktadır. Bu çalışma kapsamında blokzincir açısından değerlendirildiğinde Merkle kökü; bir bloktaki tüm işlem özetlerinin (hashlerinin) bir özeti (hashi)dir. Dolayısıyla tüm blokzinciri indirmeden doğrulama yapılmasını sağlayarak blokzincir teknolojisinin güvenliğini ve verimliliğini artırmaktadır (Sharma, 2023).

### **2.3.1.2 Zaman damgası (Time stamp)**

1991 yılında Stuart Haber ve W. Scott Stornetta, “How to Timestamp a Digital Document (Dijital Bir Belgeye Nasıl Zaman Damgası Vurulur)” isimli makaleleri ile dijital belgelerin kolayca değiştirilebilme özellikleri dolayısıyla karşılaşılan, belgenin ne zaman oluşturulduğu ve en son yapılan değişikliklerin ne zaman gerçekleştiğinin tespit edilmesi sorununa çözüm sunmuşlardır.

Öncelikli olarak bir dijital belgenin tarihinin kanıtlanması için fiziksel sistemlerdekinin bir benzeri olarak belgeye zaman damgasının vurulması önerisini getirmişlerdir. Ancak dijital ortamda belgede yapılan değişiklikler iz bırakmadan kaydedilebildiğinden bu zaman damgasının iki özelliğe sahip olması gerektiğini öne sürmüşlerdir (Haber vd., 1991, s.100):

- a. Verinin bulunduğu ortama değil kendisine, herhangi bir değişikliğin fark edilmeden yapılmasını imkânsız kılan bir zaman damgası vurulmalı,
- b. Belgeyi, gerçekte olduğundan farklı bir zaman ve veri ile damgalamak imkânsız olmalı (taklit edilemez olmalı).

Bu özelliklere sahip bir zaman damgası oluşturulması ise “dijital emanet kasası” işleyişi ile çözülebilmektedir. Bu çözüm; belgenin, zaman damgası servisi (Time Stamping Service – TSS) aracılığıyla damgalanarak saklanması ve belge bütünlüğünün sorgulanması halinde iki kopyanın karşılaştırılması şeklinde işlemektedir. Ancak bu çözüm de beraberinde; üçüncü taraf risklerini (güven, gizlilik, bütünlük gibi) ve depolama sorununu getirmektedir (Haber vd., 1991, s.101).

Depolama sorununa; hash fonksiyonları ile çözüm getirmişlerdir. Buna göre; belgenin kendisi yerine belgenin hash fonksiyonundan geçirilmesi ile özetlenen değeri TSS’ye gönderilmektedir.

Gizlilik ve bütünlük sorunu; dijital imzalar ile çözümlenmiştir. Buna göre; TSS, aldığı hash değerine zaman damgası ekleyerek bu birleşik belgeyi imzalamakta ve istemciye göndermektedir. İstemci de imzayı kontrol ederek, TSS’nin talebini doğru içerik ve zaman ile kaydettiğinden emin olmaktadır.

Güven sorunu ise dijital imza ve hash fonksiyonları ile bir dereceye kadar çözülmekte ancak tamamen ortadan kalkmamaktadır. Çünkü TSS’nin hata yaparak (kasıtlı veya değil) yanlış zaman damgası verme olasılığı hala mevcuttur. Bu zaman damgasının taklit edilebilme riski de ağın merkezi veya dağıtık olmasına göre iki yaklaşım ile çözümlenmiştir:

- a. Merkezi bir TSS’nin varlığı halinde; talepte bulunan istemcilerin önceki isteklerinden gelen bilgiler içeren bir zaman damgası sertifikası oluşturularak risk bertaraf edilmektedir. Bu zaman damgası sertifikası; (i) sertifika sıra numarası (ii) istemcinin kimlik numarası (ID), (iii) zaman damgası talep edilen belgenin hash değeri, (iv)

istemcinin önceki talebinden gelen bilgileri ve (v) sertifikanın zaman damgasından oluşmaktadır. TSS, bu bilgileri içeren sertifikayı imzalayarak istemciye göndermektedir. Böylece mevcut talep, istemcinin önceki taleplerine bağlanarak bir zaman damgası zinciri oluşturmakta ve sahte bir zaman damgası ile belgenin tarihinin değiştirilmesi engellenmektedir (Haber vd., 1991, s.103).

- b. Merkezi bir TSS'nin olmaması halinde ise istemci havuzundan rastgele seçilen bir istemcinin, belgeden üretilen hash'e zaman damgası vurması ile risk bertaraf edilmektedir. Bu yaklaşımda istemci seçimi, belgenin hash'ini tohum olarak kullanan bir “sözde rastgele üreteç (pseudo-random generator)<sup>12</sup>” ile gerçekleştirilmektedir (Haber vd., 1991, s.110).

Nakamoto blokzincir yapısının tasarımını, Haber ve Stornetta'nın zaman damgası şemalarının bir karmasına dayandırmıştır. Merkezi bir TSS'nin varlığı yaklaşımındaki zaman damgası sertifikası önerisini, blok yapısının tasarımında kullanırken; dağıtık ağ önerilerindeki katılımcıların seçimini, “sözde rastgele üreteç” yerine “mutabakat mekanizmaları”na dayandırmıştır. Böylece dağıtık bir ağda bloklardan oluşan zincir yapısını geliştirmiştir.

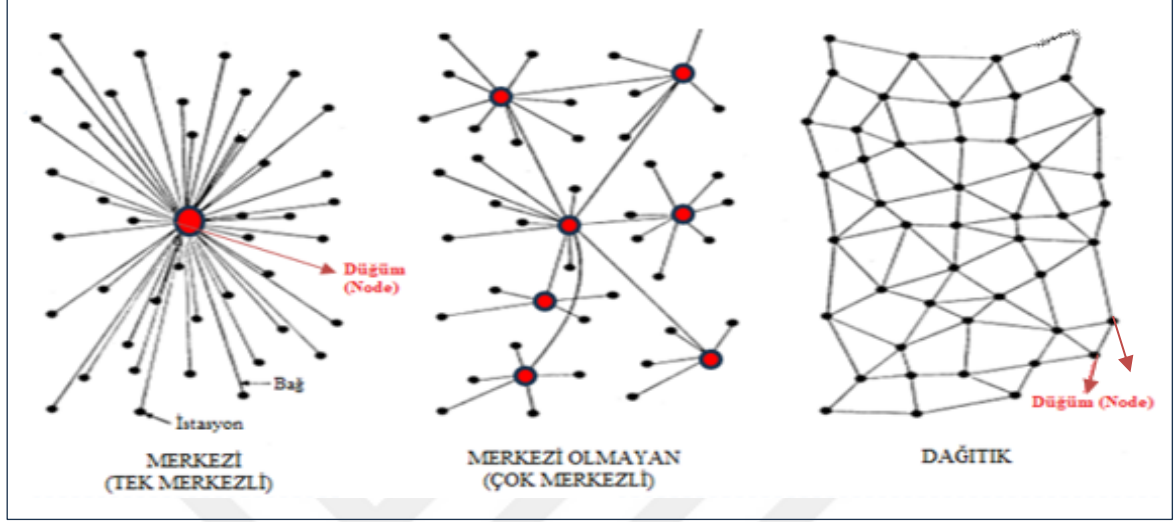
### 2.3.2 Ağ Yapıları

Ağ (network), birden fazla cihazın mevcut kaynakları ortak kullanımına imkân sağlayan bir yapıdır (Özseven, 2014, s.15). Bilgisayar ağları; bilgisayarlar ve iletişim cihazlarını, küçük veya büyük coğrafi alanlarda kablo veya radyo dalgaları gibi veri iletim ortamlarını, belirli kurallar (standart ve protokoller (HTTP, TCP/IP vb. gibi) çerçevesinde kullanarak birbirlerine bağlayan ve böylece kullanıcıların çeşitli kaynakları (yazıcı veya harddisk gibi donanım elemanlarını, uygulama yazılımlarını, verilerin depolandığı veri tabanlarını veya dosyaları) paylaşmalarını sağlayan bir sistemdir (Karadeniz, 2011, s.3).

---

<sup>12</sup> Sözde rastgele üreteç kavramı; dış gözlemci için rastgele gibi görünen ancak belirli bir başlangıç noktasından başlayarak deterministik bir algoritma ile sırayla sayılar üreten bir hesaplama yöntemidir.

Ağlar topolojik<sup>13</sup> olarak çok çeşitli türlerde çizilebilse de merkezi (centralized/star(yıldız)) ağlar ve dağıtık (distributed/mesh/grid(örgü)) ağlar<sup>14</sup> olmak üzere iki temel sınıfa ayrılmaktadır (Baran, 1964, s.3).



Şekil 2.8: Ağ Yapıları.

[Baran, 1964, s.4]'te verilen şekle yazar tarafından eklemeler yapılmıştır.

### 2.3.2.1 Merkezi ağlar

Merkezi ağ topolojisinde, istasyonların tamamı göbek (hub) veya anahtar (switch) adı verilen merkez düğümdeki bir cihaza bağlıdır. Ağ üzerindeki tüm trafik, bu merkezi noktadan geçmektedir. Ağa yeni bir istasyonun eklenmesi kolaydır ancak merkezdeki düğüm bozulduğunda istasyonlar arasındaki tüm iletişim kopmaktadır (Çölkesen & Örencik, 2008, s.39). Günümüzde en sık kullanılan ağ uygulaması, merkezi ağ topolojisidir. Bu tip topolojide merkezi bir otorite aracılığıyla tüm transfer işlemleri gerçekleşir ve yine işleme ilişkin verilerin saklanması da bu otorite tarafından sağlanır. Böylece taraflar arasında güvenilir paylaşım imkânı yaratılır. Bu otoritelere örnek olarak; göndermiş olduğunuz e-postanın karşı tarafa ulaştığı hakkında bilgilendiren bir servis sağlayıcısını veya havale yaptığınız belirli bir tutarın alıcısına ulaştığını bildiren bir bankayı verebiliriz.

<sup>13</sup> Ağ topolojisi, bir ağı oluşturan cihazların fiziksel ve mantıksal yerleşimidir.

<sup>14</sup> Dağıtık ağ kavramından ilk kez Paul Baran'ın 1964 yılında yayınlamış olduğu "On Distributed Communication Networks (Dağıtık İletişim Ağları Üzerine)" isimli makalesinde bahsedilmiştir.

### 2.3.2.2 Dağıtık ağlar

Dağıtık ağ topolojisinde ise, bilgisayarların birbirine bağlanması için hiyerarşik veya geometrik bir yapı dikkate alınmamaktadır. Ağa bağlı bilgisayarlar diğer bilgisayarlara farklı birkaç yoldan ulaşabilmektedirler. Dolayısıyla ağ üzerindeki herhangi bir düğümde bağlantının bozulması halinde diğer düğümler arasında kurulacak iletişimin engellenmesi söz konusu olmamaktadır (Uysal, 2011, s.113). Bu tip topolojiye örnek olarak; en yaygın WAN<sup>15</sup> (Wide Area Network - Geniş Alan Ağı) türü olan İnterneti verebiliriz.

Yapılan temel kavramsal açıklamaların ardından dağıtık ağ yapısını; iletişim ağları ile birbirine bağlanan, entegre ve tutarlı bir bilgi işlem ortamı yaratmak için tasarlanmış yazılım sistemleri ile donatılan, bağımsız makinelerden oluşan bir sistem olarak tanımlayabiliriz. Dağıtık sistemler, insanların iş birliği yapmalarını ve faaliyetlerini daha etkin ve verimli bir şekilde koordine etmelerini sağlar. Dağıtık sistemlerin temel amaçları: kaynak paylaşımı, açıklık, eşzamanlılık, ölçeklenebilirlik, hata toleransı ve şeffaflık ile temsil edilebilir (Jia & Zhou, 2005, s.1).

Dağıtılmış bir sistem, aslında bir ağın üzerine inşa edilmiş bir yazılım sistemidir. Sistemde yer alan birbirine bağlı birden fazla bağımsız bilgisayar arasından en iyi işlemciyi seçmek, tüm girdi dosyalarını bulup bu işlemciye taşımak ve sonuçları uygun yere koymak vb. gibi tüm sistem işlevleri kullanıcının bilgisi olmadan işletim sistemi tarafından otomatik olarak yapılmaktadır. Bu sırada ise dağıtık sistem kullanıcısı birden fazla işlemci olduğunun farkında değildir, sanal bir tek işlemcinin var olduğunu görmektedir (Tanenbaum, 1996, s.2). Bir başka deyişle; dağıtık ağ sisteminde, ortak bir amacı gerçekleştirmek üzere birbiriyle iletişim kuran bir dizi bağımsız bilgisayar tek bir ağ gibi davranmaktadır. Merkezi ağ sisteminde merkez düğüme ait olan yetki ve sorumluluklar dağıtık ağ sisteminde tüm düğümlere eş zamanlı olarak dağıtılmış bulunmaktadır.

### 2.3.2.3 Merkezi ve dağıtık ağ yapılarının karşılaştırmalı avantaj ve dezavantajları

Merkezi ağ sistemi; denetimin kolay olması nedeniyle tercih edilse de tüm kontrol ve erişimin tek bir nokta üzerinden yapılması sistem kullanıcılarını, bilgi bütünlüğü (bozulması) ve güvenliğinin (çalınması) tehlikeye girmesi ve ayrıca siyasi ve ekonomik

---

<sup>15</sup> Birbirinden çok uzak mesafede olan yerel ağları birbirine bağlamak için kullanılan, iletişimin telekom şirketiyle sağlandığı, ülke veya dünya geneline yayılmış bir ağ türüdür (Çölkesen & Örencik, 2008, s.129).

kontrol yetki gücünü elinde bulunduranların demokratik olmayan uygulamaları ve manipölasyonu (görevi kötüye kullanma) riskleri ile karşı karşıya bırakmaktadır. Bunun yanı sıra işleme aracılık eden yetkili unsurun faaliyetleri dolayısıyla hesaplanamayan işlem maliyetlerine de katlanılmaktadır (Karaarslan&Yazıcı Yılmaz, 2022, s.49).

Merkezi ağ sisteminin söz konusu risk ve dezavantajlarını bertaraf etmek üzere dağıtık ağ sistemleri kullanılmaktadır. Ancak gücün herkes tarafından kontrol edilerek işlemlerin aracısız yapılıyor olması sebebiyle merkezi ağ sisteminin, düşük işlem maliyetleri ile işlemlerin koordine edilmesi ve önceden belirlenmiş kuralların uygulanarak sistem başarısızlıklarının yetkili unsur tarafından düzeltilmesi vb. gibi avantajlarından faydalanılamamaktadır. Dağıtık ağ sistemlerinde her bir sistem katılımcısı bireysel olarak işlem ve koordinasyon maliyetlerini üstlenmek durumunda kalmaktadır (Karaarslan&Yazıcı Yılmaz, s.50). Diğer yandan; tarafların aracısız işlem yapabilme özgürlükleri, düğümler arası gizli anlaşma ve hileli işlem yapılması risklerini ve saklanan verinin herkesin erişimine açık olması (şifrelenmemiş) ise verinin tutarsız ve güvenilmez olması risklerini ortaya çıkarmaktadır. Dağıtık ağ sisteminin bu dezavantajları da sonraki bölümlerde anlatılacak olan Kriptoloji (Şifre Bilimi) ve Mutabakat Mekanizmaları sisteme dahil edilerek blokzincir teknolojisi kapsamında giderilmeye çalışılmıştır.

### **2.3.3 Kriptoloji : Kriptografi Yöntemleri**

Eski Yunanca “kryptos (gizli)” ve “logos (bilim)” kelimelerinin birleşiminden oluşan ve tüm dünyada orijinal haliyle kullanılan, Türkçe’ye “Şifre Bilimi” olarak çevrilen kriptoloji; iki taraf arasındaki bilgi iletişiminin, güvenli bir şekilde üçüncü tarafların erişiminden gizlenerek sağlanmasına yönelik yöntemlerin geliştirildiği bir bilimdir. Kriptoloji denildiğinde; verilerin belirli bir yöntem kullanılarak şifrelenmesi ile başlayan ve şifrelenmiş verinin güvenli bir ortam aracılığıyla alıcıya gönderilmesinin ardından alıcının şifreli veriye ulaşabilmesi için şifrenin çözülmesi ile tamamlanan bir süreç ifade edilmektedir (Yanar vd., 2022, s.35).

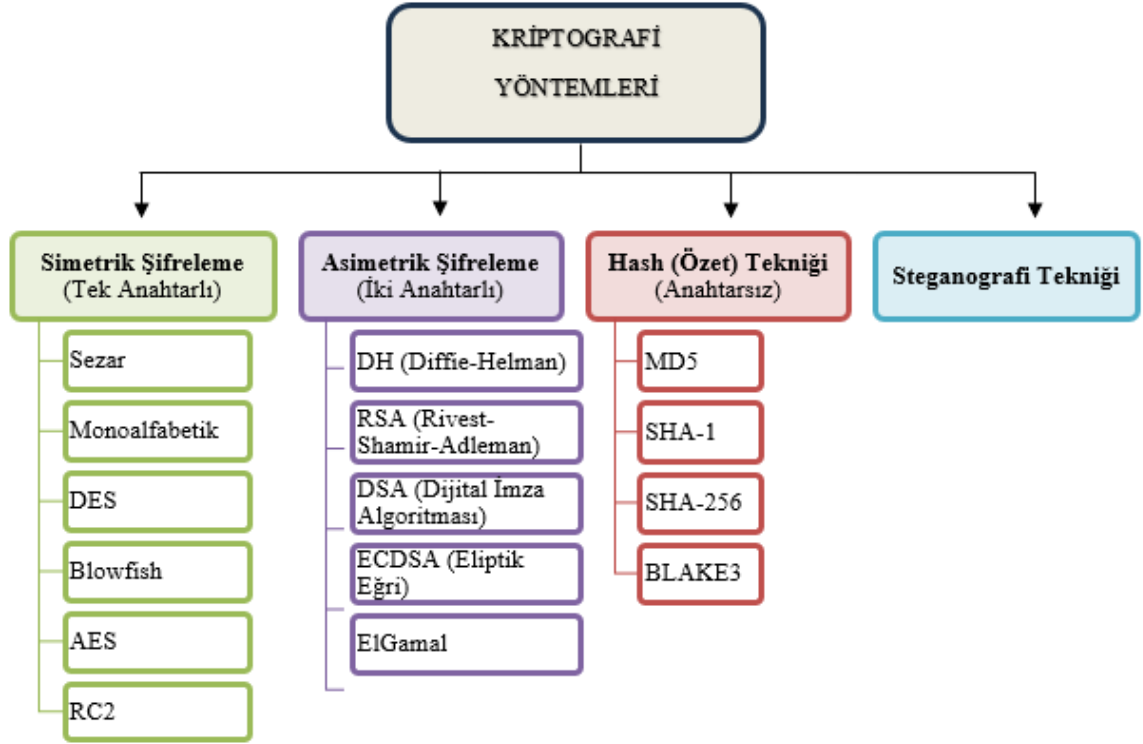
Genellikle salt şifreleme anlamında kullanılan kriptolojinin, tarihsel süreçteki gelişimine baktığımızda şifre çözümlerlerinin yarattığı büyük ve önemli olaylar neticesinde zor bir şifre oluşturarak şifreleme yönteminin güvenli bir şekilde saklanması kadar deşifre edilebilirliğinin ölçülmesine ve engellenmesine yönelik çalışmaların da önemi ortaya

çıkıştır. Dolayısıyla kriptoloji; kriptografi (şifre yazma) ve kriptanaliz (şifre kırma) olmak üzere iki temel alanı kapsamaktadır. Kriptografi, güvenilir olduğu varsayılan bir iletişim kanalı aracılığıyla gönderici ve alıcı arasındaki iletişimin gizli olarak gerçekleşmesini sağlamak üzere matematiksel algoritmalar (cipher) kullanılarak şifreleme (encipher/encrypt) ve şifre çözme (decipher/decrypt) işlemlerinin gerçekleştirilmesidir. Kriptanaliz ise, şifreleme yönteminde kullanılan gizli anahtara (private key) sahip olmadan deşifre yöntemlerinin uygulanmasıdır (Avaroğlu, 2017, s.60).

Geçmişte ve günümüzde sıklıkla karşılaşılan, özellikle de bilgi teknolojilerinin gelişimiyle birlikte hacmi ve kapsamı genişleyen, kötü niyetli diğer kişilerin kriptanaliz teknikleriyle saldırarak, ulaşılması istenmeyen şifrelenmiş bilgiyi ele geçirme, kullanma ve değiştirme tehditleri, bilgi güvenliğinin sağlanması hususunun önemini ortaya koymaktadır. Bu anlamda kriptoloji bilimi içerisinde, bilginin ele geçirilmesi, bozulması, değiştirilmesi vb. gibi potansiyel tehditlere karşı bilgi güvenliğini sağlama görevi ile kriptografi alanı ön plana çıkmaktadır. Kriptografi sisteminin başarılı olması için de bilgi güvenliğinin sağlanmasına yönelik bazı güvenlik ilkelerine uyulması gerekmektedir. Bu ilkeler; Gizlilik (Confidentiality), Bütünlük (Integrity), Erişilebilirlik (Availability), Kimlik Doğrulama (Authentication), İnkâr Edememe (Non-Repudiation) ve Güvenilirlik (Reliability)'tir (Tekerek, 2008, s.133). Bu ilkeler aşağıda kısaca açıklanmıştır:

- a. Gizlilik, gizli bilgiye yetkisiz kişilerin erişiminin engellenmesidir. Kriptografi sürecinde göndericiden alıcıya iletilen açık metnin şifreleme algoritması kullanılarak şifreli metne dönüştürülmesi gizlilik ilkesi gereğidir.
- b. Bütünlük, göndericiden çıkan bilginin alıcıya iletilmesi sürecinde bilginin herhangi bir değişikliğe uğramadığının doğrulanmasıdır. Hash (özet) algoritmalarının kullanılması veri bütünlüğünün sağlanması ilkesi gereğidir.
- c. Erişilebilirlik, yetkili kişilerin bilgiye ulaşabilir ve bilgiyi kullanabilir olmasıdır.
- d. Kimlik Doğrulama, gönderici ve alıcı kimliklerinin gerçekten onlara ait olduğunun doğrulanmasıdır. Dijital imza kullanılması kimlik doğrulama ilkesi gereğidir.

- e. İnkâr Edememe, göndericinin bilgiyi gönderdiğine ilişkin, alıcının da bilgiyi aldığına ilişkin eylemlerini reddetmemesidir. Sayısal imza tekniklerinin kullanılması inkâr edememe ilkesi gereğidir.
- f. Güvenilirlik, sistemden yapması beklenenler ile gerçekleşen sonuçların birbiriyle tutarlı olmasıdır.



Şekil 2.9: Kriptografi Yöntemleri ve En Yaygın Algoritma Örnekleri.

Bilgi güvenliği ilkeleri gözetilmiş kriptografi sürecinde kriptografi sisteminin tasarımına baktığımızda gerçekleşen saldırılara yönelik yeni önlemlerin alındığı, iyileştirmelerin yapıldığı bir model karşımıza çıkmaktadır. Her bir saldırının ardından mevcut hatalar düzeltilip iyileştirmeler yapılarak daha güçlü bir model geliştirilmektedir (Birer, 2022, s.22). Dolayısıyla kriptografi alanında, karşılaşılan çeşitli saldırı ve tehditlerden öğrenilenlere yönelik güvenli şifreleme sağlanması amacıyla farklı kriptografi yöntemleri geliştirilmiştir. Bu yöntemler ve ilgili yöntemleri temel alan bazı algoritma örnekleri Şekil 2.9’da özetlenmiş ve bölüm alt başlıklarında sınıflandırılarak söz konusu yöntemler aşağıda açıklanmıştır.

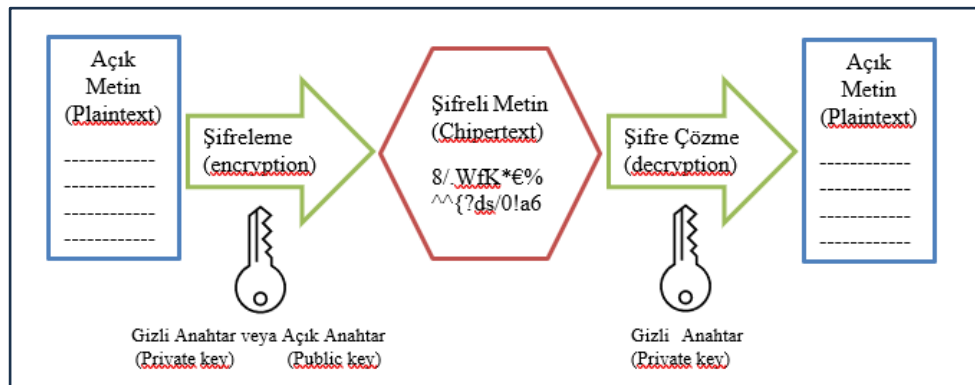


### 2.3.3.1 Simetrik şifreleme

Simetrik şifreleme, gizli veya tek anahtarlı olarak da bilinen en eski ve en basit şifreleme tekniğidir. Açık metinde yer alan bilginin gizli bir anahtar (private key) ile şifrelendiği ve sonrasında şifreli metnin yine aynı gizli anahtar (private key) yardımıyla açık metne dönüştürüldüğü bir algoritmadır. Kriptografi sürecinde iki tarafta da aynı anahtar kullanıldığından “simetrik” olarak tanımlanmıştır. Açık metne ulaşmak için gizli anahtarın bilinmesi yeterlidir dolayısıyla gizli anahtarın sadece şifreleme ve şifre çözme işlemlerini yapacak kişilerde bulunması gerekmektedir (Beşkirli vd., 2019, s.285). Simetrik şifre algoritmalarının hız performanslarının yüksek olması yaygın kullanım alanı sağlamasına rağmen şifrelemeyi yapan ile şifreyi çözen arasında paylaşılan bu ortak tek anahtarın saldırganlardan gizlenmesi (Avaroğlu, 2017, s.63) yöntemin en önemli risk unsuru olarak ortaya çıkmaktadır.

Simetrik şifreleme yöntemi; “Dizi (Karakter tabanlı) Şifreleme” ve “Blok (Bit tabanlı) Şifreleme” olmak üzere iki kategoriye ayrılmaktadır (Gönen vd., 2021, s.347). Şekil 2.9’deki sınıflandırmada Sezar ve Monoalfabetik algoritmalar dizi şifreleme yöntemlerine örnek iken, ABD Ulusal Standart ve Teknoloji Enstitüsü tarafından geliştirilen AES (Advanced Encryption Standard – Gelişmiş Şifreleme Standardı) ile IBM tarafından geliştirilen DES (Data Encryption Standard - Veri Şifreleme Standardı) gibi diğerleri blok şifrelemeye örnektir.

Kriptografi sürecinde bilginin güvenilir bir şekilde göndericiden alıcıya ulaştırılmasında izlenen tek veya iki anahtarlı şifreleme sistemlerinin temel çalışma prensibi Şekil 2.10’da gösterilmiştir.



Şekil 2.10: Anahtarlı Kriptografi Süreci.

### 2.3.3.2 Asimetrik şifreleme

Kriptografik yöntemler, 1970’li yıllara kadar yalnızca resmi ve askeri kurumlar tarafından kullanılmaktayken Diffie ve Hellman’ın 1976 yılında yayınlamış oldukları “New Directions in Cryptography” isimli makalelerinde bahsettikleri “Açık Anahtarlı (Public Key) Kriptosistem” kavramı ile devrim geçirmiştir. 1976 yılına kadar kullanılan mevcut şifreleme yaklaşımları anahtarın gizliliğine bağlı olarak güvenilir kabul ediliyordu. Ancak Diffie-Hellman (DH)’ın açık anahtarlı şifreleme yaklaşımı ile hem göndericinin hem de alıcının farklı anahtarlarıyla bilgi iletiminin gizli ve güvenilir yapılabileceği ortaya çıkmıştır (Akleyek vd., 2011, s.2).

Asimetrik şifreleme algoritmasında, simetrik şifrelemeden farklı olarak şifreleme ve şifre çözme işleminin yapılması için iki farklı anahtar kullanılmaktadır. Açık metin (plaintext) açık anahtar (public key) ile şifrlenirken, şifreli metin (chipertext) gizli anahtar (private key) ile çözülerek açık metne (plaintext) dönüştürülür (Beşkirli vd., 2019, s.286). Şifreleme anahtarının herkesin erişimine açık olmasından ve sistemin iki aşamasında farklı iki anahtar kullanılıyor olmasından dolayı bu yönteme “açık veya asimetrik” anahtarlı şifreleme denilmektedir. Bu sistemde; göndericinin de alıcının da başkaları ile paylaştığı birer açık anahtarları ve kimseyle paylaşmadıkları birer özel anahtarları bulunmaktadır. Yani her kullanıcının sadece kendisine özel açık-özel anahtar çifti vardır. Gönderici şifreli bir bilgi iletme istediğinde alıcının açık anahtarı ile bilgiyi şifreler ve gönderir. Alıcı ise şifreli bilgi kendine ulaştığında sadece kendisinin bildiği özel anahtar ile deşifre ederek bilgiye ulaşır, özel anahtarın olmaması durumunda açık (şifreleme) anahtardan özel (şifre çözme) anahtarın hesaplanması ve şifrenin çözülmesi mümkün değildir (makul bir zamanda mevcut bilgisayarların çözme kapasitesi yeterli olmadığından oldukça zor bir ihtimaldir). Ancak bu aşamada alıcı, bilginin gerçekten göndericiden gelip gelmediğine ilişkin sorun ile karşılaşmaktadır. Bu sorun da göndericinin şifreli bilgiye eklediği imza bölümü ile çözülmektedir. İmza bölümü, göndericinin özel anahtarı ile şifrlenirken göndericinin açık anahtarlarıyla çözülebilmektedir. Dolayısıyla alıcı, göndericinin açık anahtarıyla imza bölümünü deşifre ederek gerçekten de bilginin o göndericiden geldiğinin teyidini alır (Birer, 2022, s.25). Böylece kriptografi sürecinde bilgi güvenliğini etkileyen gizlilik, bütünlük, kimlik doğrulama, inkâr edememe ve güvenlik problemlerine asimetrik şifre algoritmaları ile çözüm getirilmiş olmaktadır. Ancak asimetrik şifre algoritmalarının hız performansları

değerlendirildiğinde simetrik şifre algoritmalarına göre daha yavaş oldukları belirtilmektedir. (Avaroğlu, 2017, s.64).

En yaygın kullanılan asimetrik şifreleme algoritmaları; RSA (Rivest, Shamir, Adleman), DSA (Digital Signature Algorithm - Dijital İmza Algoritması) ve ECDSA (Elliptic Curve Digital Signature Algorithm - Eliptik Eğri Dijital İmza Algoritması)'dır. Pek çok uygulamada metin şifrelemek için veya dijital imza için RSA algoritması kullanılmaktadır. DSA, adından da anlaşıldığı üzere yalnızca dijital imza için kullanılmakta metin şifrelemede kullanılmamaktadır (Kodaz vd.,2010, s.18). ECDSA ise blokzincir teknolojisinde kullanılan dijital imza algoritmasıdır (Zeng vd., 2017, s.558).

Asimetrik şifreleme algoritmasının uygulama alanlarına örnek verirse; internet üzerinden iletişimde sıklıkla kullanılan TLS (Transport Layer Security) altyapısı asimetrik RSA algoritması üzerine kuruludur ayrıca güvenilir e-posta iletişimi, kripto paralar ve dijital imza da asimetrik şifreleme algoritmaları üzerine kuruludur.

Asimetrik şifreleme yönteminin en önemli etkilerinden biri, dijital imzaların ortaya çıkmasıdır. Bu nedenle dijital imza kavramını tanımlamak sistemi anlamak açısından faydalı olacaktır.

### ***Dijital imza***

Literatürde “elektronik imza (e-imza)” veya “sayısal imza” olarak da adlandırılan dijital imza; elektronik ortamda gerçekleştirilen işlemlerin adres sahibini temsil edip doğrulayan, bir eşi daha olmayan kod kümesidir (Blockchain Türkiye Platformu, 2019, s.15).

Kamusal veya özel birçok işlemde kimliğinizi kanıtlamanız ve imza atmanız gerekmektedir. Bu işlemlerin elektronik ortamda yapılması halinde de yine ortama uygun olarak kimliğinizi kanıtlamanız ve imza atmanız gerekmektedir. Dijital imza, elektronik ortamlarda ıslak imzanın yerine geçerek bireyin kimliğini içeren ve gönderilmek istenen elektronik iletiye eklenen bir elektronik veridir (Akleyek vd., 2011, s.3). İki anahtarlı şifreleme algoritmasına dayalı olan dijital imza hem iletiyi gönderenin kimliğinin doğrulanmasında hem de gönderilen iletinin sayısal içeriğinin aktarım süresince değiştirilmediğinin ispatında kullanılan bölümdür (Kodaz vd., 2010, s.16).

Dijital imza şeması, anahtar yapısındaki asimetri dışında tipik bir mesaj kimlik doğrulama şeması gibidir. Her kullanıcının kendisine özel, bir gizli/özel anahtar (secret key) ve bir açık anahtar (public key) olmak üzere anahtar çifti bulunmaktadır. Herkesten gizlenmesi gereken özel anahtar, imzaları oluşturmak için kullanılırken; karşı tarafın da bildiği - herkese açık olan - açık anahtar, imzaları doğrulamak için kullanılmaktadır ve birbirlerinden farklıdır (Bellare, 2005, s.237). Dolayısıyla dijital imza süreci; “imzalama aşaması” ve “doğrulama aşaması” olmak üzere iki aşamadan oluşmaktadır. Örneğin, bir (A) kullanıcısının, (B) kullanıcılarına bir mesaj göndermek istediğini varsayalım. İmzalama aşamasında; (A), verileri kendi özel anahtarıyla imzalar ve (B)’ye imzalı sonucu ve orijinal verileri gönderir. Doğrulama aşamasında ise (B), (A)’nın açık anahtarı ile imzayı çözerek verinin (A)’dan geldiğini doğrular. Bu şekilde (B), verinin iletim sırasında değiştirilip değiştirilmediğini de kontrol etmiş olur (Zheng vd, 2017, s.558). Sonuç olarak; sadece gizli anahtara sahip olan bir imzacı imza oluşturabilirken, imzacının açık anahtarına sahip olan herkes imzaları doğrulayabilir (Bellare, 2005, s.237).

Kullanılacak dijital imzaların oluşturulması ve doğrulamasının yapılabilmesi için ise iki prosedürün yerine getirilmesi gerekmektedir. Birincisi kullanılacak dijital imza algoritmasının (RSA, DSA, ECDSA vb. gibi) belirlenmesi, ikincisi ise dijital imzanın atılacağı platformun diğer bir deyişle hangi kriptografik donanımlar (akıllı kartlar vb. gibi) aracılığı ile atılacağını belirlenmesidir (Akleyek vd., 2011, s.3).

### **2.3.3.3 Hash (Özet) tekniği**

Hash kelimesi İngilizce’de; küçük parçalara bölmek ya da karmakarışık yapmak, karıştırmak anlamlarında kullanılmaktadır. Bu iki eylemin bir araya getirildiği bir tekniğin de kriptografide kullanılması sebebiyle söz konusu yönteme “hash tekniği” adı verilmiştir. Hash tekniğinde; herhangi bir büyüklükteki mesaj, bloklara ayrılarak bir algoritma aracılığıyla karıştırılmakta ve uzunluğu sabit, eşsiz bir matematiksel özete dönüştürülmektedir (Çidem, 2012 s.38). Burada mesaj bir anahtar ile şifrelenerek gizlenmemekte, karmaşık bir özet haline dönüştürülmektedir. Bu nedenle hashing algoritmalarına, “anahtarsız algoritmalar” ve algoritmanın çıktısı değere, “özet değeri (hash değeri)” denilmektedir. Şifreleme sürecinde anahtar kullanmayan hash algoritmaları genellikle sistemde tek başlarına kullanılmazlar ve kriptografi süreci içerisinde simetrik veya asimetrik algoritmalara yardımcı olmak üzere işlev görmektedirler (Kara, 2009, s.38) Aynı

zamanda mesajın kendisini açığa çıkarmadan temsil edilmesini sağlamaktadırlar. Buna göre hash algoritmalarının bazı genel özellikleri aşağıda sıralanmıştır (Yılmaz, 2023):

- a. Hash fonksiyonlarında, şifreleme anahtarı kullanılmaz (Anahtarsız şifreleme).
- b. Hash fonksiyonlarında; özet veriden, asıl veriye ulaşılamaz (Tek yönlü fonksiyon).
- c. Bir girdi ile her zaman aynı çıktıya ulaşılır (Determinizm).
- d. Birden fazla girdiden aynı çıktıya ulaşma ihtimali düşüktür (Çarpışma direnci).
- e. Girdideki herhangi bir değişiklik, çıktı sonucunu değiştirmektedir (Çıg etkisi).

Bu özellikleri dolayısıyla hash algoritmaları; bilgi güvenliğinin, veri bütünlüğü ilkesi ve kimlik doğrulama ilkesi gereklerini sağlamaktadırlar. Verilerin bir nevi parmak izini oluşturmada kullanılırlar ve şayet verinin değiştirilmesi söz konusu olursa bu durumda yeni bir parmak izi oluşturulacak, eskisi geçersiz sayılacaktır. Ayrıca veriler, güvenilir olmayan bir kanal aracılığıyla iletilse bile veri bütünlüğü, yeniden hesaplanmış parmak izi ile önceden hesaplanmış parmak izi karşılaştırılarak doğrulanabilecektir (Çidem, 2012, s.39).

Hash algoritmaları; genellikle güvenli parola saklamada, dijital (sayısal) imza algoritmalarında ve bütünlük denetimlerinde sıklıkla kullanılmaktadır. Güvenli parola saklamada kullanılmasına yönelik uygulama şu şekildedir; çevrim içi sistemlerde, üyelerin kullanıcı parolaları hash algoritması ile özetlenerek veri tabanına kaydedilmektedir. Üyenin sisteme her girişinde ise, parolası aynı yöntemle hash değere dönüştürülerek diğer hash değeri ile karşılaştırılmakta ve böylece kimlik doğrulaması yapılmaktadır (Birer, 2022, s.26). Sistemde parola saklanmadığından özet değer ele geçirilse bile hash algoritmalarının tek yönlü fonksiyon olma özellikleri sebebiyle parolanın ortaya çıkarılması mümkün olamamaktadır (literatürde ters-görüntüye dayanıklılık veya tersine mühendislik olarak ifade edilmektedir). Çünkü hesapsal olarak metnin özetini almak kolay iken özeten metne ulaşmak zordur (Kara, 2009, s.38).

Bir diğer alan olan dijital imza uygulamalarına değinecek olursak; asimetrik şifreleme sistemlerini anlatırken bahsettiğimiz açık metne imza uygulamasında, metin ne kadar büyük olursa imzanın atılması da o kadar uzun sürecektir. Üstelik imzanın metin kadar büyük olması halinde ise metinden fazla yer kaplayacaktır. Dolayısıyla metnin özetenin alınıp

imzalanması durumunda süreç çok daha kısa olacaktır (Kara,2009, s.39). Bu nedenle dijital imza uygulamalarında hash algoritmalarını kullanmak hız sorununu azalttığından geniş uygulama alanı bulmaktadır. En yaygın kullanılan hash algoritmaları MD5, SHA 1 ve SHA256'dır.

Ayrıca Hash fonksiyonları veri bütünlüğünü sağlamak, bloklar arasında bağlantı kurmak ve güvenliği artırmak amacıyla blokzincir teknolojisinde de kullanılan bir kriptografik algoritmadır. Blokzincir teknolojisinde kullanılan hash algoritması ise SHA-256'dır.

### **Sha-256 fonksiyonu (Secure Hash Algorithm - 256 bit)**

ABD National Security Agency (NSA – Ulusal Güvenlik Ajansı) tarafından geliştirilmiş bir SHA hash fonksiyonu ailesinden algoritmadır.

SHA-256 hash fonksiyonunda; Binary Sistemde (2'lik taban) gösterilen 0 ve 1'lerden oluşan 256 bit değerindeki bir uzunluk, Hexadecimal Sistem<sup>16</sup> (16'lık taban)'e dönüştürülerek her bir karakter 4 bitlik bir değeri ifade edecek şekilde gösterilmektedir.

Bu fonksiyon aracılığıyla; herhangi bir uzunluğa sahip (ister bir roman isterse de bir harf veya rakam olsun) açık metin, 0'dan 9'a (0-9) rakamlar ve a'dan f'ye (a-f) harflerden oluşan sabit 64 karakterli (256 bit / 4 bit = 64 karakter) şifreli bir metne dönüştürülmektedir (Şekil 2.11)<sup>17</sup>.



**Şekil 2.11: SHA-256 Fonksiyon Özeti.**

<sup>16</sup> Hexadecimal Sistemde; rakamlar 0'dan 15'e kadar olan sayıları ifade eder. Ancak 10'dan 15'e kadar olan sayılar harflerle temsil edilir. Bu harfler, "a" ile "f" arasındadır. Her basamak, 16'nın bir kuvvetine karşılık gelir. Sağdan sola doğru, basamaklar 16'nın üssüne göre artar: 16<sup>0</sup>, 16<sup>1</sup>, 16<sup>2</sup>, 16<sup>3</sup>, vb. gibi.

<sup>17</sup> Deneme için bkznz. "<https://demoblockchain.org/hash>".

#### 2.3.3.4 Steganografi tekniği

Yunanca “steganos: gizli, saklı” kelimesinden türemiş, gizli yazı anlamına gelen steganografi, verinin başka bir içerik üzerine yerleştirilerek şifrelenmeden gizlenmesi yöntemidir. Veri; metin, ses, resim, video görüntüleri, sayısal resim vb. gibi unsurlar üzerine saklanabilmekte ve çözümülemesi sadece tekniği bilenler tarafından yapılabilmektedir. Amerikan Bağımsızlık Savaşı’nda casusların iletmek istedikleri mesajları mektupların satır aralarına yazmaları ve bunun sadece ısıtıldığında görülebilir olması ya da Yunan komutanın, iletmek istediği mesajı ulağın tıraş edilmiş kafasına yazdırıp saçı uzayınca ulağı alıcıya göndermesi ve saç tekrar tıraş edildiğinde görünür olması ya da müzik notalarına harflerin atanması ya da mors kodlarının II. Dünya Savaşı’nda kullanılması bu tekniğin örneklerindendir. Ayrıca teknolojinin gelişimiyle birlikte günümüzde verilerin korunması amacıyla da yeniden kullanım sıklığı artmıştır. Dosyaya önemsiz bite ekleme, maskeleye, filtreleme, mikro noktaları birleştirme gibi teknikler kullanılarak dijital nesneler üzerinde bilgilerin gizlenmesi şeklinde uygulama alanı bulmaktadır (Şahin vd., 2006, s.17,18).

#### 2.3.4 Mutabakat Algoritmaları (Consensus Algorithm)

İngilizce “consensus” kelimesi Türkçe’de fikir birliği, oy birliği, uzlaşma, mutabakat kelimelerine çevrilmektedir ve Türk Dil Kurumu (2024)’na göre; kelime anlamı olarak “bir iş, düşünce, görüş vb. üzerinde anlaşmaya varmayı” ifade etmektedir. Kelime anlamından yola çıkılarak “Concensus Algorithm” literatürde “Fikir birliği”, “Uzlaş/Uzlaşma” ve “Mutabakat” Algoritmaları olarak yer almakta hatta bazı kaynaklarda ise algoritmaların, kuralların adım adım tanımlanması yapıları gereğince Mutabakat “Protokolleri” veya “Mekanizmaları” ifadeleriyle de yer bulmaktadır.

Mutabakat algoritmalarında<sup>18</sup> mutabakat kavramı, güvenilir olmayan dağıtık bir ağ sisteminde kullanıcıların veya işlemcilerin ağ üzerinde yayınlanan işlemlerin kaynağının hatalı veya güvenilir olduğuna ilişkin “oy birliğine” ulaşmalarını ifade etmektedir.

Çalışmanın 2.3.2 bölümünde detaylı bir şekilde anlatılan ağ yapılarına baktığımızda merkezi sistemlerde; merkeze (sunucu) bağlı işlemcilerde bir arıza olduğunda ya da iletilen verilerde

---

<sup>18</sup> Kavramı literatüre kazandıran Lamport, Pease ve Shostak (1980), algoritma ifadesini kullandıklarından bu çalışmada da aynı terim kullanılmıştır.

bütünlük veya çalınma gibi güvenlik ihlalleri söz konusu olduğunda, merkez birim kriz durumunu kontrol etme ve hataları düzeltme yetkisine sahip olmaktadır. Verdiği işlem kararı konusunda ise uzlaşması gereken başka bir birim bulunmamaktadır. Ancak dağıtık sistemlerde merkezi bir birim olmadığından kriz durumunda yapılması gereken işlemlere ilişkin tüm birimlerin ortak bir karar alarak uygulamaya geçmeleri gerekmektedir. Buradan hareketle birimler arası güvenin söz konusu olmadığı bu dağıtık sistemlerde oy birliğinin sağlanıp sağlanamayacağına ilişkin problem Lamport, Pease ve Shostak (1980) tarafından “Bizans Generalleri Problemi (The Byzantine Generals Problem)” olarak adlandırılmış (Dolev, 1982, s.1) ve mutabakat algoritmaları ile çözümlenmiştir.

#### **2.3.4.1 Bizans generalleri problemi**

Lamport vd. (1982)’ye göre güvenilir bir bilgisayar sistemi, bir veya daha fazla birimin arızalanmasıyla başa çıkabilmelidir. Arızalı bir birim, sistemin farklı birimlerine çelişkili bilgiler gönderebilir. Bu tür bir arıza ile başa çıkma sorunu soyut olarak Bizans Generalleri Problemi olarak ifade edilmiş ve şu şekilde senaryolaştırılmıştır: Bizans ordusunun birkaç tümeni bir düşman şehrinin dışında kamp kurmuş ve her tümen kendi generali tarafından komuta edilmektedir. Generaller birbirleriyle sadece haberci aracılığıyla iletişim kurabilmektedirler. Düşmanı gözlemledikten sonra şehre “saldırmak” veya “geri çekilmek” konusunda ortak bir karar almaları gerekmektedir. Ancak bazı generaller hain olabilir ve sadık generallerin anlaşmaya varmasını engellemeye çalışabilmektedirler. Bu sorunun çözümünde; generaller oy birliğine ulaşmalıdırlar. Kararın geri çekilme veya saldırı olması kötü karar olarak değerlendirilmemektedir. Ancak mutabakata varılamayıp bir kısmının saldırıp bir kısmının geri çekilmesi daha kötü sonuç doğurmaktadır. Yani problem, hatasız işlemcilerin anlaşmaya varmasını sağlayacak bir algoritma bulunmasıyla çözülmektedir. Buna göre; herhangi bir dağıtık sistemde oybirliği, ancak ve ancak sistemdeki hatasız işlemci sayısının: i) toplam işlemci sayısının üçte ikisinden ( $2/3$ ) fazla olması ve ii) sistem ağının bağlanabilirliğinin yarısından fazla (%51) olması halinde sağlanmaktadır (Dolev, 1982, s.1). Ancak bu algoritmanın doğru çalışabilmesi için yani çoğunluk oylamasının güvenilir bir sistem oluşturabilmesi için iki koşulun yerine getirilmesi gerekmektedir<sup>19</sup>:

---

<sup>19</sup> Hikayeleştirilmiş açıklamada "komutan" girdiyi üreten birimi, "teğmenler" işlemcileri ve "sadık" ise hatalı olmayı tanımlamaktadır.



- a. Hatasız tüm işlemciler aynı girdi değerini kullanmalıdır (böylece aynı çıktıyı üretirler).
- b. Eğer girdi birimi hatalı değilse, hatasız tüm süreçler girdi olarak sağladığı değeri kullanır (böylece doğru çıktıyı üretirler).

Blokzincir teknolojisi açısından değerlendirdiğimizde; blokzincirin dağıtık ağ yapısı gereğince düğümler arası iletişimin sağlanması, Bizans Generalleri Problemine yani mutabakat algoritmalarına dayandırılmaktadır. Blokzincirin ilk uygulaması olan Bitcoin kripto para biriminin yaratıcısı Nakamoto, bir mutabakat algoritması olan “İş Kanıtı” uygulamasını ilk kez Bitcoin’i yarattığı makalede (Nakamoto, 2008) tanımlamıştır. Ancak literatürde iş kanıtı kavramı yeni değildir. Nitekim Nakamoto (2008, s.3) söz konusu makalede; “Adam Back’in Hashcash’ine benzer bir iş kanıtı (proof-of-work) sistemi kullanılması” gerekliliğinden bahsetmiştir. Diğer yandan Back (2002, s.1) ise 1997’de hashcash mekanizmasını önerdiğinde Dwork & Naor (1993)’ın çalışmalarından haberdar olmadığını ve Jakobsson & Juels (1999)’un iş kanıtı çalışmalarında da maliyet fonksiyonun daha farklı bir amaç taşıdığını ifade etmiştir.

Mutabakat algoritmaları, esasen Nakamoto’nun Bitcoin’de iş kanıtı mutabakat protokollerini uygulamasıyla önem kazanmıştır ve kripto para birimleri ile blokzincir teknolojisindeki gelişmelerden etkilenecek çeşitlenmiştir. Dolayısıyla literatürde çok çeşitli mutabakat algoritmaları geliştirilmiştir ve her biri blokzincir teknolojisinin mevcut problemlerine çeşitli bakış açıları sunarak farklı çözümler getirmiştir. Bu algoritmaların her birinin temel varsayımları farklı olduğundan, sunduğu çözümlerin etkinliği ve önemi de değişkenlik göstermektedir (Kardaş, 2019, s.483). Bu mutabakat algoritmalarından en sıklıkla karşılaşılan ve en temel varsayımlara sahip olan üç tanesine ilişkin açıklamalar bölüm alt başlıkları sınıflandırması altında yapılmış bulunmaktadır.

#### **2.3.4.2 İş kanıtı (Proof of work -POW)**

İş Kanıtı kavramı, ilk kez Dwork ve Naor (1993)’ın “Pricing via Processing or Combatting Junk Mail (İşlem Yoluyla Fiyatlandırma veya Gereksiz Posta ile Mücadele)” isimli makalesinde önemsiz e-postaları önlemek amacıyla kullanılmıştır. Bu makale; Fiat-Shamir Şeması (1986)’na dayalı bir PoW algoritması ile önemsiz e-posta gönderim maliyetlerinin artırılarak önemsiz e-posta gönderiminin sınırlandırılabilceğini önermektedir.

Fiat ve Shamir (1986)'in kimlik doğrulama ve dijital imza şeması; ispatlayıcının kendisini doğrulamasını sağlayan, etkileşimsiz (alıcı-gönderici iletişime girmez) bir kanıt doğrulama protokolüdür. Bu şemada; ispatlayıcı, rastgele bir özel anahtar seçmekte ve bu anahtarı kullanarak bir açıklama oluşturmaktadır. Daha sonra, hash fonksiyonları aracılığıyla bu açıklamanın özetini alıp bir kanıt üreterek ve bu kanıtı e-postaya ekleyerek alıcıya göndermektedir. Alıcı ise göndericinin eklediği özet ile göndericinin kimliğinin doğrulamasını yapmakta ve sonuç doğru ise kimlik beyanını onaylamaktadır; değil ise reddetmektedir. Alıcı burada aktif rolde değildir, sadece doğrulama işlemini gerçekleştirir bu nedenle de bu şema interaktif olmayan bir yöntemdir (Fiat vd., 1986).

Dwork ve Naor (1993); Fiat-Shamir şemasına, ispatlayıcının iddiasını desteklemesi için ilave bir hesaplama maliyeti gerektiren iş kanıt algoritmasını entegre etmişlerdir. Böylece ispatlayıcının iddiasını doğrulamak için sadece özetin kontrol edilmesi yeterli olmamakta, aynı zamanda PoW'un da doğrulanması gerekmektedir. PoW algoritmasının işleyişinde; e-posta göndericileri gönderdikleri her bir e-posta için orta zorlukta ama zor olmayan bir hesaplama görevi çözmek durumundadırlar. Gerçekte ücretsiz sağlanan bu e-posta hizmetinde, e-posta göndericisi gönderiminin gerçekleşmesi için belirli bir maliyete katlanarak bu hesaplamayı çözmektedir. CPU maliyet fonksiyonu olarak ifade edilen bu değer; göndericinin bilgisayarının, CPU (Central Processing Unit - Merkezi İşlem Birimi) kapasitesini, enerjisini ve zamanını ayırması anlamına gelmektedir. Gönderici hesaplamayı çözdükten sonra MD4 hash fonksiyonu aracılığıyla özetini almakta ve e-postaya ekleyerek alıcıya göndermektedir. Alıcı da hash fonksiyonlarıyla özeti doğrulamakta ve sonuç doğru ise e-postayı kabul etmektedir. Bu sistemde, normal miktarda mesaj gönderen bir kullanıcı için, her mesaj başına gereken toplam kaynak kullanımı minimum gerçekleşmekte ve kullanıcı maliyeti hissetmemektedir. Ancak çok sayıda ve belirli özellikteki mesajları göndermeyi amaçlayan bir kullanıcı için, toplam kaynak kullanım maliyeti daha yüksek hesaplanmakta ve caydırıcı olmaktadır. Böylece gereksiz e-posta gönderimi azaltılmaktadır (Dwork vd., 1993).

1999 yılında ise Jakobsson ve Juels, “Proofs of Work and Bread Pudding Protocols (İş Kanıtları ve Ekmek Pudingi Protokolleri)” isimli makalelerinde Dwork ve Naor (1993)'un

iş kanıtı kavramını, "Bread Pudding– Ekmek Pudingi"<sup>20</sup> olarak adlandırdıkları bir protokol kapsamında tanımlayarak temel prensiplerini ortaya koymuşlar ve literatüre resmi olarak kazandırmışlardır. Bu makalede PoW, “bir tarafın (ispatlayıcı), diğer tarafa (doğrulamaya) belirli bir zaman diliminde belirli bir seviyede hesaplama gücü harcadığını gösteren bir protokoldür” şeklinde tanımlanmıştır (Jakobsson vd., 1999).

Yine 1999 yılında Juels ve Brainard, “Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks (İstemci Bulmacaları: Bağlantı Tüketme Saldırılarına Karşı Kriptografik Bir Karşı Önlem)” isimli makalelerinde Dwork ve Noar (1993)’ın iş kanıtı modelinin, “İstemci Bulmacası (Client Puzzles)” kavramı ile çevrimiçi hizmet reddi<sup>21</sup> saldırılarının önlenmesinde kullanılmasına yönelik uygulanabilirliğini tartışmışlardır. Bu makaleye göre istemci bulmacası; sistem saldırı altında değil iken taleplerin fark gözetmeksizin kabul edildiği ancak saldırı altındayken sunucunun, istemciden gelen talebi kabul edebilmesinin, istemci tarafından kriptografik bir bulmacanın, belirli bir hesaplama gücü kullanılarak doğru çözülmesi koşuluna bağlandığı bir protokol olarak tanımlanmıştır.

Ayrıca yine bir hizmet reddi (DoS) karşı önlem tekniği olarak 1997 yılında Adam Back tarafından “Hashcash” iş kanıtı algoritması icat edilmiştir (www.hashcash.org). Back daha sonra 2002 yılında, “Hashcash - A Denial of Service Counter-Measure (Hashcash – Bir Hizmet Reddi Karşı Önlemi)” isimli makalesi ile hashcash iş kanıtı mekanizmasının esaslarını ve ilk uygulama sonuçlarını açıklamıştır. Bu makalede açıklanan hashcash mekanizmasına göre; göndericinin, e-postayı gönderebilmesi için belirli bir işlem gücü harcayarak istemci bulmacasını çözmesi gerekmektedir. Bulmaca, SHA 1 veya MD 5 gibi kriptografik hash fonksiyonları kullanılarak çözüldüğünde belirli bir zorluk seviyesini gösteren benzersiz bir bit dizesi (hash değeri) üretilmektedir. Bulmacanın çözüldüğü yani hash değerinin üretildiğine ilişkin iş kanıtı, istemciye “token (damga/jeton)” dağıtılması yoluyla oluşturulmaktadır. İstemci de göndermek istediği e-postaya bu token’ı ekleyerek

---

<sup>20</sup> Ekmek pudingi, boşa gitmesi muhtemel bayat ekmeği tekrar değerlendirmek için tasarlanmış bir yemektir. Ekmek pudingi protokolü ise, kaynakların etkin kullanımını sağlamak amacıyla hesaplama sürecini tekrar döngüye sokmaktadır. Geleneksel ekmek pudingi tarifi, eski ekmekleri geri dönüştürürken, ekmek pudingi protokolü hesaplama gücünü en verimli şekilde kullanmaktadır (Jakobsson vd., 1999, s.259).

<sup>21</sup> Hizmet reddi (Denial of Service - DoS) saldırıları; bir bilgisayar ağı veya hizmet sunucusuna kapasitesinin üzerinde aşırı istek gönderilerek sisteminin çalışmaz hale getirilmesine ve sisteme erişimin engellenmesine yönelik siber saldırılardır. Kalabalık bir insan grubunun, bir mağazanın kapılarına yığılıp, mağaza çalışanlarının ve müşterilerin içeri girmesini engelleyerek normal faaliyetlerin aksamasına sebep olmalarını buna örnek verebiliriz.

alıcıya göndermektedir. Alıcı ise gelen e-postaların doğrulamasını bu token üzerinden yapmaktadır. Eğer token belirli bir zorluk seviyesini karşılıyorsa e-postanın gerçek bir kullanıcıdan geldiği kabul edilmekte aksi halde karşılamıyorsa gereksiz olarak (spam) işaretlenmekte veya reddedilmektedir. Burada zorluk seviyesini gösteren hash değeri uzunluğudur<sup>22</sup> ve hash değeri uzunluğu belirli bir zorluk seviyesi için gerekli olan sıfır bitlerinin sayısına bağlıdır. Daha yüksek bir zorluk seviyesi daha fazla başlangıç sıfırı yani daha fazla işlem gücü gerektirmektedir. Dolayısıyla bir yandan alıcılar açısından e-posta göndericisinin gerçekliği doğrulanırken diğer yandan daha fazla işlem gücü harcanması sebebiyle otomatikleştirilmiş istenmeyen (spam) e-posta gönderimi, maliyetli hale getirilerek gönderimi engellenmektedir (Back, 2002).

İş kanıtı algoritmasını mutabakat mekanizması olarak literatüre kazandıran ise blokzincir tabanlı Bitcoin kripto para birimi uygulamasıyla Nakamoto (2008) olmuştur ve bu algoritma en yaygın olarak Bitcoin madenciliğinde kullanılmaktadır ([www.hashcash.org](http://www.hashcash.org)). Bu nedenle blokzincir teknolojisi terminolojisinde kullanılan “Madencilik (Mining)” veya “Kripto Para/Bitcoin Madenciliği” kavramları İş Kanıtı Mutabakat Algoritması (PoW) işlem sürecini ifade etmektedir.

Nakamoto 2008 yılında yayınladığı Bitcoin White Paper’ında; güvenilir üçüncü bir taraf olan finans kuruluşlarının aracılığına dayalı çevrimiçi elektronik para transferine alternatif bir çözüm olarak iş kanıtı algoritmalarının kullanıldığını “Eşler Arası Elektronik Nakit Sistemi”ni önermiştir. Dağıtık ağ yapısına dayalı bu sistemde; para transferinin birbirine güvenmeyen taraflar arasında dolandırıcılık veya çift ödeme sorunu yaşanmadan gerçekleştirilebilmesi için tüm transfer işlemlerinin kamuya duyurularak her bir düğümde aynı kayıt bilgilerinin olması ve sistem katılımcılarının tek bir işlem sırası üzerinde anlaşma sağlamaları gerekmektedir. Düğümler arası bu anlaşmanın sağlanması için mutabakat algoritmaları kullanılmaktadır. Diğer yandan işlemi gerçekleştiren tarafların kimlik doğrulamaları, veri ve sistem güvenliği risklerinin bertaraf edilmesi için hash tabanlı iş kanıtı algoritmaları kullanılmaktadır. Ayrıca işlemin doğruluk ve geçerliliğinin kanıtlanması

---

<sup>22</sup> Hashcash şeması ilk yayımlandığında hash değeri zorluk seviyesine göre aratan bir bit dizesi olarak belirlenmiştir. Ancak sonrasında daha basit, adil ve doğrulama maliyeti düşük olması sebebiyle Finney ve Thomas (2002) tarafından önerilen sabit çıktı dizesi (k-bit) kabul edilmiştir (Back, 2002, s.5).

yanında mutabakat algoritmalarının yapısı gereği çoğunluk temsiliyetinin belirlenmesinde de iş kanıtı algoritması kullanılmaktadır (Nakamoto, 2008).

Dolayısıyla Nakamoto'nun geliştirmiş olduğu “İş Kanıtı Mutabakat Algoritması”, kriptografik algoritmaların birleştirildiği karmaşık bir yapıdır ve bu yapı aşağıda maddeler halinde açıklanan protokol adımları itibarıyla işlemektedir:

- a. Blok oluşturma (İş kanıtı üretme)
- b. Bloğun ağda paylaşımı
- c. Zincire blok ekleme (doğrulama ve mutabakat)
- d. Ödül alma

a. Blok oluşturma (iş kanıtı üretme): Merkeziyetsiz bir ağ sistemine dayalı blokzincirde işlem kaydı yapan yani yeni blok oluşturan ağ katılımcılarına, “madenci (düğüm)” denilmektedir. İsteyen herhangi bir kullanıcı kişisel bilgisayarına açık kaynak kodlu<sup>23</sup> madencilik yazılımını (Bitcoin Core, CGMiner, EasyMiner vb. gibi) kurduktan sonra ağa erişim sağlayarak madenci olabilmektedir. İstedikleri zaman ağdan ayrılabilme inisiyatifine sahip olan bu gönüllü madenciler, ağa erişimleriyle birlikte tüm veri tabanının bir eşi üzerinde işlem yapabilir olmaktadır. Ancak blok oluşturma işlemini hangi madencinin yapacağını seçilmesi gerekmektedir. Bu seçim, sonunda ödülü olan bir iş kanıtı üretme rekabetinin sonucuna bağlıdır. Ağdaki tüm madenciler, Hashcash iş kanıtı algoritmasındaki istemci bulmacasına benzer şekilde, belirli bir zorluk seviyesindeki kriptografik problemi CPU işlemci gücü ve enerji kullanarak diğer madencilerden önce çözmeye çalışırlar. Madenciler için bulmaca çözüm süreci aşağıdaki adımlardan oluşmaktadır:

- i. Madenci, işlem havuzunda toplanan işlemlerden blok içerisinde yer almasını istediklerini seçer.

---

<sup>23</sup> Açık kaynak kodlu yazılımlar; kullanıcıların yazılımın kaynak kodlarına erişebildiği ve bu kodları inceleyip, gerektiğinde değiştirebildiği ücretsiz yazılımlardır. Kodların açık olması, yazılıma şeffaflık ve denetlenebilirlik katmakta dolayısıyla güvenlik riskinin düşük olmasını sağlamaktadır. Herkesin kodlara erişebilmesi sayesinde de sınırsız sayıda potansiyel katılımcı aracılığıyla yazılım geliştirilebilmektedir.

- ii. Seçilen işlemler ile Merkle kök hash değeri oluşturulur.
- iii. Merkle kök hash değeri, üst blok hash değeri ve zaman damgası bilgileri ile birlikte blok başlığı oluşturulur. Blok başlığında Nonce alanı da bulunmaktadır. Ancak bu aşamada Nonce değeri 0 yerine 32 bitlik (4 byte) rastgele bir sayı olarak görünmektedir.
- iv. Blok başlığında yer alan bilgilerin tümü birleştirilerek SHA-256 fonksiyonu (bkz. s.41) uygulanır ve bloğun hash değeri hesaplanır. Madencinin bulmacayı çözme süreci burada başlamaktadır. Madenci, belirlenen zorluk derecesine uygun blok hash değerine ulaşmak için gizli bir değer olan Nonce değerini, rastgele olarak sürekli değiştirerek bulmaya çalışır. Bu süreç Nonce değeri bulunana kadar devam eder.
- v. Uygun blok hash değerini veren Nonce değer tahmin edilmesiyle iş kanıtı üretilmiş olur. Böylece blok, ilk iş kanıtını üreten madenci tarafından oluşturulur.

### ***İş kanıtı bulmacası (Hash puzzle)***

Bitcoin blokzinciri protokolüne göre madencilerin çözmesi istenilen kriptografik bulmaca şu şekildedir (Bakırcı, 2017) :

*“İşlem havuzundan seçtiğin işlemlerden oluşturduğun blok belli bir büyüklüğe ulaşınca SHA-256 fonksiyonu uygulayarak, 256 basamaklı bir şifre yaratacaksın. Ancak bu şifrenin ilk 30 basamağının sadece ve sadece sıfırlardan oluşması gerekiyor. Bu kuralı sağlayan bir şifre yaratmak için, kendi hesap defterinden ürettiğin bloğun sonuna belli bir sayı eklemen gerekiyor. Bu sayıyı bul.”*

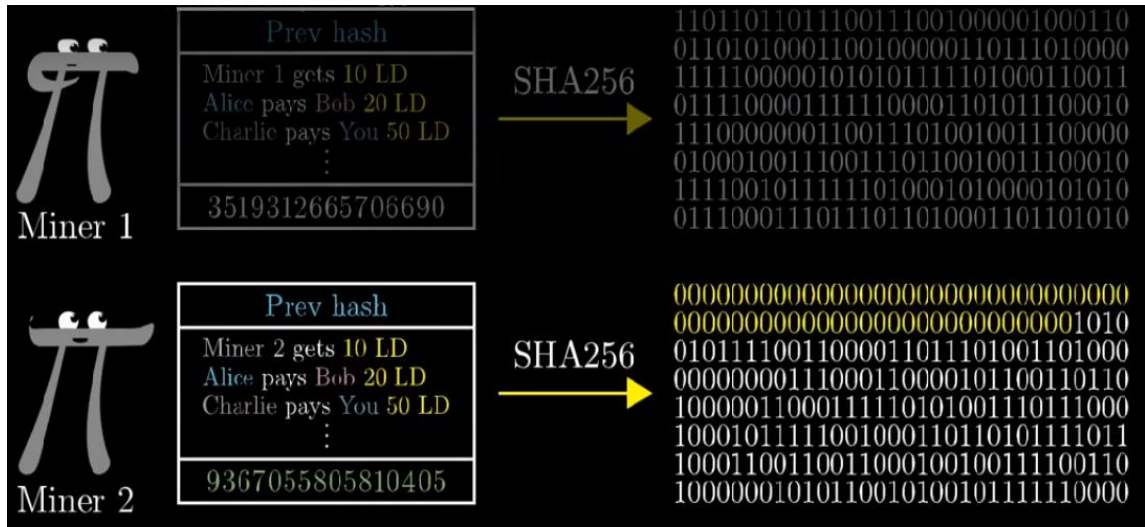
Yani madenciler öyle bir sayı bulmalıdırlar ki blokzincire eklemek istedikleri bloğa bu sayıyı ekleyip SHA-256 fonksiyonu uyguladıklarında ortaya çıkan 256 basamaklı değer ilk 30 basamağı “0 (sıfır)” olsun. Böylece madenciler bu gizli sayı “Nonce”u deneme yanılma yolu ile tahmin ederek bulmacayı çözmeye çalışırlar (Şekil 2.12 ve Şekil 2.13).

Hash bulmacalarını çözmek olasılıksaldır çünkü hiç kimse, hangi nonce değer hash bulmacasını çözeceğini tahmin edemez. Bunu yapmanın tek yolu nonce'ları teker teker denemek ve birinin başarılı olmasını ummaktır. Matematiksel olarak bu sürece “Bernoulli denemeleri” denilmektedir. Bernoulli denemesi, iki olası sonucu olan bir deneydir ve her

sonucun gerçekleşme olasılığı birbirini izleyen denemeler arasında sabittir (Narayanan vd., 2016, s.66). Ayrıca her deneme birbirinden bağımsızdır, yani bir denemenin sonucu diğer denemeleri etkilemez.



Şekil 2.12: İş Kanıtı Bulmacası.



Şekil 2.13: Madencilik ile Hash Üretme.

[<https://www.youtube.com/watch?v=bBC-nXj3Ng4>]

### Zorluk seviyesi (Difficulty level)

İş kanıtı bulmacası belirli bir zorluk seviyesine göre ayarlanmaktadır. Zorluk seviyesi ise çıktı hash değerinde bulunması gereken başlangıçtaki “0 (sıfır)” bitlerin sayısına bağlıdır. Daha yüksek bir zorluk seviyesi için daha fazla başlangıç sıfırı gerekirken, daha düşük bir zorluk seviyesi için daha az başlangıç sıfırı gerekmektedir. Buna göre Bitcoin blokzinciri protokolünde zorluk düzeyinin, artırılması istenirse başlangıç sıfırları 30 adetten fazla (örneğin 50 adet), azaltılması istenirse başlangıç sıfırları 30 adetten az (örneğin 20 adet) olarak belirlenmelidir.

İş kanıtı bulmacasında Nonce değerin bulunması için bilgisayar CPU gücü ve elektrik kullanılarak olası tüm kombinasyonları rastgele deneme yöntemi olan kaba kuvvet saldırısı uygulanmaktadır. İlk 30 basamağı sıfır olan 256 basamaklı bir sayıyı bulma olasılığı ( $\frac{1}{2^{30}}$ )  $\cong \frac{1}{1,000,000,000}$ ) yaklaşık 1 milyarda 1 mümkündür. Yani 1 milyar denemeden sonra ancak bu sayı bulunabilir. Bunun için de çok yüksek düzeyde CPU gücüne sahip olunması ve elektrik harcamasının yapılması gerekmektedir. Dolayısıyla zorluk seviyesi ne kadar yüksekse o kadar çok CPU gücü ve elektrik kullanılacak ve çözüm süresi ona göre uzayacaktır.

Bitcoin blokzincir protokolünde zorluk düzeyi, zincire her 2016 blok ilave edildiğinde otomatik olarak ayarlanmaktadır. Böylece zincire yeni blok ekleme süresi ortalama olarak 10 dakikayı bulmaktadır (Nguyen vd., 2018, s.106). Bu da yaklaşık 2 haftada<sup>24</sup> bir zorluk düzeyinin yeniden ayarlanması anlamına gelmektedir.

Blok üretim süresi; eğer 10 dakikadan kısa sürmeye başladıysa (2016 adet blok için 1.209.600 saniyeden az<sup>25</sup>), madencilerin özetleme kapasiteleri artmış demektir bu durumda bulmacanın zorluk seviyesi otomatik olarak sistem tarafından %300 artırılır. Eğer ki 10 dakikadan uzun sürmeye başladıysa (2016 adet blok için 1.209.600 saniyeden fazla), madencilerin özetleme kapasiteleri azalmış (madenci sayısı azalmış) demektir bu durumda ise bulmacanın zorluk seviyesi otomatik olarak sistem tarafından %75 azaltılır (Çarkacıoğlu, 2016, s.47).

- b. Bloğun ağda paylaşımı: İş kanıtı bulmacasının herhangi bir madenci tarafından çözülmesiyle yeni oluşturulan blok ağdaki tüm madencilerle paylaşılır. Bu aşamada diğer madenciler artık daha fazla hesaplama yapmaya devam etmez, bulmaca çözümünü bırakırlar ve oluşturulan yeni bloğun doğrulamasını yapmaya başlarlar.
- c. Zincire blok ekleme (doğrulama ve mutabakat): Bloğun oluşturulup ağda paylaşılmasıyla diğer madenciler, “bulunduğu iddia edilen bu gizli sayı” Nonce değerini blok başlığına ekleyip ikinci kez SHA-256 fonksiyonundan geçirirler. Ve çıktı blok hash değerini, belirlenen zorluk seviyesindeki hash değeri ile karşılaştırırlar. Eğer ki Nonce

---

<sup>24</sup> (10 dakika x 2016 adet blok) / (60 dakika x 24 saat) = 14 gün = 2 hafta.

<sup>25</sup> 10 dakika x 2016 adet blok x 60 saniye = 1.209.600 saniye.



değeri 30 adet “0 (sıfır)”lı hash değerini üretiyorsa bloğu doğrulayarak kendi zincirlerine de eklerler. Nonce değeri bulmanın zorluğuna rağmen bulunup bulunmadığına ilişkin doğrulamanın yapılması saniyeler süren bir kolaylıktır. Dolayısıyla blokzincire eklenene kadar iki kez SHA-256 fonksiyonundan geçirilmektedir. İlki, iş ispatı üretmek için, ikincisi ise bloğun geçerli olup olmadığını belirlemek yani doğrulama yapmak içindir.

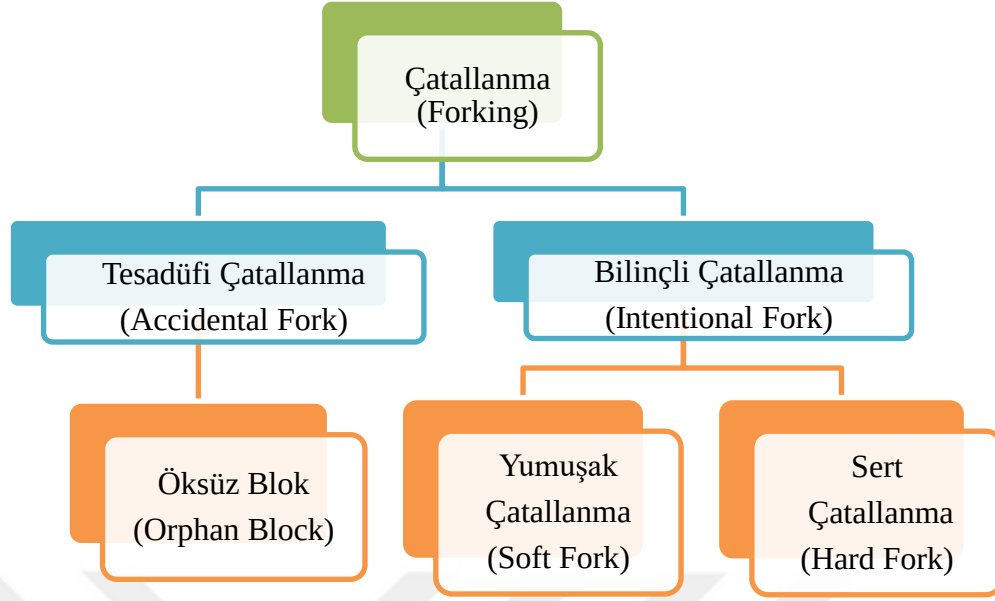
Diğer yandan sistemin saldırıya uğraması veya rastlantısal sebepler dolayısıyla birden fazla madencinin aynı anda blok oluşturması ve bu blokların diğer madenciler tarafından doğrulanarak zincire eklenmesi mümkün olabilmektedir. Bu durumda zincirde, aynı yükseklikte (sırada) birden fazla blok olduğundan çatallanma gerçekleşir. Söz konusu çatallanmaya sebep olan bloklardan hangisinin ağ genelinde kabul edileceğine madencilerin %51’nin mutabakatı sonucu karar verilir.

### ***Çatallanma (Forking)***

En basit tanımı ile çatallanma; blokzincirin bölünerek birden fazla kola ayrılmasıdır (Blockchain Türkiye Platformu, 2019, s.14). Blokzincir ağında ortaya çıkabilecek;

- a. Saldırganların blok bulma olasılığından (Nakamoto, s.6) (kötü niyetli düğümlerin varlığından)
- b. Bloğun iletimi sırasındaki gecikmelerden (Dilek, 2018, s.63)
- c. Teknik değişikliklerden (Blockchain Türkiye Platformu Teknoloji Çalışma Grubu, 2019, s.14) (blok boyutu değişikliği gibi yazılım güncellemelerinden)

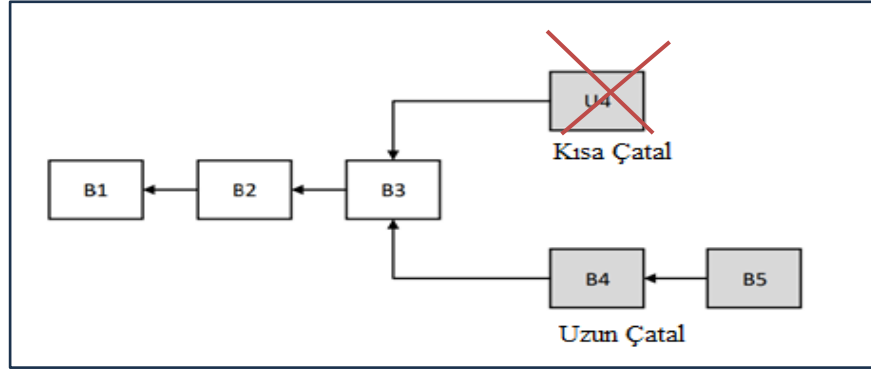
kaynaklanan sebeplerle farklı madenci düğümlerin, aynı yükseklikteki (yani bloğun zincirdeki sırası) iki farklı bloğu onaylayarak kendi zincirlerine eklemesi mümkündür. Bu durum, ağda iki alternatif zincirin oluşmasına yol açmakta ve literatürde "çatallanma" olarak adlandırılmaktadır (Dilek, 2018, s.63).



**Şekil 2.14:** Çatallanma Türleri.

Şekil 2.14'te görüldüğü üzere çatallanma, “Tesadüfi” ve “Bilinçli” olarak sınıflandırılmaktadır. Buna göre bilinçli çatallanma, teknik değişikliklerden kaynaklanan sebeplerle ortaya çıkan çatallanma iken; tesadüfi çatallanma ise, blok iletimindeki gecikmeler ve kötü niyetli saldırılar nedeniyle madencilerin aynı anda blok oluşturması durumunda ortaya çıkan çatallanmadır.

Tesadüfi çatallanmada; birden fazla madenci uygun nonce değerini kazara aynı anda bulduğunda geçerli bloklar eş zamanlı olarak üretilmekte ve sonuç olarak Şekil 2.15'te gösterildiği gibi farklı dallar oluşabilmektedir. Ancak rakip dalların aynı anda bir sonraki bloğu üretmeye devam etmesi pek mümkün olmamaktadır (Zheng vd., 2017, s.560). Çünkü çatallanma ortaya çıktıktan sonra madencilerin hangi zincirin dikkate alınması gerektiğine ilişkin karar vermesi gerekmektedir. Bu durum mutabakat algoritmaları ile çözümlenmiştir ve ağdaki düğümlerin %51'inin kararı neticesinde sonraki blok, zincire eklenmektedir. %51'lik çoğunluğun temsiliyeti de üretilen iş kanıtı ile belirlenmektedir. Buna göre 1 CPU harcaması 1 oyu temsil ettiğinden çoğunluğun kararı en fazla CPU harcaması yapılan yani en fazla iş kanıtı çabası yatırılan işlem sırası (blokszinciri) olmaktadır (Nakamoto, s.3). Buradan hareketle en çok iş kanıtı üreten zincir, uzun olan çatalı ifade etmekte ve uzun olan çatal geçerli kabul edilmektedir. Kısa olan çatal ise terkedilerek zincirden atılmaktadır. Kısa çatalın ucundaki terkedilen bloğa literatürde “Öksüz (Yetim/Bayatlamış) Blok” denilmektedir.



**Şekil 2.15:** Blokzincirin Çatallanması.

[Zheng vd., 2017, s.560]

Şekil 2.15’te görüldüğü üzere B4 ve U4 blokları aynı anda oluşturulmuş ve çatallanma meydana gelmiştir. Bu aşamadan sonra madenciler iki dal üzerinde de daha uzun bir dal bulunana kadar çalışmayı sürdürürler. B5 bloğunun oluşturulmasıyla birlikte ise daha uzun bir zincir ortaya çıktığından U4’teki madenciler U dalını terk ederek uzun olan B dalına geçerler (Zheng vd., 2017, s.560). Zincir B dalından devam ederken U4 bloğu öksüz blok olarak kalır.

Diğer yandan blokzincir yazılımının açık kaynak kodlu olması dolayısıyla isteyen tüm düğümler yazılımı değiştirme ve güncelleme önerisinde bulunabilmektedir. Söz konusu öneri, ağdaki tüm düğümler tarafından kabul edilmesi halinde zincir bölünmeden uygulanmaktadır, aksi takdirde güncellemeyi benimseyen ve benimsemeyen iki farklı madencilik süreci dolayısıyla yeni bir blokzincir çatallı ortaya çıkmaktadır. Blokzincir ağının tek bir zincir üzerinde yeniden birleşmediği bu bölünme türü ise “Bilinçli Çatallanma” olarak adlandırılmaktadır. Bilinçli çatallanmada; protokol değişikliklerinin, güncelleme yapmayan düğümler ile geriye dönük uyumlu olup olmamasına göre “Yumuşak” ve “Sert” olmak üzere iki farklı türde çatallanma ortaya çıkmaktadır.

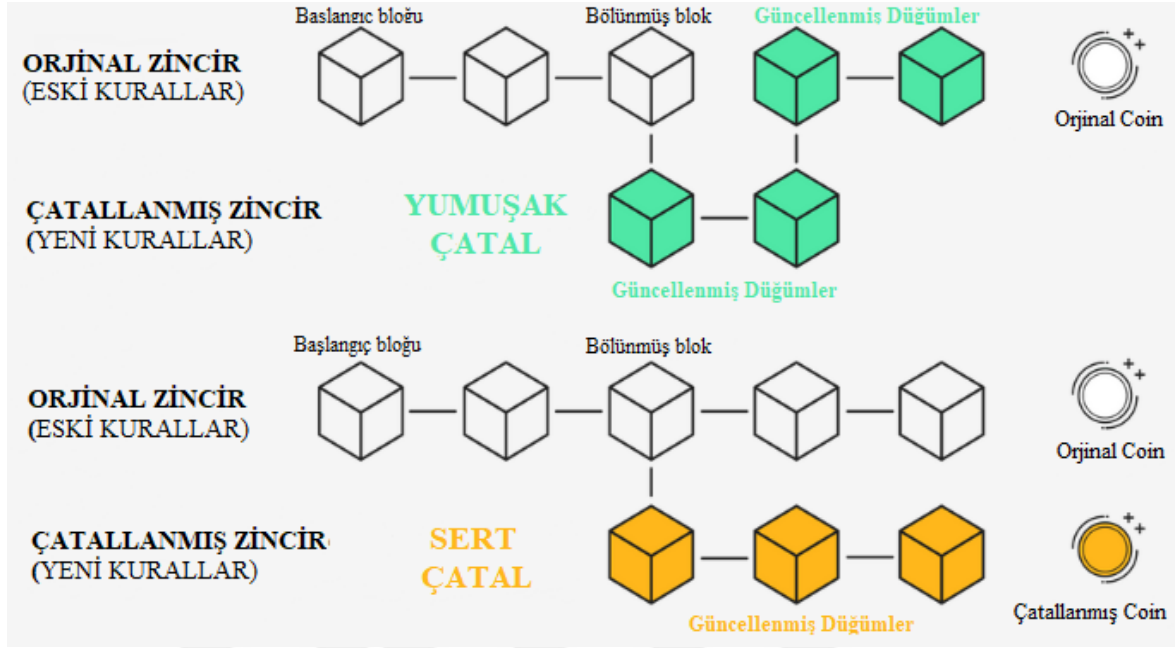
“İsteğe bağlı / Gönüllü çatal” olarak da tanımlanan yumuşak çatallanma; protokol değişikliklerinin, güncellenmemiş düğümlerle geriye dönük uyumlu olduğu çatallanmadır (Yaga vd., 2018, s.29). Tüm blokzinciri düğümleri aynı ağ üzerinde çalışmakta, ancak bazıları eski kurallar altında, bazıları da yeni kurallar altında işlem yapmaktadır (Tangem Team, 2017). Yani yeni kurallar, eski kurallar altında da geçerli olmakta; eski düğümler,

yeni kurallar ile çıkarılan blokları reddetmemektedirler. Bu nedenle, düğümlerin güncelleme yapması zorunlu değil isteğe bağlıdır.

Zorunlu veya sert çatallanma ise yumuşak çatallanmanın tam tersi olarak protokol değişikliklerinin, güncellenmemiş düğümlerle geriye dönük uyumlu olmadığı çatallanmadır. Çünkü yazılım güncellemesi, yeni kurallar ile oluşturulmuş blokların eski sürüm tarafından kabul edilemeyeceği şekilde değiştirilmiştir. Dolayısıyla güncellenmemiş düğümler, değişiklikleri takip eden blokları reddetmektedirler. Bu durum blokzinciri ağında bir bölünmeye yol açarak aynı blokzincirinin birden fazla versiyonunun oluşmasına neden olmaktadır (Yaga vd., 2018, s.29). Sonuç olarak düğümlerin yeni kurallar ile işlem yapabilmesi için güncelleme yapmaları zorunlu olmaktadır. Güncelleme yapmayan düğümler ise eski kurallar ile işlem yapmaya devam etmektedirler.

Yumuşak çatallanma daha çok küçük ölçekli değişiklikleri içermektedirken sert çatallanma geniş kapsamlı değişiklikler getirmektedir. Örneğin bir mobil cihaz ya da bilgisayarda temel işletim sistemi güncellemesi yapıldığını varsayalım. Güncellenmenin ardından, cihazdaki tüm uygulamalar güncellenmiş işletim sistemiyle sorunsuz bir şekilde çalışmaya devam edecektir. Bu güncelleme yumuşak çataldır. Buna karşın, tamamen yeni bir işletim sistemine geçmek sert çatalı ifade etmektedir (Tangem Team, 2017). Şekil 2.16’da yumuşak çatallanma ve sert çatallanma süreçleri karşılaştırmalı olarak gösterilmiştir.

Uygulamada blokzincir ağında karşılaşılan ölçeklenebilirlik (işlem kapasitesi ve hızı) sorununa yönelik birçok yazılım güncellemesi çözüm önerileri getirilmiştir. Bunlardan imza verilerinin işlemlerden ayrıldığı ve verilerin blokta yeniden düzenlendiği SegWit (Segregated Witness – Ayrılmış Tanık) güncellemesi yumuşak çatala örnek iken, Ağustos 2017’de blok boyutu sınırının 1MB’dan 8 MB’a çıkarılması güncellemesine uyum sağlayamayan madenciler dolayısıyla gerçekleşen çatal sonucu piyasaya sürülen Bitcoin Cash (BCH) sert çatala örnektir (BİTLO AKADEMİ, 2022) .



Şekil 2.16: Yumuşak Çatallanma ve Sert Çatallanma.

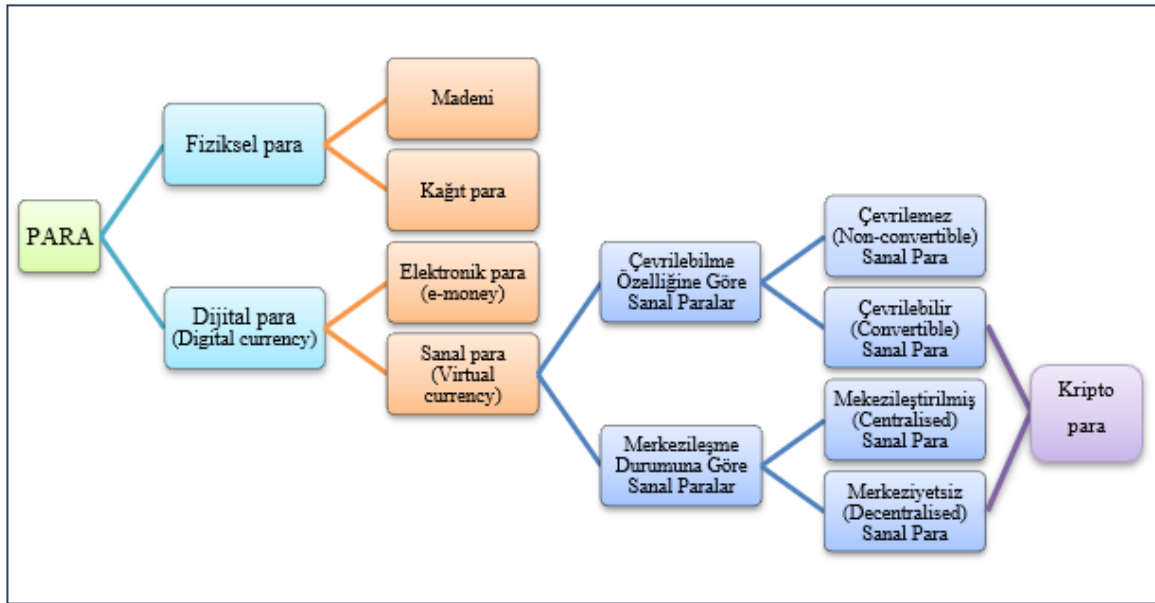
[Tangem Team, 2023]

- d. **Ödül Alma:** İş kanıtı mutabakat protokolünün son adımı madencinin, madencilik faaliyetini başarı ile gerçekleştirmesi sonucunda ödül kazanmasıdır. Bu aşamada; iş kanıtı üreterek blok oluşturan ve bu bloğu, diğer madencilere doğrularak %51 çoğunluk mutabakatını sağlayıp blokzincirine "ilk ekleyen" madenciye ödül verilmektedir. Verilen bu ödül bir "coin" yani kripto paradır. Kripto para bulmak için bulmaca çözülmesi eyleminin maden bulmak için kazı yapılmasına benzetilmesinden dolayı iş kanıtı sürecine veri madenciliği denilmektedir. Bitcoin blokzinciri protokolünde veri madenciliğinin sonunda ulaşılan maden de bitcoindir.

#### **Kripto para : Bitcoin (btc - □)**

Kripto para; "crypto (şifreli)" ve "currency (para birimi)" kelimelerinin birleşiminden oluşan "Cryptocurrency" teriminin Türkçeleştirilmiş halidir ve şifreli para birimi anlamına gelmektedir. Bitcoin ise ilk kripto para birimidir. Bitcoin'in tanımı ve özelliklerinin net bir şekilde açıklanabilmesi için öncelikle kripto para birimlerinin ortaya çıkışından yani paranın gelişimi ve sınıflarından kısaca bahsedilmesi gerekmektedir.

Bankacılık sektörü ve paranın gelişimine baktığımızda; öncelikle altına endeksli kâğıt para sisteminin sona ermesiyle para, temsili<sup>26</sup> statüden merkez bankaları tarafından belirlenen kaydi<sup>27</sup> para statüsüne evrilmiş; sonrasında ise teknolojik gelişmeler sayesinde paranın elektronik olarak transfer edilmesiyle banka kartlarının kullanımı yaygınlaşmış ve para fiziksel niteliğini neredeyse kaybederek dijitalleşmiştir (Dilek, 2018, s.9). Paranın dijitalleşmesiyle çok çeşitli dijital para ürününün ortaya çıkması bu yeni parasal araçların (bu çalışmanın konusu gereğince özellikle kripto paranın) anlaşılabilirliğini olumsuz yönde etkilemiştir. Diğer yandan; dijital, elektronik ve sanal kelimelerinin anlam benzerliği, paranın sınıflandırılmasında terimsel açıdan da bu kelimelerin birbirlerinin yerine kullanılmasına yol açmakta ancak aynı tanımlamaları ifade etmemektedir. Bu durum da literatürde kavramsal karmaşaya sebebiyet vermektedir. Bu karışıklığın giderilerek kavramsal netliğin sağlanması amacıyla aşağıda Şekil 2.17’de para sınıflandırılması verilmiştir.



**Şekil 2.17: Paranın Sınıflandırması.**

[Karacan vd., 2021, s.15]’den esinlenilerek yazar tarafından oluşturulmuştur.

<sup>26</sup> Temsili para; istenildiğinde altın ve gümüş gibi değerli madene çevrilebilen ödeme aracıdır. Altına dayalı bir mali sistemde; para basanlar veya sertifika düzenleyenler, bastıkları miktarın karşılığını sabit bir oranda altın veya gümüş olarak tutarlar (Yılmaz, 2022, s.3).

<sup>27</sup> Kaydi para; mevduat/banka parası da denilen bankaya yatırılan mevduatların kredi olarak verilmesiyle bankalar tarafından yaratılan paradır.

Şekil 2.17’de gösterildiği üzere; fiziksel ve dijital olmak üzere iki temel yapıda para kullanımı söz konusudur. Fiziksel para; madeni ve kâğıt paralar (fiat/itibari para) aracılığıyla yüz yüze mal ve hizmet değişiminde kullanılan, elle tutulabilen ve doğrudan elden ele geçen bir ödeme aracıdır. Dijital para ise taraflar karşı karşıya gelmeden, elden ele geçmeden transfer edilebilen ve fiziksel varlık göstermeyen, elektronik olarak saklanabilen (Çarkacıoğlu, 2016, s.6) değerlerdir. Dijital para; paranın, mübadele aracı, değer ölçüm birimi ve değer saklama işlevlerini dijital olarak yerine getirmekle birlikte ödeme aracının yasal (legal tender) bir statüye sahip (Karacan vd., 2021, s.14) olup olmamasına göre “Elektronik Para” ve “Sanal Para” olarak ikiye ayrılmaktadır

Elektronik para; fiziksel paranın (fiat para), dijital cihazlarda veya sunucularda saklanan dijital temsilidir (Bozkurt Yüksel, 2015, s.183). Diğer yandan elektronik para, yasal para biriminin elektronik forma dönüştürüldüğü salt dijital değerden daha kapsamlı olarak geniş para tanımı ile hukuki olarak yetkilendirilmiş özel sektör kuruluşları tarafından çıkarılan ve zorlayıcı gücü bulunmayan bir parasal değeri de ifade etmektedir (Sugiara vd., 2009, s.155).

6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun’un md.3/ç bendinde göre; *“Elektronik para, elektronik para ihraç eden kuruluş tarafından kabul edilen fon karşılığı ihraç edilen, elektronik olarak saklanan, bu Kanun’da tanımlanan ödeme işlemlerini gerçekleştirmek için kullanılan ve elektronik para ihraç eden kuruluş dışındaki gerçek ve tüzel kişiler tarafından da ödeme aracı olarak kabul edilen parasal değer”*dir.

Elektronik paranın ilk uygulama biçimi; banka mevduat hesabına dayalı “borç kartları (debit card)”dır. Bu banka kartları ile mevduat sahipleri, ATM (Automated Teller Machine - Otomatik Vezne Makinesi) aracılığıyla hesaplarından doğrudan para çekebilmekte ya da POS (Point Of Sale – Ödeme Noktası) cihazları aracılığıyla ödeme yapılabilmektedirler. İkinci uygulaması; karta önceden yüklenen değer ile satın alınan gerçekleştirildiği “akıllı kartlar”dır. Üçüncü uygulama şekli ise e-cash, Netcash, CyberCash ve Mondex vb. gibi “elektronik nakit (elektronik cash)”tir (Bozkurt Yüksel, 2015, s.190).

Paranın dijitalleşme sürecinde elektronik para ve ödeme yöntemleri (elektronik para, kredi kartı, e-cash, e-cüzdan, elektronik çek, PayPal, First Virtual vb. gibi) çeşitlenmiş ve hacimleri giderek artmıştır. Ancak bu dijitalleşme; kartların çalınması, banka/kredi kartı

sistemlerinin hacklenmesi, bilgi güvenliği tehditleri ve yüksek transfer maliyetleri gibi risk ve olumsuzlukları da beraberinde getirmiştir (Dilek, 2018, s.9). Diğer yandan elektronik ödeme sistemleri, yapıları dolayısıyla kişisel gizliliğin korunması açısından da zayıflıklara sahiptir (Chaum, 1983, s.199). Bu eksiklik ve risklerin bertaraf edilmesine yönelik elektronik paranın kriptografik olarak güvenli olduğu türleri geliştirilmiştir. Söz konusu “kriptografik elektronik ödeme sisteminin” (Çarkacıoğlu, 2016, s.7) temelleri 1983 yılında yayınlanan “Blind Signatures for Untraceable Payments (Takip Edilemeyen Ödemeler için Kör İmzalar)” isimli makalesi ile David Chaum tarafından atılmıştır. Sonraki yıllarda da bu konudaki çalışmalarını sürdürerek (Bknz. Chaum, 1985 ve 1992) dünya ekonomisinde kullanılabilmesi için fiziksel para birimini taklit edecek bir para simgesinin yaratılması için ve en önemlisi güvenli bir şekilde anonim ödemeleri mümkün kılacak gizlilik özelliğine sahip bir “elektronik para” kavramının geliştirilmesine katkı sağlamıştır (Peters vd., 2015, s.4).

Chaum (1983, s.199); hem dijital para transferinin en önemli risklerinden dijital imzaların kopyalanması yoluyla ortaya çıkan çift harcama sorununa hem de yapmış olduğu çeşitli ödeme işlemlerinin miktarı, zamanı, alacaklısı gibi kişisel bilgileri üzerinden kullanıcının ilişkileri, yaşam tarzı, nerede olduğu gibi bilgilere 3. tarafların erişebilmesi sorununa çözüm getirmiştir. Bu çözümü; güvenilir bir üçüncü taraf (Trusted Third Party -TTP) olan bankayı, kör imza yani kriptografik dijital imza<sup>28</sup> kullanarak e-para işlemlerinin doğrulamasını yapması için sisteme dahil etmesiyle sağlamıştır (Yanar vd. 2022 s.34). Bu dijital imza ile bankalar; ödemeyi veya miktarı gönderene doğru geriye takip edememekte ve böylece anonimlik sağlanmaktadır. Ayrıca ödemenin veya miktarın hangi hesaba yatırıldığının da doğrulanmasına imkân tanınmaktadır. Eğer ki farklı bir hesaba ödeme yatırılmışsa bu durum dolandırıcılığın kanıtı olmaktadır (Chaum, 1983, s.203).

David Chaum; 1989 yılında, kör imza teknolojisine dayalı ve kişisel gizliliği koruyarak çevrimiçi ödemelerin izlenememesini sağlayan elektronik ödeme şirketi DigiCash'i kurmuştur. DigiCash'in kurulduğu Amsterdam'daki merkez bankasıyla ortaya çıkan sorunlar nedeniyle, bu tür bir para biriminin yalnızca bankalara bir ürün olarak satılmasına karar verilmiştir. Bu e-cash girişimi çok şey vaat etmesine rağmen daha çok siyasi ve işle ilgili

---

<sup>28</sup> “Dijital imza” hakkında detaylı bilgi için bknz. s.36.



sorunlar nedeniyle benimsenememiştir (Peters vd., 2015, s.4). Dahası çevrimiçi teknolojinin henüz yaygınlaşmadığı bir dönemde ve yüksek kurulum maliyetleri nedeniyle kullanıcı sayısının azalması, ticari açıdan başarısız olmasına sebep olmuş ve Digicash 1998 yılında iflas etmiştir. Ancak bu girişim, kripto paraların günümüzdeki örneklerinin gelişimine öncülük etmiş ve onların temelini oluşturmuştur (Yanar vd., 2022, s.34).

DigiCash'in iflasından sonra, kripto para birimi olmamakla birlikte, First Virtual ve PayPal gibi elektronik ödeme sistemleri tarafından boşluk doldurulmaya çalışılmıştır. PayPal gerçek para birimine dayalı, sınırlı ve devletlerin yasal düzenlemelerine uyumlu bir dijital para olarak hizmet vermektedir (Çarkacıoğlu, 2016, s.7). Buna karşılık, kara para aklama ve suç girişimleriyle ilgili faaliyetler için bu hizmetleri almış olabilecek bazı müşterilerin şüpheli doğası nedeniyle Liberty Reserve ve e-gold gibi başarısızlıkla sonuçlanan örnekleri de bulunmaktadır (Peters vd., 2015, s.4).

Dijital paranın gelişimine baktığımızda; Chaum'un önerdiği e-cash ödeme sisteminde ilk kez kripto para birimi kullanılmıştır. Ancak bu sistem, merkezi bir otorite ve denetim birimine dayandığından (Tetik vd., 2020 s.17), teorik altyapısı sanal para temelli olan günümüz kripto para sistemlerinden farklıdır.

Bir diğer dijital para türü olan sanal para, elektronik paradan farklı olarak fiziksel bir gerçekliği temsil etmemektedir (Çarkacıoğlu, 2016, s.7). Avrupa Bankacılık Otoritesi sanal parayı; *“Bir merkez bankası veya kamu otoritesi tarafından ihraç edilmeyen ya da fiat paraya bağlı olmayan, ancak gerçek veya tüzel kişiler tarafından bir ödeme aracı olarak kabul edilen ve elektronik olarak aktarılabilen, saklanabilen veya ticareti yapılabilen bir değer dijital temsildir.”* şeklinde tanımlamıştır (EBA, 2014, s.5).

Mali hukuk teorisine göre; para birimi (currency), paranın (money) belirli bir şekli veya türüdür. Bu anlamda para ekonomik bir kategori iken para birimi yasal bir kategoridir. Dolayısıyla paranın bir para birimi olarak etiketlenebilmesi için, paranın şeklini belirleyen ve paranın kullanılacağı kesin koşulları belirleyen bir otorite (genellikle devlet) tarafından bu şekilde kabul edilmesi gerekmektedir (Vondráčková, 2016, s.1). Bu açıdan değerlendirildiğinde fiat paranın dijital temsili olan elektronik paranın aksine sanal para birimleri, devlet tarafından tanınmadığından gerçek anlamda bir para birimi olmayıp, temel

para birimi karakteristiklerini yerine getirmemektedir (Chuen, 2015, s. 269; Vondráčková, 2016, s.1).

Sanal paralar, yönetim otoritesi ve denetim merkezi olup olmamasına göre “Merkezileştirilmiş (Centralised Virtual)” ve “Merkeziyetsiz (Decentralised Virtual)” olmak üzere ikiye ayrılmaktadır. Buna göre; merkezileştirilmiş sanal paralarda, sanal paranın ihraç edilmesi, kullanım kurallarının belirlenmesi, kayıt altına alınması merkezi bir otorite tarafından yapılmaktadır. Paranın kontrol ve denetimi, hatta paranın dolanımdan geri çekilmesi yetkisi de merkeze aittir (Karacan vd., 2021, s.15). Merkeziyetsiz (Decentralised Virtual) sanal paralarda ise herhangi bir yönetim otoritesi ve kontrol merkezi bulunmamaktadır. Bu para mekanizması; para transferinin katılımcılar arasında doğrudan, aracısız sağlandığı açık kaynaklı, matematik temelli, eşler arası (Karacan vd., 2021, s.16) bir yapıya dayanmaktadır. Söz konusu sistemin işleyişini yöneten ve sistem katılımcılarının işlemlerini doğrulayan iç protokoller, merkez bankasının rolünü üstlenmektedir (Üzer, 2017, s.17).

Sanal paralar, gerçek paralara (fiat para) çevrilebilir çevrilememelerine göre de bir başka sınıflandırmaya tabi tutularak “Kapalı/Çevrilemez (Closed/Non-convertible)” ve “Açık/Çevrilebilir (Open/Convertible)” olarak ikiye ayrılmaktadır.

Kapalı/Çevrilemez sanal paranın reel ekonomiyle neredeyse hiçbir bağlantısı bulunmamaktadır. Aynı zamanda “sadece oyun içi para” olarak adlandırılmaktadır. Kullanıcılar genellikle bir abonelik ücreti ödemekte ve ardından çevrimiçi performanslarına göre sanal para kazanmaktadırlar. Sanal para birimi yalnızca sanal topluluk içinde sunulan sanal mal ve hizmetleri satın alarak harcanabilmekte ve sanal topluluk dışında alınıp satılamamaktadır (ECB, 2012, s.13).

Sanal para birimleri, 1990’larda tipik olarak yine merkezi olan ancak en azından ilk biçimlerinde çevrimiçi mesajlaşma ve sanal oyun ortamlarında kullanılmak üzere sınırlandırılmış kapalı/çevrilemez para birimleri olarak ortaya çıkmıştır. İlk örneklerden biri, Tencent’in çevrimiçi mesajlaşma platformunda kullanılmak üzere Çin’deki tuğla ve harç dükkanlarından satın alınabilen Q coin’dir. Günümüzde ise çok oyunculu çevrimiçi oyunlarda (örneğin World of Warcraft’ta WoW Gold, Entropia Universe/Project Entropia’da

PED) veya yaşam simülasyonu oyunlarında (örneğin Second Life’da Linden doları) yaygın olarak kullanılmaktadır (Peters vd., 2015, s.4).

Açık/Çevrilebilir sanal para ise fiat para cinsinden değeri olan ve fiat paraya çevrilebilen paradır. Ayrıca bu tip sanal para gerçek dünyada da mal ve hizmet bedelinin ödenmesinde kullanılabilir (Karacan vd., 2021, s.16). Çevrilebilir sanal paralar “tek yönlü (unidirectional)” ve “çift yönlü (bidirectional)” olmak üzere iki türde olabilmektedir. Tek yönlü sanal para, belirli bir döviz kuru üzerinden doğrudan gerçek para birimi kullanılarak satın alınabilmekte, ancak orijinal para birimine geri dönüştürülememektedir. Sanal ve bazen gerçek mal ve hizmet satın almada tek yönlü sanal para kullanılabilir. Facebook’un sanal parası Facebook Credits ve Nintendo’nun Nintendo Points’i bu tip sanal paralara örnektir (ECB, 2012, s.14). Çift yönlü sanal para ise kullanıcılar kendi para birimleriyle döviz kurlarına göre sanal para alıp satabilirler. Sanal para birimi, gerçek dünya ile birlikte çalışabilirliği açısından diğer konvertible para birimlerine benzemektedir. Hem sanal hem de gerçek mal ve hizmet satın almada çift yönlü sanal para kullanılabilir (Üzer, 2017, s.15). İlk kripto para birimi Bitcoin bu çift yönlü sanal paralara örnektir.

Özetleyecek olursak; Şekil 2.17’de de gösterildiği üzere günümüzdeki anlamı ile kripto para, merkeziyetsiz ve çift yönlü çevrilebilme özelliklerine sahip bir sanal para türüdür. Bu tür bir sanal para biriminin teorik alt yapısı, Chaum’un 1983 yılında ortaya koyduğu merkezi bir yapıya dayalı kör imzalı e-nakit (e-cash) sisteminin, merkeziyetsiz yapıya dayalı bir versiyonu olan Wei Dai’nin 1998 yılında önerdiği “b-para (b-money)” sistemidir. Anonim ve merkezi olmayan bir e- nakit sistemi olan b-money sistemi ile; izlenebilir olmayan dijital takma isimlere (pseudonyms – yani açık anahtarlar) sahip bireylerden oluşan bir topluluğun kendi aralarında b-para kullanarak ödemeler yapabilmesi ve grup dışından hiçbir yardım almadan kendi aralarındaki anlaşmaları yerine getirebilmeleri sağlanmaktadır (Tetik vd., 2020, s.16). B-para sisteminin keşfedilmesi kriptografik yöntemlerin kullanıldığı merkeziyetsiz elektronik ödeme sistemlerine temel olmuştur.

Bir başka merkeziyetsiz sanal para önerisi ise, Nick Szabo’dan 2005 yılında “Bitgold” ismi ile ortaya atılmıştır. Szabo; paranın değerinin üçüncü taraflara olan güvene bağlı oluşunun bir şekilde güvensizlikle sonuçlanmasının hırsızlık ve enflasyona yol açmasına karşı, merkeziyetsiz ve enflasyon direnci sağlayan bir para kavramı sunmuş ve Bitgold sisteminin işleyişini yedi adımda açıklamıştır (Szabo, 2005):

- a. Genel bir “zorluk dizisi” oluşturulur,
- b. Alice, iş kanıtı algoritmaları kullanılarak zorluk dizisinden bit dizisi hesaplar,
- c. Bu iş kanıtı zaman damgası ile imzalanır,
- d. Alice, zorluk dizisi ve zaman damgalı iş kanıtını dağıtılmış dijital imza zincirine ekler,
- e. Son oluşturulan bitgold dizisi, sonraki dize için zorluk dizisini sağlar,
- f. Bob; Alice’in bitgold sahipliğini, bitgold dijital imza zincirinden kontrol eder,
- g. Bob, belirli bir bitgold dizisi değerini denemek için iş kanıtı ve zaman damgasını kontrol eder ve doğrular.

Szabo (2005)'nın, merkeziyetsiz, çevrimiçi ve taklit edilemeyecek kadar maliyetli bitler oluşturabilen, benzeri görülmemiş bir güvenilirlikte saklanabilen ve aktarılabilen bir protokol olarak tanımladığı Bitgold sistemi, ne yazık ki hayata geçirilememiştir. Ancak bu sistem, kripto para birimi Bitcoin'in tasarımında önemli bir ilham kaynağı olmuştur. 2008 yılında Satoshi Nakamoto'nun önerdiği eşten eşe elektronik nakit ödeme sistemi “bitcoin” de günümüz kripto para birimlerinin teknik ve teknolojik altyapısını ortaya koymuştur.

Her ne kadar bankacılığın ve paranın gelişiminde teknoloji ve değişen ticaret yapısı itici güç olsa da kripto paraların ortaya çıkışıyla ilgili farklı bakış açıları da bulunmaktadır. Bunlardan biri, son finansal krizin merkez bankaları ve finans kurumlarına olan güveni sarsmasıdır. 2008'deki küresel finansal çalkantılar, dünya ekonomisinde derin izler bırakmıştır: ülke borsaları çökmüş, kredi derecelendirme kuruluşlarının güvenilirliği sorgulanmış, finans kuruluşları ve şirketler batma tehlikesiyle karşı karşıya kalmış ve büyük bankalar iflas etmiştir. Sonuç olarak ne yazık ki insanların finans sektörüne ve bankalara olan güvenleri zarar görmüştür. Finans piyasalarının bu çöküşünün ardından Bitcoin, geleneksel finansal sisteme ve rezerv para birimlerine alternatif bir çözüm olarak geliştirilmiştir (Dilek, 2018, s.10).

Daha önce de bahsedildiği üzere bitcoin kripto paraların öncüsüdür. Ancak "bitcoin" terimi sadece bir para birimini ifade etmekle kalmamakta, aynı zamanda üç farklı kavramı da içermektedir. İlk olarak, Bitcoin terimi, altta yatan blokzincir teknolojisi platformunu belirtmektedir. İkincisi, varlıkların blokzinciri üzerinde nasıl transfer edildiğini tanımlamak için temel blokzincir teknolojisine dayanan bir protokolü tanımlamaktadır. Son olarak ise, bitcoin, kripto para birimlerinin ilk ve en büyüğü olan dijital para birimini ifade etmektedir

(Swan, s.1). Bitcoin, büyük harfle (Bitcoin) yazıldığında ödeme sistemi ağı, küçük harfle (bitcoin) yazıldığında da kripto para birimini temsil etmektedir. Bitcoin para birimi olarak kullanıldığında genellikle "BTC" kısaltmasıyla veya “□” sembolü ile gösterilmektedir (Alıcı, 2021, s.10).

Resmi internet adresine göre bitcoin; para kavramının, belirli bir ülkede veya sosyo-ekonomik çerçevede mal ve hizmet alışverişi için kullanılan herhangi bir değer veya kaydolduğu düşüncesinden hareketle, para yaratımı ve transferini kontrol etmek için merkezi otoritelere güvenmek yerine kriptografi kullanmak fikri çerçevesinde tasarlanmıştır. Ve aşağıda maddeler halinde sıralanan özellikleri itibarıyla tanımlanmıştır ([https://en.bitcoin.it/wiki/Main\\_Page](https://en.bitcoin.it/wiki/Main_Page)) :

- a. Bitcoin, dünyanın herhangi bir yerindeki herhangi bir kişiye anında ödeme yapılmasını sağlayan merkezi olmayan bir dijital para birimidir.
- b. Bitcoin, para benzeri bir malın tüm özelliklerine sahiptir : Taşınabilir, Dayanıklı, Bölünebilir, Tanınabilir, Değiştirilebilir, Az Bulunur ve Taklit Edilmesi Zordur.
- c. Bitcoin’in depolama maliyeti yoktur. Miktarı ne olursa olsun fiziksel yer kaplamazlar.
- d. Bitcoin, merkezi otorite olmadan çalışan eşler arası (P2P) teknolojiyi kullanır. İşlem yönetimi ve para ihracı ağ tarafından kolektif olarak gerçekleştirilir.
- e. Bitcoin, basılamaz ya da değeri düşürülemez. Veri madenciliği ile üretilebilecek bitcoin sayısı 21 milyon adet ile sınırlıdır.
- f. Madencilerin buldukları her blok için kazandıkları ödül yani ürettikleri bitcoin miktarı “bitcoin üretim algoritması”na bağlıdır. Buna göre blok başına üretilen bitcoin sayısı, her 210.000 blokta bir ya da yaklaşık 4 yılda bir %50 azalacak diğer yandan blok üretme zorluk seviyesi<sup>29</sup> artırılacak şekilde ayarlanmıştır. Bu “Azalan Arz Algoritması” veya “Kontrollü Para Birimi Arzı”, altın gibi emtiaların çıkarılma hızına yakın olduğundan seçilmiştir. İlk blok 2009 yılında üretildiğinde, ödül 50 BTC idi. Ancak 20 Nisan 2024'te gerçekleşen dördüncü yarılamayla (halving) bu ödül 3,125 BTC'ye indirildi. Bu tarihte,

---

<sup>29</sup> “Zorluk seviyesi” hakkında detaylı bilgi için bkz. s.48.

dolaşımdaki toplam BTC miktarı yaklaşık olarak 19,7 milyon ve üretilen blok sayısı ise 840.000 adet olarak gerçekleşmiştir.

- g. Madencilere ödül olarak verilen Bitcoin'e ek olarak, işlem gönderen kullanıcılar tarafından işlem ücretleri de ödenmektedir. Bu ücret, bir madencinin işlemi bloğuna dahil etmesi için ikincil bir teşvik mekanizmasıdır. Yarılımlarla birlikte her blokta yaratılan yeni Bitcoin miktarı azaldıkça, işlem ücretleri madencilik gelirinin giderek daha büyük bir yüzdesini oluşturacaktır.

Herhangi bir işlemin yaratıcısının, işlem çıktılarının toplam değerini girdilerinin toplam değerinden daha az yapmayı seçtiği bir mekanizmada; aradaki fark, bu işlemi blokzincirine ilk koyan madenci tarafından işlem ücreti olarak tahsil edilmektedir. Şimdilik gönüllülük esasına dayanan işlem ücretleri, blok ödülü tükenmeye başladıkça zorunlu hale gelecektir. Ancak sistemin nasıl gelişeceği henüz tam olarak belli değildir (Narayanan vd., 2016, s.63).

- h. Bitcoin'in enflasyon oranı, sürekli bir düşüş eğilimindedir. Bu, BTC arzının azalmasıyla ilişkilidir. Her yarılamada, BTC yıllık enflasyon oranı düşmektedir. Nitekim 2013 yılında %12'lerden 2017 yılında %4'e, 2020 yılında %1,7'ye ve 2024 yılında ise %0,83'e kadar gerilemiştir ([https://bashco.github.io/Bitcoin\\_Monetary\\_Inflation/](https://bashco.github.io/Bitcoin_Monetary_Inflation/)). Enflasyon sıfıra indiğinde, yani daha fazla bitcoin üretilemez hale geldiğinde, madenciler yalnızca işlem ücretlerinden gelir elde edeceklerdir. Bu da madenciliği sürdürmeye teşvik edecektir.
- i. Yeni bitcoin üretilmesi için iş kanıtı bulmacasının çözülmesi, bulmacanın çözülebilmesi için de ileri düzeyde uzmanlık ve teknik altyapı gerekmektedir. Bitcoin blokzincir protokolünü kullanarak işlem veya ödeme yapmak isteyen, ancak bulmaca ile uğraşmak yani madencilik yapmak istemeyenler, Bitcoin satan web sitelerinden fiat para karşılığında bitcoin satın alabilmektedirler. Bitcoin'in satın alma değeri ise, ulusal para birimlerinin birbirleri karşısındaki döviz kuru gibi, piyasada arz ve talebe bağlı olarak belirlenmektedir (Eğilmez, 2017). Örneğin; 07.06.2024 tarihinde 1 BTC 69.403 USD (2.241.627 TL)'den işlem görmüştür (<https://www.binance.com/tr/price/bitcoin>). Satın alınan bitcoinler sanal cüzdanlarda saklanmakta ve buradan istenilen yere para transferi

yapılabilmektedir. Ancak bu transferin ne kadar, kime ve ne zaman yapıldığının takip edilmesi mümkün olmamaktadır (Eğilmez, 2013).

- j. Genel olarak bloğunu zincire ekleyen madencinin hak ettiği bitcoini harcayabilmesi için, en az 100 bloğun (10 dakika x 100 blok  $\cong$  17 saat) daha zincire eklenmesi gerekmektedir. Çünkü madencinin ürettiği blok yüksekliğinde, aynı anda başka bir madenci de blok üretebilir ve bu bloğun öksüz blok<sup>30</sup> olma riski bulunmaktadır. Ödülü sadece, bloğunu zincire başarılı ve geçerli bir şekilde ekleyebilen madenci kazanmaktadır (Çarkacıoğlu, 2016, s.45).
- k. Bazı bitcoinlerin ise harcanmasını engelleyen teknik özellikler bulunmaktadır. Örneğin Genesis bloğunda yer alan ilk 50 BTC, söz konusu işlem global veri tabanında olmadığı için harcanmamaktadır. Diğer yandan işlemin, ona ait özel anahtarının gerçekte bilinmediği veya geçerli aralıkta bulunmadığı bir adrese kasıtlı olarak gönderilmesi durumunda da bitcoinlerin harcanması imkânsız hale gelmektedir.
- l. Bitcoinin bir başka harcanamama durumu da harcanmaları için gereken koşullar artık bilinmiyorsa ortaya çıkmaktadır. Örneğin, işleme ilişkin özel anahtarın kaybolması veya unutulması halinde eşleşen bir özel anahtarın rastgele bulunması olasılığı genellikle imkânsız kabul edileceğinden, bu bitcoin de kayıp olarak kabul edilmektedir.
- m. Bitcoin'in korunması ve saklanması kolaydır. Bir telefonda, bilgisayarda, şifrelenmiş olarak kâğıt bir yedekte ya da ezberlenmiş olarak saklanabilmektedir.
- n. Bitcoin'in karşı taraf riski bulunmamaktadır. Bir bitcoin cüzdanının tohum cümlesi gizli tutulur ve işlem yeterli onayı alırsa ne sebeple olursa olsun hiç kimsenin bitcoini ele geçirme ihtimali olmayacaktır.
- o. Bitcoin, çoklu imza (multisignature) ile bölünmüş mülkiyet altında olabilmektedir. Örneğin, 3'te 2 çoklu imza modelinde, herhangi iki tarafın parayı harcayabilmesi için üç özel anahtarın bilinmesi yeterli olmaktadır. Bu üç anahtar farklı yerlerde saklanabilmekte, birden fazla kişi tarafından tutulabilmekte veya birden çok lokasyonda olabilmektedir.

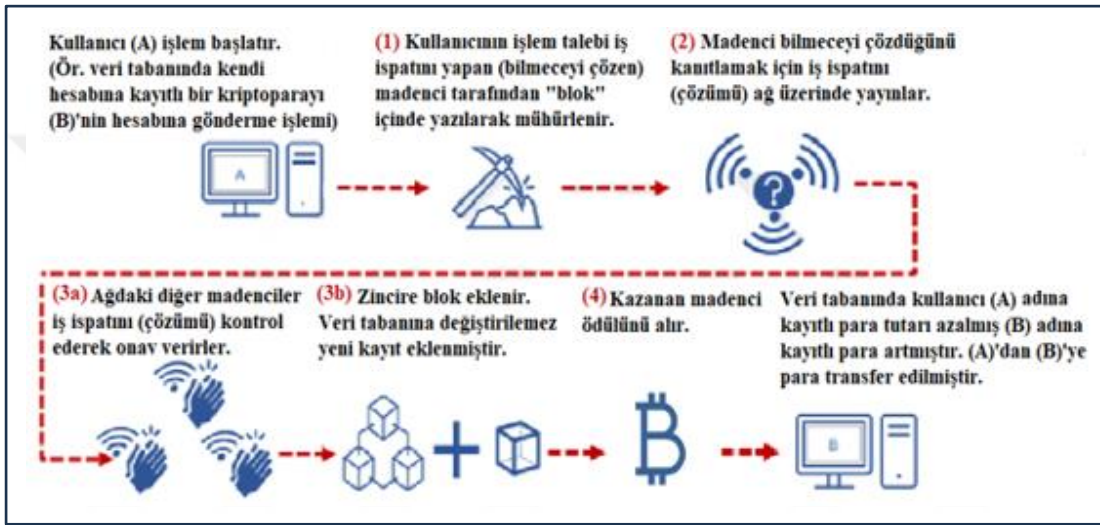
---

<sup>30</sup> “Öksüz blok” hakkında detaylı bilgi için bkz. s.51.

Diğer varlıklar, örneğin altın paralar, bu tür bir çoklu imza sistemini kullanarak tutulamamaktadır.

### ***İş kanıtı (POW) mutabakat algoritmasının avantaj ve dezavantajları***

Bu bölümde detaylı bir şekilde ele alınan iş kanıtı mutabakat süreci Şekil 2.18’de gösterildiği üzere bir grafik yardımıyla özetlenmiştir. Teorik olarak ortaya konulan bu sürecin uygulanması aşamasında yani veri madenciliği sırasında bazı avantaj ve dezavantajlar ile karşılaşilmektedir.



**Şekil 2.18:** İş Kanıtı Mutabakat Algoritması.

[Aslaner, 2022, s.62]'dan uyarlanmıştır

Dağıtık bir ağ sisteminde, veri güvenliği ve bütünlüğü bozulmadan sisteme yeni veri girişinin sağlanması işlemini, sistemdeki düğümlerden rastgele biri gerçekleştirmektedir. Blokzincir teknolojisinde bunun karşılığı madencinin zincire yeni blok eklemesidir. Hangi madencinin bu işlemi gerçekleştireceği ve gerçekleştirmesi için ne gibi nedeni olduğu sorunu da PoW mutabakat algoritması ile çözülmüştür. Buna göre işlem gücü kullanarak ve enerji sarfederek en önce bloğun özel nonce değerini bulan ve nonce değerinin doğruluğu konusunda diğer madencilerle mutabakat sağlayan madenci zincire blok ekleyebilmektedir. Bunun karşılığında da belirli miktarda itibari para birimlerine çevrilebilen kripto para bitcoin üreterek kazanmaktadır.

Dolayısıyla PoW, sadece teşvik sistemi ile üretilen bitcoini kazanacak olan madenci seçiminin rastlantısal olmasını ve sistemde hiçbir madencinin tekel davranamamasını



sağlamaktadır (Ünsal vd., 2018, s.56). Bu özelliği dolayısıyla blokzincir teknolojisinin temelini oluşturmaktadır.

Ayrıca bir işlemin geçerliliği ve doğruluğu ağın %51'inin kabulüne bağlı olduğundan verilerin güvenliği açısından da taraflara fazlasıyla güvence sağlamaktadır (Deloitte&TÜSİAD, 2018, s.26). Böylece dijital varlık sahiplerinin aynı varlığı birden fazla kez harcaması veya transfer etmesi girişimi olan “Çifte Harcama Saldırısı”na da çözüm getirmektedir. Blokzincir ağında kaydedilen tüm işlemler birbirine dijital imzalar ile bağlandığından ve her bir yeni işlemin ağın çoğunluğunun onayı ile eklenebilmesi sayesinde bir işlem göndericisinin sadece sahip olduğu bitcoinleri kullandığından emin olunmaktadır (Yurdabak, 2022, s.11).

Aynı zamanda PoW; kötü niyetli bir madencinin ağdaki toplam madencilik gücünün çoğunluğunu ele geçirme saldırısı olan “%51 saldırısı”na karşı da dirençlidir. Ağın çoğunluğunun ele geçirilebilmesi için zincirdeki tüm blokların değiştirilmesi ve sahte çatalın orijinal çatal uzunluğunu geçmesi gerekmektedir. Ancak bu manipülasyon teoride gerçekleştirilebilir gibi görünse de sadece bir blok eklemek için bile gereken yüksek işlemci gücü, enerji ve zaman (10 dakikada bir blok eklenebilmesi, zorluk seviyesi, blok boyutu, donanım ihtiyacı vb. gibi) dikkate alındığında tüm ağın yeniden düzenlenmesi için gereken koşulların sağlanması uygulamada mümkün olamamaktadır. Bunun yanı sıra; saldırganın manipülasyondan beklediği getiri, başarı için katlandığı maliyetten fazla olmalıdır. PoW mekanizması ise bunu karşılamadığından, *“saldırgan, oyunu kuralına göre oynamayı, sisteme ve kendi servetinin geçerliliğine zarar vermekten daha karlı bulacaktır* (Nakamoto, s.4).”

Diğer yandan PoW; hesaplama açısından zor bir bulmacanın kullanılması, bir saldırganın etki kazanmak ve kontrol uygulamak için birçok düğüm oluşturabildiği (yani birden fazla sahte kimlik oluşturduğu) bir bilgisayar güvenliği saldırısı olan "Sybil Saldırısı" ile mücadeleye de yardımcı olmaktadır. Bunu; genellikle maliyetsiz olan ağ kimliklerine karşı, bir piyango sistemiyle (en güçlü donanım olasılığı artırır ancak garanti etmez) harmanlanmış hesaplama (bilgisayar) gücü miktarı (paraya mal olan donanım) ile sağlamaktadır (Yaga vd., 2018, s.21).

Aynı zamanda ağdaki gecikmelere, düğüm hatalarına, bozuk ve düzensiz verilere karşı da bir kontrol ve regülasyon mekanizması olarak işlev görmek ve zincire her yeni eklenen bloktaki verilerin benzersiz ve tek olmasını sağlamaktadır (Baliga, 2017).

Dolayısıyla PoW veri madenciliğinin avantajlarını maddeler halinde aşağıdaki gibi özetleyebiliriz:

- a. İş kanıtı üretme süreci yüksek hesaplama gücüne ve enerjiye ihtiyaç duyduğundan ağ üzerinde karşılaşılabilecek güvenlik problemleri (dijital bilgilerin kopyalanması, verilerin değiştirilmesi, çifte harcama saldırısı, Sybil saldırısı, %51 saldırısı, vb. gibi) engellenebilmektedir.
- b. Yeterli donanıma sahip olunması halinde isteyen herkes madencilik yapabilir. Böylece ağın dağıtık yapısı muhafaza edilebilmektedir.
- c. İşlemler şifrelenmediğinden bloğa erişim sağlayabilen herkes verileri görebilir. Bu durum madencilik sürecinin şeffaf ve herkes tarafından denetlenebilir olmasını sağlamaktadır. Herhangi bir hile ya da yanlışlık kolayca tespit edilebilmektedir.
- d. İşlemler ağın çoğunluğunun mutabakatı ile kaydedildiğinden ve ağ katılımcılarının her biri tüm işlemlerin bir örneğine sahip olduğundan, veriler değiştirilememektedir.
- e. Madenciler, ağdaki işlem verilerini doğrulama yoluyla ek kazanç sağlayabilirler. Bu yolla ağ güvende tutulmakta ve katılım teşvik edilmektedir.

PoW algoritmasının dezavantajlarına değinecek olursak; öncelikle mekanizmanın temel unsuru olan iş kanıtı üretebilmek için gerekli olan işlemci gücü ve enerjinin elde edilmesinde kullanılan araçların ve sistemin dönüşümünden bahsetmemiz gerekmektedir. Bu bağlamda bitcoin'in ilk yıllarını incelediğimizde, madencilik için gereken tek şeyin Microsoft Outlook programını kişisel bilgisayarlara indirip çalıştırmak olduğunu görmekteyiz. Ancak günümüzde, madencilik işlemi giderek zorlaşmış ve daha az karlı hale gelmiştir. Artan işlem karmaşıklığı ve kullanıcı sayısı, bireyler ve kurumları daha yüksek kazanç sağlamak amacıyla özel olarak tasarlanmış depolarda, geniş ve pahalı Bitcoin madencilik makinelerine yatırım yapmaya doğru yöneltmiştir (Dilek, 2018, s.18). Bu anlamda iş kanıtı mutabakat süreci yani bitcoin madenciliği Şekil 2.19'da görüldüğü üzere; CPU'lardan grafik kartlarına dayalı GPU (Graphics Processing Unit – Grafik İşlemci Birimi)'lara, FPGA (Field Programmable Gate Arrays - Alan Programlanabilir Kapı Dizisi)'lara ve şimdilerde özel tasarlanmış tümleşik

devreler olan ASIC (Application-Specific Integrated Circuit - Uygulamaya Özgü Entegre Devre)'lere doğru bir evrim göstermiştir.

Diğer yandan; pahalı donanımlara yatırım yapabilecek kaynağı olmayan küçük katılımcılar için güçlerini birleştirdikleri ve blok oluşturarak ödül kazanma olasılıklarını artırdıkları “havuz madenciliği (pool mining)” ikinci bir seçenek olarak sisteme dahil olmuştur (Gönen vd., 2021, s.68). Havuz madenciliğinde, her bir madenci nonce değerini tahmin etmeye çalışmak yerine, bir grup halinde toplanmakta, daha sonra bir havuz operatörüne oy vermekte ve nonce'yi birlikte bulmaktadırlar. Bu birliktelik, ödül kazanma ihtimalini çok daha kolaylaştırmaktadır. Ödüller, coin-base adı verilen bir yerde saklanmaktadır. Böylece daha sonra bu havuza katılan her madenci, her biri için eşit olan teşviklerini buradan alabilmektedir (Nguyen vd., 2018, s.108).



Şekil 2.19: PoW Madenciliğinin Evrimi.

[Narayanan vd., 2016, s.145]

İş Kanıtı mutabakat mekanizmasında gerçekleşen söz konusu gelişmelerle birlikte PoW veri madenciliğinde karşılaşılan dezavantajları aşağıdaki gibi sıralayabiliriz:

- Bir bloğun onaylanması için belirli bir süre gerektiğinden ağda zincire eklenebilecek blok sayısı az ve işlem süresi uzundur. Bu nedenle PoW’da verimlilik düşüktür (Gönen vd., 2021, s.65).
- Verimliliği artırma amacıyla blok boyutunun genişletilmesi ve/veya blok oluşturma aralığının kısaltılması gibi önlemler çatallanma sıklığını artırarak güvenlik risklerine maruz kalma olasılığını artırabilmektedir (Gönen vd., 2021, s.65).
- Madencilikte, kullanıcı sayılarının ve dolayısıyla zorluk seviyesinin giderek artması ile işlemci gücü ve enerji ihtiyacı katlanarak artmaktadır. Bu ihtiyacı karşılamak adına tüketilen ülkelerin neredeyse yıllık elektrik sarf miktarına denk enerji miktarı, geliştirilen yeni donanımlar (GPU – FPGA) ve sistemler (ASIC) madencilik faaliyetine ilişkin genel maliyetleri yükseltmektedir.

- d. Madencilik faaliyetleri, yüksek enerji tüketimi nedeniyle elektriğin yanı sıra alternatif kaynaklara (kömür vb. gibi) da yönelinmesi ile hem doğal kaynakların aşırı kullanımı hem de karbondioksit emisyonunun küresel ısınmaya sebep olması dolayısıyla ekolojik dengenin bozulması gibi birçok olumsuz çevresel etkiye de sebep olabilmektedir (Dilek, 2018, s.21).
- e. Bitcoin'in itibari paraya dönüştürülebilmesi cazibe yarattığından madenciler daha çok blok üretmek amacıyla donanımına daha çok yatırım yapmaktadırlar. Bu durum da görece daha fazla donanım gücüne sahip olanların zincirde daha fazla etkin olmalarına ve daha fazla bitcoin kazanmalarını sağlamaktayken, özel donanımlara yatırım yapamayanları sistem dışına itmektedir. Sonuç olarak madencilik için özel olarak tasarlanmış ASIC cihazları gibi yüksek performanslı donanımlar ağda sadece güçlü katılımcıların etkinliği doğrultusunda madencilik faaliyetlerinde merkezileşme riskini ortaya çıkarmaktadır (Gönen vd., 2021, s.67).
- f. Havuz madenciliği şeklindeki madencilik grubu ile küçük katılımcılar sisteme dahil ediliyor olsa da bu tür madencilik ile blok üretiminin belirli havuzların tekeline bırakılması riski ortaya çıkmaktadır (Gönen vd., 2021, s.69). Bu durum da ağı %51 saldırı riskine açık hale getirmektedir (Nguyen, vd., 2018, s.108).
- g. Son olarak bitcoin ödül değerlerinin yarılamalar ile düşmesi, madenci sayılarının azalmasına ve dolayısıyla ağın hesaplama gücünün düşmesine neden olabilecektir. Bu durumun kullanıcıların sisteme olan güvenlerinin sarsılması riskine yol açabileceği eleştirilerinde de bulunmaktadır (Kardaş, 2019, s.488).

PoW algoritması blokzincir teknolojisinde ilk uygulanan ve en yaygın kullanılan mutabakat mekanizmasıdır. Bitcoin kripto parası dışında Bitcoin Cash, Litecoin, NameCoin, Dogecoin ve Monero gibi kripto paralarda da PoW algoritması kullanılmaktadır (Baliaga, 2017, s.4). Ancak yukarıda açıklanan söz konusu dezavantajlarına çözüm üretmek amacıyla alternatif mutabakat algoritmaları da geliştirilmiştir.

### 2.3.4.3 Hisse kanıtı (Proof of stake - POS)

Hisse Kanıtı kavramı, ilk olarak 2011 yılında bitcoin forumu [bitcointalk.org](http://bitcointalk.org)'ta QuantumMechanic takma isimli bir kullanıcı tarafından Nakamoto'nun PoW'u yerine bir seçenek olarak sunulmuştur (Gönen vd., 2021, s.70) Resmi bir alternatif mutabakat protokolü olarak ise, Sunny King ve Scott Nadal tarafından “PPCoin: Peer-to-Peer Cryptocurrency with Proof-of-Stake (PPCoin: Hisse Kanıtı ile Eşler Arası Kripto Para Birimi)” isimli makale ile önerilmiş ve 2012 yılında Peercoin (Peer-to-Peer Coin / PP Coin / PPC)’de ilk kez uygulanmıştır. Hisse kanıtı tabanlı bu blokzincirinde, ağ üzerinde etki sahibi olan, yeni bloklar üreten ve zinciri güvence altına alan kişiler “coin” sahipleridir. Peercoin'in paydaşları, hissedarların halka açık bir şirkete birlikte sahip olmalarına benzer şekilde, blokzinciri ağına etkin bir şekilde birlikte sahip olmaktadırlar (<https://www.peercoin.net/university/#/9-peercoin-proof-of-stake-consensus>). Mekanizma; bir sonraki bloğu üretecek liderin, ağdaki hisse sahipleri arasından hisselerinin miktarıyla orantılı olmak üzere rastgele belirlenmesi yoluyla işlemektedir. Yani daha fazla hisseye sahip olanların, daha fazla bilet elde ettiği bir piyango çekilişi ile lider belirlenmektedir (Gönen vd., 2021, s.70).

PoS, PoW'un yüksek enerji ve işlemci gücü sarfına çözüm olarak sürdürülebilir bir sistem önermekte ve bir kullanıcı sisteme ne kadar çok hisse yatırır, sistemin başarılı olmasını isteme olasılığının o kadar artacağı ve sistemi yıkma olasılığının o kadar azalacağı fikrine dayanmaktadır (Yaga vd., 2018, s.21).

King ve Nadal'ın hibrit PoS tasarımında, iş kanıtının esas olarak ilk para basımını sağladığı ve sonrasında uzun vadede PoW'a ihtiyaç duyulmadığı belirtilmiştir. Dolayısıyla ağın güvenliği enerji tüketimine bağlı olmamakta böylece enerji açısından verimli ve maliyet açısından daha rekabetçi bir eşler arası kripto para birimi sağlanmaktadır (King vd., 2012, s.1). PoW'da blok üreticilerine, madenci yerine “minter (para basan)”denilirken; blok üreten minter'ın seçimi, hash gücü yerine “para yaşı (coin age)”na dayanmaktadır (<https://www.peercoin.net/university/#/9-peercoin-proof-of-stake-consensus>). Para yaşı; para miktarının, elde tutma süresi ile çarpımıdır. Örneğin; (B), (A)'dan 10 coin aldıysa ve 90 gün boyunca elinde tuttuysa, (B) 900 coin-gün para yaşı biriktirmiş olacaktır. Ayrıca; (B), (A)'dan aldığı 10 coini harcadığında, (B)'nin bu 10 coinle biriktirdiği jeton yaşı da

tüketilmiş olmaktadır. Bu sistemde coin yaşının hesaplanması için her bir işlemde, işlem zaman damgası bulunmaktadır (King vd., 2012, s.1).

Blokzincir ağının hisse kanıtı mekanizmasını nasıl kullandığına ilişkin literatürde farklı yöntemler bulunmaktadır. Temel olarak ise dört yaklaşımdan bahsedebiliriz: i) hisseli kullanıcıların rastgele seçimi, ii) çok turlu oylama, iii) coin yaşlandırma sistemleri ve iv) temsili sistemler. Ancak hangi yaklaşım olursa olsun, daha fazla hisseye sahip kullanıcıların yeni blok yayınlama olasılığı daha yüksektir (Yaga vd., 2018, s.21). Bu durum da ağda zengin olanların sadece etkili olması dolayısıyla merkezileşme riski taşıması açısından eleştirilmektedir. Peercoin dışında PoS mutabakat algoritmasını uygulayan kripto paralara BitShares, Steem, Blackcoin, NXT, Cardano ve Algorand'ı örnek verebiliriz. Ethereum ağı da Ethereum 2.0 (Casper uygulamasına)'a geçişiyle birlikte blokzincirinde PoS uygulamaya başlamıştır (<https://bilgiplatformu.btcturk.com/blokzinciri/proof-of-stake-hisse-kaniti-nedir-nasil-calisir/>).

#### **2.3.4.4 Pratik bizans hata toleransı (Practical Byzantine fault tolerance- PBFT)**

1999 yılında Miguel Castro ve Barbara Liskov tarafından aynı isimli makale ile önerilen Pratik Bizans Hata Toleransı algoritması, Bizans hataları karşısında uzlaşa sağlamaya yönelik bir çoğaltma (replikasyon) algoritması olup ilk pratik çözüm örneklerinden biridir (Baliga, 2017, s.12). Castro ve Liskov; PBFT algoritmasını, NFS (Network File System – Ağ Dosya Sistemi) üzerinde uygulayarak standart çoğaltılmamış NFS'den %3 daha yavaş işlem göstererek eş zamansız ağlarda (asenكرون) Bizans hatalarına karşı durum makinesi çoğaltma protokolü ile etkili bir çözüm sunduklarını ifade etmişlerdir (Castro vd., 1999, s.1).

Bizans hata toleransı (BFT); Bizans generalleri probleminin<sup>31</sup> yarattığı çeşitli arıza türlerine karşı direnç sağlayabilen bir sistemin özelliğidir (<https://academy.binance.com/tr/articles/byzantine-fault-tolerance-explained>) ve dağıtık bir ağda, kötü niyetli veya yanıltıcı düğümlerin varlığında dahi güvenilir şekilde iletişim kurabilen iki düğümün bir mutabakata varması anlamına gelmektedir (Monrat vd., 2019, s.8).

---

<sup>31</sup> “Bizans Generalleri Problemi” hakkında detaylı bilgi için bkz. s.41.

PBFT ise BFT sađlamanın Pow ve PoS'dan farklı bir yaklaşımıdır ve bazı düğümlerin dürüst davranmadığı veya hatalı olduđu varsayımı ile mutabakatın, ađdaki belirlenmiş güvenilir düğümler üzerinden sađlanmasına yönelik tasarlanmıştır. Bu düğümler, bir lider ve yedekler olarak hareket etmektedirler. Lider düğüm; işlem talebi aldıđında, yedekleri bu konuda bilgilendirerek talebi işlemekte ve ardından talep sahibine sonuçlar hakkında bilgilendirmede bulunmaktadır. Talep sahibi de yedeklerden gelen yanıtların, liderin bildirdiğı sonuçlar ile birebir aynı olup olmadığını karşılaştırmaktadır. Eğer bir karar alınmışsa; bu durumda, imzalı mesaj kaynağı ve mesaj bütünlüğünün kanıtlanması için düğümler birbirleriyle iletişim kurmuş ve çoğunluk oyu sađlanmış demektir (Monrat vd., 2019, s.8).

Bu mekanizmada; her turda yeni bir blok belirlenmekte ve bazı kurallara göre işlem sıralamasından sorumlu bir birinci seçilmektedir. Genel süreç üç aşamaya ayrılmaktadır: ön hazırlık, hazırlık ve onay. Her aşamada bir düğüm, tüm düğümlerin 2/3'ünden fazlasından oy almışsa bir sonraki aşamaya geçmektedir. Dolayısıyla PBFT'de her düğümün, ađ tarafından bilinmesi gerekmektedir (Zheng vd., 2017, s.560). Böylece 1/3 kötü niyetli Bizans düğümlerin varlığına rağmen mekanizma verimli çalışmış olmaktadır (Monrat vd., 2019, s.8). Ancak replika (düğüm) sayısının artması mesajlaşma ek yükünü önemli ölçüde arttırmakta olduğundan  $n < 20$ 'nin altındaki küçük gruplarda verimliliğı daha yüksektir (Baliga, 2017, s.12).

IBM, Intel gibi büyük firmaların verdiğı destek ile Linux Foundation önderliğinde, blokzincir teknolojisini günlük uygulamalara entegre etmek amacıyla geliştirilen açık kaynak kodlu bir blokzincir projesi olan (Gönen vd., 2021, s.83) Hyperledger Fabric, mutabakat algoritması olarak PBFT'yi kullanmaktadır (Zheng vd., 2017, s.560).

#### **2.3.4.5 Mutabakat algoritmalarının karşılaştırması**

Mutabakat algoritmaları bu bölümde detaylı bir şekilde açıklandığı üzere, blokzincir teknolojisinin karakteristik bileşenidir ve Bizans hatalarını bertaraf ederek dağıtık defterde yer alan kayıtların tüm kopyalarının güncellenmesini yani tüm düğümlerde aynı olmasını sađlamaktadır. Mutabakat algoritmalarının; düğümlerin ortak karar almasında, protokollerin çeşitli özellikleri (işlemci gücü, kripto para miktarı, depolama alanı, kullanıcı kimliğı, vb. gibi) ve yetkinliklerine göre farklı düzeyde söz hakkı almasına dayanan bir işleyiş mekanizması bulunmaktadır. Buna göre mutabakat algoritmaları, yetmişten fazla bilinen

türde uygulanmaktadır (Dursun, 2020, s.13). En yaygın kullanılan PoW, PoS ve PBHT bu çalışmada detaylı bir şekilde anlatılmıştır. Hangi mutabakat protokolünün uygulanacağı ise seçilen blokzincir türüne<sup>32</sup> bağlıdır. Açık blokzincirlerde, yüksek risk nedeniyle genellikle maliyetli olan PoW gibi güçlü algoritmalar kullanılmaktayken izinli blokzincirlerde, kullanıcıların daha tanıdık olması ve düğümlerin daha kontrollü çalışma ortamı sebebiyle genellikle BFT temelli mutabakat yöntemlerinin versiyonları tercih edilmektedir. Ayrıca birden fazla algoritma türünün birlikte kullanıldığı hibrit mutabakat algoritmaları da bulunmaktadır. Bunlardan en yaygın kullanılanları, PoW ve PoS algoritmalarının birlikte kullanıldığı modellerdir (Bingöl, 2020, s.41).

Bu çalışmada üzerinde durulan üç yöntem olan PoW, PoS ve PBHT'nin benzerlik ve farklılıkları aşağıdaki Tablo 2.6'da karşılaştırmalı olarak özetlenmiştir.

**Tablo 2.6:** Mutabakat Algoritmalarının Karşılaştırılması.

|                                     | PoW                           | PoS                   | PBFT                     |
|-------------------------------------|-------------------------------|-----------------------|--------------------------|
| <b>Blokzincir Türü</b>              | Açık                          | İkisi de              | İzinli                   |
| <b>Düğüm Kimliği</b>                | Bilinmesine gerek yok         | Bilinmesine gerek yok | Bilinmeli                |
| <b>İşlem Hızı</b>                   | Yavaş                         | Normal                | Çok hızlı                |
| <b>Katılım Maliyeti</b>             | Var - Yüksek                  | Var - Düşük           | Yok                      |
| <b>Ölçeklenebilirlik</b>            | Yüksek                        | Yüksek                | Düşük                    |
| <b>Enerji Gereksinimi</b>           | Çok yüksek                    | Düşük                 | Çok düşük                |
| <b>Donanım Gereksinimi</b>          | Çok önemli                    | Önemli                | Önemsiz                  |
| <b>Token Gereksinimi</b>            | Var                           | Var                   | Yok                      |
| <b>İşlem kabulü için onay oranı</b> | %25'den fazla bilgisayar gücü | 51%'den fazla hisse   | %66 (2/3)'dan fazla onay |
| <b>Düğüme Güven</b>                 | Yok                           | Yok                   | Yarı-güven var           |
| <b>İşlem kesinliği</b>              | İhtimale bağlı                | İhtimale bağlı        | Kesin                    |
| <b>Düğüm ağının büyümesi</b>        | Yüksek                        | Yüksek                | Düşük                    |
| <b>Örnek uygulama</b>               | Bitcoin                       | Peercoin              | Hyperledger Fabric       |

**Kaynak:** [Baliga, 2017, s.15; Nguyen vd., 2018, s.114; Kardaş, 2019, s.493 ve Zheng vd., 2018, s.361]'den esinlenilerek yazar tarafından düzenlenmiştir.

<sup>32</sup> “Blokzincir türleri” hakkında detaylı bilgi için bkz. s.100.



### 2.3.5 Kripto Cüzdan (Crypto Wallet)

Kripto cüzdan (kripto para cüzdanı), kripto para birimi için cüzdan işlevi gören bir uygulamadır. İçine nakit para ve kart konulan bir cüzdana benzer şekilde kullanıldığından “cüzdan” olarak adlandırılmaktadır. Ancak fiziksel öğeleri tutmak yerine, kripto para birimi işlemlerini imzalamak için kullanılan geçiş anahtarlarını saklamakta ve kripto paraya erişimi mümkün kılan arayüzü sağlamaktadır (Investopedia Team, 2024).

Kripto cüzdanları, blokzinciri kullanabilme aracıdır. Herhangi bir işlem için blokzincir platformunda işlem yapmak isteyen her kullanıcı kripto cüzdan kullanmak zorundadır. Geleneksel cep cüzdanlarının aksine, kripto para birimleri kripto cüzdanlarda saklanmamaktadır. Aslında, kripto para birimleri ne tek bir alanda depolanmakta ne de fiziki bir formda herhangi bir yerde bulunmaktadır, ancak blokzincirde depolanan işlemlerin verileri olarak var olmaktadır (Suratkar vd., 2020, s.1).

Aşamalar itibarıyla detaylandırırsak kripto para cüzdanları; kullanıcıların, dijital imza<sup>33</sup> oluşturmaları, oluşturdıkları bu genel ve özel anahtarlarını saklamaları, kripto para gönderimi ve alımı gerçekleştirebilmeleri ve bakiyelerini izleyebilmeleri için çeşitli blokzincirleriyle arayüz oluşturan yazılım programlarıdır (Rosic, 2023).

Bir kripto cüzdan işlemi, iki adres arasında kripto para birimi göndermeyi içermektedir. Bir işlemin gerçekleşmesi için göndericinin özel anahtarı ve alıcının açık anahtarı gereklidir. Genel – özel anahtar bilgilerini, sırasıyla IBAN (International Bank Account Number) - kullanıcı şifresi ile ilişkilendirebiliriz (Oğuz vd., 2023, s.132). Gönderici, sahip olduğu herhangi bir miktardaki coin'i özel anahtarı ile dijital olarak imzalayarak alıcının açık anahtarına aktarmaktadır (Nowroozi vd., 2023, s.2) Böylece coinlerin sahipliği alıcının cüzdan adresine devredilmiş olmaktadır. Alıcının bu coinleri harcayabilmesi ve fonların kilidini açabilmesi için kendi cüzdanında sakladığı özel anahtarının, para biriminin aktarıldığı açık adresle eşleşmesi gerekmektedir. Alıcının genel ve özel anahtarı eşleşirse, dijital cüzdanındaki bakiye artacak ve göndericinin cüzdanındaki bakiye aynı tutarda azalacaktır (Rosic, 2023).

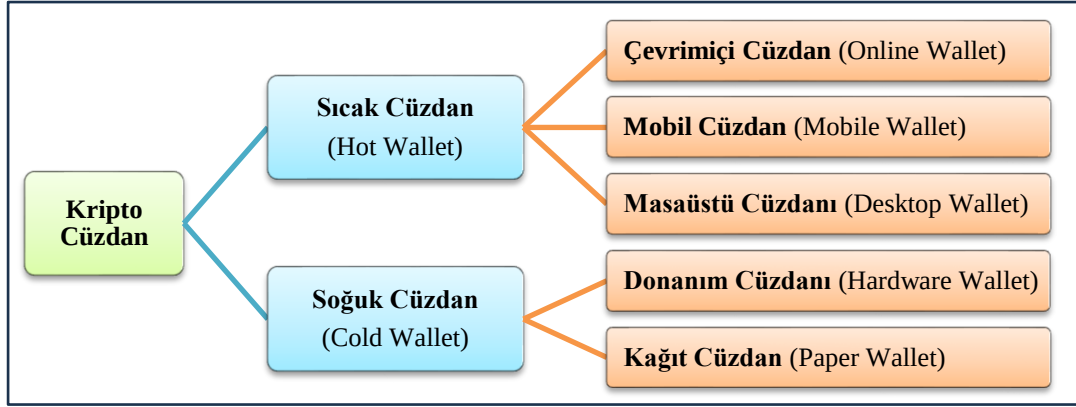
---

<sup>33</sup> “Asimetrik şifreleme ve dijital imza” hakkında detaylı bilgi için bkz. s.35 ve 36.

Dolayısıyla blokzincir ağında bireysel bir kullanıcı açısından, coin işlemlerinde bir adres, bir özel anahtar ve cüzdan yazılımı önemli unsurlardır. Adres, başkalarının kullanıcıya bitcoin gönderebileceği yer yani açık anahtardır. Özel anahtar, kullanıcının başkalarına bitcoin gönderebileceği kriptografik sırdır. Cüzdan yazılımı ise, kullanıcının bitcoinini yönetmek için kendi bilgisayarında çalıştırdığı yazılımdır. Kullanıcının kaydolması gereken herhangi bir merkezi "hesap" yoktur; bir adresin özel anahtarına sahip olunması halinde, bu özel anahtar kullanılarak internete bağlı herhangi bir bilgisayardan (akıllı telefonlar da dahil) o adresle ilişkili coin'e erişilebilmektedir. Cüzdan yazılımı Ayrıca coin işlemlerinin doğrulandığı merkezi olmayan planın bir parçası olarak, o para biriminde gerçekleşen tüm işlemlerin kaydı olan blokzincirinin bir kopyasını da tutabilmektedir (Swan, 2015, s.3).

İlk kripto cüzdan yazılımı Bitcoin-Qt (şimdiki adıyla Bitcoin Core), Şubat 2009'da piyasaya sürülmüştür ve blokzincir ağındaki ilk cüzdan Bitcoin'in geliştiricisi Satoshi Nakamoto'ya (sonrasında Bitcoin Core Developers ekibi devralmıştır) aittir. Blokzincir ağındaki ikinci cüzdan ise, Nakamoto ile yazışan ve Bitcoin istemci yazılım cüzdanını ilk çalıştıran Hal Finney'e aittir. Nakamoto ona test olarak 10 bitcoin göndermiş ve kripto para transfer işlemleri başlamıştır (Sedgwick, 2019). İlk zamanlarda cüzdanlar, Bitcoin yazılımının bir parçası olarak bilgisayarlara indirilen ve kullanıcıların özel anahtarlarının, kullanıcı masaüstünde "wallet.dat" isimli bir dosyada saklandığı bir program idi. Bu yazılım, kullanıcıların kendi cüzdanlarını oluşturmalarına ve Bitcoin'lerini yönetmelerine imkân tanıyordu. Diğer yandan kripto para göndermek uzun anahtarlar girmeyi gerektiren manuel bir işlemdi. Ancak günümüzde çok çeşitli yazılımlar ile bu işlem kullanıcılar adına yapılmaya başlamıştır. Böylece modern kripto para cüzdanları, blokzincirini herkes için erişilebilir hale getirmiştir (Investopedia Team, 2024).

Dolayısıyla günümüzde çeşitli blokzincir ağları için geliştirilmiş, farklı platformlarda kullanılan, farklı özelliklere sahip ve farklı güvenlik seviyeleri sağlayan çok çeşitli kripto cüzdan bulunmaktadır. Kullanıcılar, cüzdan seçimini güvenlik ve kullanılabilirlik özelliklerini değerlendirerek yapmaktadırlar. Buna göre belirli kullanıcı ihtiyaçlarını ve işlem koşullarını karşılamak üzere sınıflandırılan kripto cüzdan kategorileri Şekil 2.20'de özetlenmiştir.



Şekil 2.20: Kripto Cüzdan Türleri.

Kripto para cüzdanları, temelde internet bağlantısına ihtiyaç duyup duymamalarına göre “Sıcak Cüzdan” ve “Soğuk Cüzdan” olmak üzere iki ana kategoriye ayrılmaktadır. Sıcak cüzdan, çevrimiçi yani bir internet bağlantısının gerekli olduğu cüzdan iken; soğuk cüzdan, çevrimdışı yani internet bağlantısının gerekli olmadığı cüzdandır. Sıcak cüzdan, genellikle internette alışveriş yapmak ve bu amaçla az miktarda para tutmak için kullanılırken; soğuk cüzdan, bankadaki kasa kullanımına benzer bir şekilde farklı dijital değerleri saklamak için kullanılmaktadır (Jokić vd., 2019, s.67).

Risk açısından karşılaştığımızda; internetteki hiçbir şey %100 güvenli olmadığından sıcak bir cüzdanda tutulan fonlar her zaman bir hırsızlık veya yazılım hatalarından kaynaklanan kayıp riski altındadır (Suratkar vd., 2020, s.1). Kullanıcıların özel bilgileri çevrimiçi olarak saklandığı için bilgisayar korsanlarına veya kimlik avı saldırılarına karşı koruma ancak cüzdan sağlayıcısının güvenlik önlemleri ölçüsünde güçlü olmaktadır. Soğuk cüzdanlar ise çevrimdışı olarak saklandıklarından kötü niyetli kişilerin onlara erişmesi daha zordur, ancak bu tip cüzdanlar da pratik değildir ve kaybolma veya imha olma riskleri söz konusudur (<https://www.coinbase.com/tr/learn/crypto-basics/what-is-a-crypto-wallet>).

Diğer yandan Şekil 2.20’de de görülmekte olduğu üzere; sıcak ve soğuk cüzdanlar da kendi içinde özel anahtarın korunmasını sağlamak için kendi güvenlik seviyesi düzeyinde farklı sınıflara ayrılmaktadır (Jokić vd., 2019, s.67). “Çevrimiçi”, “Mobil” ve “Masaüstü” cüzdanlar sıcak cüzdan kategorisinde; “Donanım cüzdanı” ve “Kâğıt cüzdan” ise soğuk cüzdan kategorisinde bulunmaktadır. Bir başka sınıflandırma ise “Yazılım”, “Donanım” ve “Kâğıt” cüzdanlar olmak üzere üçlü yapılan gruplandırmadır. Soğuk cüzdan olan donanım ve kâğıt cüzdanlar zaten Şekil 2.20’deki sınıflandırmada görülmektedir. Sıcak cüzdan

kapsamındaki tüm cüzdan tipleri ise bu üçlü sınıflandırmada yazılım cüzdanı kapsamında topluca dikkate alınmaktadır. Buradan hareketle yazılım cüzdanları; kullanıcıların özel anahtarlarını saklamak için veya yerel olarak masaüstü, dizüstü veya mobil cihazlarına indirebilecekleri uygulamalar yani istemci yazılımlar ve çevrimiçi (bulut tabanlı) hizmetlerdir (Mosakheil, 2018, s.90). Donanım cüzdanı, kripto para verilerini cihazın içinde bulunan özel olarak tasarlanmış bir sabit diskte saklayan fiziksel kasalardır (Suratkar vd., 2020, s.1) Genellikle üstünde ekranı olan, içinde yazılımı bulunan USB cihazı şeklindedirler (Jokić vd., 2019, s.69). Kâğıt cüzdan ise, açık ve özel anahtar bilgilerine ait iki QR barkod kodunun bulunduğu bir fiziksel kâğıdı ifade etmektedir (Bulut vd., 2020, s.159).

Kripto cüzdan seçiminin; kullanıcıların ihtiyaçlarına, işlem koşullarına ve güvenlik derecelerine bağlı olarak belirlendiğinden bahsetmiştik. Buna göre örneklendirecek olursak; kullanıcının ihtiyacı borsalarda olduğu gibi adresleri ve anahtarları her zaman çevrimiçi olarak kullanmaksa, donanım cüzdanları doğru seçim olmayacaktır veya bir perakende mağazasında kripto cüzdanı kullanmak gerekiyorsa, masaüstü cüzdanlar işe yaramayacaktır. Diğer yandan riskleri açısından değerlendirdiğimizde; donanım cüzdanları donanım arızalarına, donanım saldırılarına ve hırsızlığa karşı hassas olabilirken, yazılım cüzdanları yazılım arızalarına ve ağ saldırılarına karşı savunmasızdır. Mobil, masaüstü veya bulut platformlarının donanım arızaları halinde ise yazılım cüzdanları etkilenebilmektedir (Bulut vd., 2020, s.160).

Ayrıca bu kategorilerin dışında tek tür kripto para birimini kabul eden ve etmeyen kripto cüzdanlar şeklinde yapılan bir sınıflandırma da mevcuttur. Bitcoinin cüzdanları, tek tür kripto para birimini kabul edenlere örnek iken; Exodus ve Jaxx gibi cüzdanlar çok çeşitli kripto para birimlerini kabul edenlere örnektir (Nowroozi vd., 2023, s.2).

Dolayısıyla çeşitli ihtiyaçlar ve risklerin azaltılması doğrultusunda blokzincir sisteminde kullanılacak birçok kripto cüzdan geliştirilmiştir. Bunlardan en yaygın tercih edilen 10 adet kripto cüzdan yazılım örnekleri; geliştiricileri, ait oldukları blokzincir ağı, cüzdan tipi ve kullanıldıkları platformlar düzeyinde ilk sürüm tarihleri itibarıyla kronolojik olarak aşağıda Tablo 2.7’de verilmiştir.

**Tablo 2.7:** Kripto Cüzdanlar.

| Kripto Cüzdan Adı         | İlk Sürüm | Geliştirici                | Blokzincir Ağı                             | Cüzdan Türü     | Platform                            |
|---------------------------|-----------|----------------------------|--------------------------------------------|-----------------|-------------------------------------|
| Bitcoin Core (Bitcoin Qt) | 2009      | Bitcoin Core Developers    | Bitcoin                                    | Masaüstü        | Windows, macOS, Linux               |
| Blockchain.com            | 2011      | Clockchain Luxembourg S.A. | Bitcoin                                    | Online          | Web, İOS, Android                   |
| Electrum                  | 2011      | Thomas Voegtlin            | Bitcoin                                    | Masaüstü        | Windows, macOS, Linux, Android      |
| Coinbase Wallet           | 2012      | Coinbase                   | Bitcoin, Ethereum, diğer                   | Online          | Web, İOS, Android                   |
| Mycelium                  | 2013      | Mycelium Developers        | Bitcoin                                    | Masaüstü, Mobil | Android, İOS                        |
| Trezor Suits              | 2014      | SatoshiLabs                | Bitcoin, Ethereum, diğer                   | Donanım         | Windows, macOS, Linux               |
| Exodus                    | 2015      | Exodus Movement Inc.       | Bitcoin, Ethereum, diğer                   | Masaüstü, Mobil | Windows, macOS, Linux, İOS, Android |
| Ledger Live               | 2015      | Ledger                     | Bitcoin, Ethereum, diğer                   | Donanım         | Windows, macOS, Linux               |
| Metamask                  | 2016      | ConsenSys                  | Ethereum                                   | Mobil           | Web, İOS, Android                   |
| Trust Wallet              | 2017      | Trust Wallet               | Ethereum, Binance Smart Chain (BSC), diğer | Mobil           | İOS, Android                        |

### 2.3.6 Akıllı Sözleşmeler (Smart Contracts)

Hukuk profesörü ve aynı zamanda bilgisayar bilimci olan Nick Szabo 1994 yılında “Smart Contracts” başlıklı yazısı ile kavramsal olarak ilk kez ortaya koyduğu akıllı sözleşmeyi, “*bir sözleşmenin şartlarını yerine getiren bilgisayarlı bir işlem protokolü*” olarak tanımlamıştır. Szabo, POS terminal ve kartları, EDI (Electronic Data Interchange – Elektronik Veri Değişimi) sistemi ile dijital nakit protokollerine benzer ancak daha kapsamlı bir mekanizmanın sözleşmeler için kullanılabileceği önerisinde bulunmuştur. Bu öneriye göre; akıllı sözleşme ile - örneğin bir alım-satım işleminde ödeme yapılırsa, ürünün teslim edileceği ya da tersi durumu garanti altına alan bir protokolle – sözleşme yürütme otomatikleştirilerek ticari dolandırıcılık ve uygulama maliyetleri (tahkim, icra, işlem vb. gibi) azaltılabilecektir. Ayrıca; menkul kıymetler ve türev ürünlerin birleşimi olan sentetik

varlıkların karmaşık yapılarının, standart sözleşmelere entegre edilmesinde akıllı sözleşmelerin kullanılarak işlem maliyetlerinin düşürülebileceği de belirtilmiştir (Szabo, 1994).

Szabo, kavramsal olarak ortaya koyduktan sonra da akıllı sözleşmeler hakkında çalışmalarına devam etmiştir. 1995 yılında “Smart Contracts Glossary (Akıllı Sözleşmeler Sözlüğü)” başlıklı yazısı ile teknik terimlerin açıklamalarını yapmış, 1996 yılında “Smart Contracts: Building Blocks for Digital Markets (Akıllı Sözleşmeler: Dijital Pazarlar için Yapı Taşları)” isimli makalesi ile akıllı sözleşmelerin, bilgisayar bilimi ve hukuk alanı arasındaki kesişim noktasını ortaya koymuş ve bu teknolojinin gelecekteki potansiyelini vurgulamıştır. 1997 yılında ise “The Idea of Smart Contracts (Akıllı Sözleşmeler Fikri)” başlıklı yazısı ile akıllı sözleşme uygulama örneklerine yer vermiş ve yine aynı yıl “Formalizing and Securing Relationships on Public Networks (Kamusal Ağlarda İlişkileri Resmileştirmek ve Güvence Altına Almak)” adlı makalesi ile ise akıllı sözleşmelerin teknik ve hukuki zeminini tartışarak, tarihsel gelişimini ve dijital pazarların inşasında potansiyel rollerini daha da derinlemesine ele almıştır. Ayrıca 2005 yılında “Bitgold” başlıklı blog yazısı ile merkeziyetsiz, enflasyondan arınmış, kriptolojik hesaplamalara ve iş kanıtına dayalı bir para yaratma protokolü ortaya koymuştur<sup>34</sup>. Kripto para bitcoin ve bitcoin sözleşmelerinin altında yatan çoğu fikir, Szabo’nun tüm bu çalışmalarında - özellikle 1997 ve 2005 yıllarındaki - tanımlanmıştır (<https://en.bitcoin.it/wiki/Contract>).

Akıllı sözleşmeler; sözleşme maddelerinin (teminat, kefalet, mülkiyet haklarının tanımlanması vb. gibi), ihlal edilmesi durumunda karşılaşılabilecek maliyetlerin ihlal eden için pahalı hale getirilmesini sağlayacak şekilde, donanım ve yazılım içine yerleştirilmesi fikrine dayanmaktadır. Bu fikrin en ilkel örneği otomat makineleridir. Otomatlar; belirli miktar bozuk para karşılığında, basit bir hesaplama ile ürün ve para üstü sağlayan mekanizmalardır. Yeterli miktarda parası olan herkes bu takas işleminin tarafı olabilmektedir. Makineye atılan paralar kilitli bir kutu ve diğer güvenlik mekanizmaları ile korunmaktadır. Ayrıca saldırganlar için mekanizmayı ihlal etme maliyeti kasadan elde edecekleri toplam paradan çok daha fazladır (Szabo, 1997a).

---

<sup>34</sup> “Bitgold” hakkında detaylı bilgi için bkz. s.60.

Diğer yandan akıllı sözleşmeler; değerli ve dijital yollarla kontrol edilen her türlü varlığa ilişkin sözleşmeler için kullanmayı önererek, otomat makinasından çok daha fazlasını vadetmektedir. Örneğin, bir kredi için arabanın teminat gösterildiği varsayımında; araç sahibi temerrüde düşer ve ödemelerini yapmazsa; haciz memurunun gelip arabaya el koyması yerine, akıllı sözleşmedeki haciz protokolünün otomatik olarak devreye girdiği ve aracın anahtarlarını bankanın kontrolüne bıraktığı, kredinin ödenmesi halinde ise haczin kaldırıldığı bir sistem sunmaktadır (Szabo, 1997b).

Akıllı sözleşmeler; ödeme koşulları, rehinler, gizlilik, icra vb. gibi sözleşme koşullarını otomatik olarak yerine getiren, dolandırıcılık riskini azaltarak uygulama maliyetlerini ve güvenilir araçlara olan gereksinimi minimize eden avantajlı bir sistemdir (Szabo, 1994). Ancak Szabo'nun teorik olarak öne sürdüğü bu akıllı sözleşme kavramının pratikte uygulamaya geçebilmesi için gerekli teknoloji o dönemde henüz geliştirilme aşamasındaydı. Blokzincir teknolojisinin ortaya çıkmasıyla birlikte ise bu mümkün hale gelmiştir. Kripto para bitcoin'in temel prensiplerinin, blokzincir teknolojisi ve Szabo'nun çalışmalarına dayanmasına rağmen, akıllı sözleşme kavramı ilk nesil blokzincir ağı olan Bitcoin içinde doğrudan yer almamıştır. Her ne kadar akıllı sözleşmelerin hayata geçirilmesinde blokzincir teknolojisi önemli bir yere sahipse de aynı zamanda akıllı sözleşmeler de blokzincir teknolojisinin gelişerek yaygınlaşmasına katkı sağlamıştır (Tanrıverdi vd., 2019, s.210). Nitekim 2013 yılında Rus asıllı Kanadalı üniversite öğrencisi Vitalik Buterin tarafından yayınlanan Ethereum White Paper'ı ile yerleşik Turing-tam programlama dili kullanılarak akıllı sözleşmeler ve merkezi olmayan uygulamalar yazılabilmesini sağlayan bir blokzinciri olan Ethereum tanıtılmıştır. 2014 yılında, Gavin Wood tarafından Ethereum Yellow Paper'ı yayınlanarak Ethereum'un teknik protokolü detaylı bir şekilde açıklanmıştır. 2015 yılında ise Ethereum piyasaya sürülmüş (<https://ethereum.org/en/history/#whitepaper>) ve ikinci nesil blokzincir ağı geliştirilmiştir. Böylece günümüzdeki akıllı sözleşme yazılımlarının temeli atılmıştır. Ayrıca akıllı sözleşmelerle birlikte blokzincir teknolojisi, çeşitli alanlarda (finans, gayrimenkul, lojistik, sağlık vb.) kullanılmaya başlanarak yaygınlaşmıştır.

### ***Ethereum blokzinciri***

Ethereum, Bitcoin blokzinciri gibi merkeziyetsiz ve açık kaynak kodlu ancak blokzincir üzerine akıllı sözleşmeler ve merkezi olmayan uygulamalar (DApps) yazılmasına olanak sağlayan genişletilmiş bir blokzincir protokolüdür (Buterin, 2013, s.13). Ethereum ile

blokzincir üzerine akıllı sözleşmelerin ve DApps'lerin yazılabilmesi ise ağdaki bütün düğümlerde çalışan ve senkronize edilen dağıtık sanal bilgisayar "Ethereum Virtual Machine (EVM)" yazılımı sayesinde gerçekleşebilmektedir (Blockchain Türkiye Platformu, 2021a, s.6). Buradan hareketle akıllı sözleşme mekanizmasının işleyişinin anlaşılabilmesi için mekanizmanın yürütülmesini sağlayan EVM ve Ethereum blokzincirinin sahip olduğu özellikler aşağıda maddeler halinde sıralanmıştır (Genet vd., 2020; Buterin, 2013; Wood, 2014):

- a. Bitcoin blokzincirinde kullanılan Script adlı betik dilin (scripting language) aksine EVM'nin programlama dili Turing-tam özelliğe sahiptir yani teorik olarak her türlü hesaplama işlemini yapabilmektedir.
- b. Sözleşmeler, Solidity veya Vyper gibi ileri seviye dillerde programlanmaktadır.
- c. Solidity/Vyper dilinde yazılan sözleşmeler, EVM tarafından anlaşılabilen bytecode formatında derlenmektedir. Bytecode, sözleşmenin yürütülmesi için gerekli talimatların bir listesidir. Her talimat, EVM'nin yürütme sırasında işlemesi gereken bir komutu veya operasyonu temsil etmektedir.
- d. EVM, bir yığın makinesidir yani yürütme sırasında kullanılan veri ve komutların saklandığı yığın (stack) tabanlı bir yapıya sahiptir. Aritmetik operasyonlar, veri yapılarındaki işlemler, depolama talimatları gibi işlemler, yığın üzerinde yapılan okuma ve değişikliklerle gerçekleştirilir.
- e. Program sayacı (program counter, pc), EVM'nin yürütme sırasında bir sonraki talimatın indeksini belirler ve bu talimatı işlemek için yığın üzerinde gerekli operasyonları gerçekleştirir.
- f. Ethereum blokzincirinin kripto parası "ether (ETH)" olarak adlandırılmaktadır. Ether, hesaplar arasında takas edilebilmektedir ve akıllı sözleşmeler yürütülürken kullanılan hesaplama gücü karşılığı olarak ödeme yapmak için kullanılmaktadır.
- g. Ether kripto para arzı, bitcoin gibi sınırlı değildir; her yıl belirli bir enflasyon oranına göre ether arzı artmaktadır. Mayıs 2024 itibarıyla dolaşımda olan Ethereum coin sayısı 120 milyonun biraz üzerindedir.



- h. Bitcoin ağına her 10 dakikada bir blok eklenirken; Ethereum ağına yaklaşık 15 saniyede bir blok eklenmektedir.
- i. Bitcoin’de blok büyüklüğü, zincirin büyümesini kontrol altında tutmak ve veri trafiğini yönetmek için belirli bir MB ile sınırlandırılmışken; Ethereum’da böyle bir MB sınırlandırması yoktur. Ancak onun yerine gaz limiti (gas limit) uygulanmaktadır. Gaz limiti, bir bloktaki maksimum gaz miktarını belirlemekte; bu da doğrudan blok büyüklüğüne etki etmektedir. Her bloğun gaz limiti değişkenlik gösterebilmektedir. Böylece Ethereum bloklarının geniş işlem kapasitesine sahip karmaşık işlemleri gerçekleştirebilmesi sağlanabilmektedir.
- j. Ethereum sistemi, sonlandırılmayan programlardan (sonsuz döngülerden) ve protokolün kötüye kullanımından “Gaz (gas)” mekanizması ile korunmaktadır. Bir sözleşmenin her bir talimatının işlenmesi için EVM, gaz tüketmekte ve bir sözleşmenin çalıştırılması için sağlanan gaz ise sınırlı olmaktadır.

Gaz, işlem yapılırken kullanılan işlemci zamanı, bellek kullanımı vb. kaynakların miktarını belirleyen bir ölçü birimidir ve işlemi gerçekleştiren kullanıcı tarafından ödenmektedir. Kullanıcının ödediği bu gaz ücreti, işlemde kullanılan gaz limiti ile ağdaki gaz fiyatı (gas price) çarpılarak hesaplanmaktadır. Gaz fiyatı, bir birim gaz için ödenen ether miktarıdır ve “gwei” birimi ile ölçülmektedir. (En küçük ether birimi weidir ve  $1 \text{ ETH} = 10^9 \text{ gwei} = 10^{18} \text{ wei}$ ). Gaz ücreti, kullanıcıların işlemlerini ne kadar hızlı işlemek istediklerine bağlı olarak belirlenmekte ve daha yüksek gaz ücreti, işlemin daha hızlı onaylanmasını sağlamaktadır.

- k. Ethereum blokzinciri ilk yayınlandığında PoW mutabakat algoritma yöntemini kullanıyordu. Eylül 2022 itibarıyla PoS mutabakat algoritmasına geçiş yapmıştır. Bu algoritmaya göre bir kullanıcının Ethereum PoS mutabakat ağında doğrulayıcı olabilmesi için cüzdanında 32 ETH olması (stake edilmesi) gerekmektedir.
- l. Ethereum’da 20 baytlık adresi olan bir hesap; (i) nonce, (ii) bakiye (ether miktarı), (iii) veri deposu ve (iv) kod olmak üzere dört unsurdan oluşmaktadır. Nonce, harici hesapta işlem sayısı, sözleşme hesabında sözleşme sayısıdır; bakiye, hesabın mevcut ether miktarı; veri deposu, hesabın varsa depolama alanı ve kod, hesabın varsa sözleşme kodudur.

m. Ethereum'da iki tür hesap bulunmaktadır: (i) koda sahip olmayan “harici hesaplar” ve (ii) bir koda sahip “sözleşme hesapları”. Harici hesaplar, kullanıcılar (özel anahtarlar) tarafından kontrol edilen hesaplardır ve kendi özel anahtarlarını kullanarak işlem oluşturup diğer harici ve sözleşme hesaplarına mesaj iletebilirler. Harici hesaplar bilgi ve ether depolamak için kullanılmaktadır. Sözleşme hesapları ise sözleşme kodları tarafından kontrol edilen, veri işlemlerini ve mantıksal koşulları içeren kod parçalarının olduğu hesaplardır. Gelen mesajlara yanıt olarak işlem başlatabilir, tek başlarına yeni bir işlem başlatamazlar. Dolayısıyla Ethereum blokzincirinde gerçekleşen tüm eylemler harici hesaplar kontrolünde gerçekleşmektedir.

Akıllı sözleşme kodu, Ethereum Virtual Machine (EVM) üzerinde çalışacak şekilde derlenmiş bir programdır. Bu kod, belirli koşullar altında otomatik olarak çalışmakta ve işlemleri gerçekleştirmektedir. Bu durumda akıllı sözleşmeler, bir kullanıcı tarafından kontrol edilme ihtiyacı olmayan, kendi bakiyeleri olan ve ağ ile etkileşime girme kabiliyetine sahip bir hesap türüdür. (Andolfatto vd., 2022, s.156).

Ethereum blokzincirinde akıllı bir sözleşmede, anlaşmanın tamamı bilgisayar programının bir parçası olarak belirtilmekte ve blokzincirinde saklanmaktadır. Örneğin bir teminatlı kredi işleminde; program, kredi koşullarının yanı sıra uygunluğa bağlı olarak gerçekleştireceği belirli eylemleri de içermektedir (örneğin, temerrüt durumunda teminat mülkiyetinin devri). Blokzinciri sözleşmenin sadık bir şekilde yürütülmesini sağladığından, borç alan ve borç veren dışında herhangi bir tarafın sisteme dahil edilmesine gerek bulunmamaktadır (Andolfatto vd., 2022, s.157). Diğer yandan sözleşmeler daha önce imkânsız olan hiçbir şeyi mümkün kılmamaktadır. Bunun yerine sıklıkla karşılaşılan sorunlar, güven unsuru azaltılarak çözümlenmektedir. Minimum güven ile insan kararları döngüden çıkarılmakta ve böylece tam otomasyon sağlanarak işler daha kolay hale getirilmektedir (<https://en.bitcoin.it/wiki/Contract>).

Akıllı sözleşmeler; (i) Statik, (ii) Dinamik ve (iii) Oracle güdümlü olmak üzere üç ana kategoriye ayrılmaktadır. Statik akıllı sözleşmeler; insan etkileşimine dayanmayan, dış dünya verilerine ihtiyaç duymayan, diğer akıllı sözleşmeleri çağırmayan, tek adımda gerçekleşen ve önceden tanımlanmış koşulların ve parametrelerin asla değiştirilemediği sözleşmelerdir. Basit matematik işlemlerini (dört işlem) gerçekleştirip aynı kuralları izleyerek aynı sonuca ulaşan ve “evet/hayır” yanıtını verebilen programlardır. Örneğin bir

diploma doğrulama talebinde; diploma listesine bakıp kurum adı, veriliş tarihi gibi bilgilerin istekte bulunana verilmesi veya token transferinin yapılması statiktir işlemlerdir (Terzi vd., 2019, s.2).

Dinamik akıllı sözleşmeler; insan etkileşimine dayanan, bazen dış dünya verilerine ihtiyaç duyabilen, koşulların ve parametrelerin değiştirilebildiği buna göre farklı sonuçlara ulaşp farklı eylemlerin gerçekleştirilebildiği programlardır. Örneğin; döviz kurları, piyasa fiyatları gibi veriler takip edilerek ödeme yapılması veya enerji akıllı bir binada aşırı elektrik tüketimini ve maliyetleri azaltmak için ısıtma ve tüketim düzeylerinin ölçülerek ayarlanması (Terzi vd., 2019, s.2) dinamik işlemlerdir.

Oracle güdümlü akıllı sözleşmeler ise dış verilere ihtiyaç duyan ve bu verileri doğrudan almak ve işlemek için Oracle adı verilen blokzincir dışı hizmetlere güvenen programlardır. Bu sözleşmeler, gerçek dünyadan bilgi talep etme ve diğer akıllı sözleşmelerin kullanması için bunları blokzincirine yazma becerisine sahip yapay zekâ araçları olarak hareket etmektedirler. Örneğin noterlerin değişen miras kanunları ile ilgili bilgilendirilmelerinde; bu akıllı sözleşmeler, yapay zekâ kullanarak devlet veri havuzundaki miras kanunu değişikliklerini takip edip, bu bilgileri blokzincire yazarak zaman damgası ile kaydetmekte ve ilgili tarafları otomatik olarak bilgilendirmektedirler (Terzi vd., 2019, s.3). Ya da uçuşta belirli bir süre gecikme veya iptal olduğunda otomatik olarak yolcuya sigorta tazminatı ödenmesini sağlayan bir akıllı sözleşme (Blockchain Türkiye Platformu, 2021a, s.12) de oracle güdümlü akıllı sözleşme işlemine örnektir.

Diğer yandan önceden belirlenmiş koşulların yerine getirilip getirilmediği, statik ve dinamik akıllı sözleşmelerde blokzincir üzerinde bulunan (on-chain) verilerle doğrulanırken; Oracle güdümlü akıllı sözleşmelerde ise dış veri sağlayıcısı Oracle'ın, blokzincir dışındaki (off-chain) verileri (hava durumu, uçak kalkış-iniş saatleri, faiz oranları vb. gibi) blokzincire aktarmasıyla tespit edilmektedir (Blockchain Türkiye Platformu, 2021a, s.12).

Akıllı sözleşmeler; (i) Durum değişkenleri (State variables), (ii) Fonksiyonlar (Functions) ve (iii) Olaylar (Events) olmak üzere üç bileşenden oluşmaktadır (BKM vd., 2020, s.11). Durum değişkenleri, blokzincir üzerinde saklanan akıllı sözleşme durum ve geçmiş bilgileridir. Fonksiyonlar, kullanıcılar veya diğer akıllı sözleşmeler tarafından çağrılabilen

belirli görevleri yerine getiren kod bloklarıdır. Olaylar ise belirli durum değişiklikleri veya önemli olaylarda tetikleme bildirimlerini göndermede kullanılır.

Kısacası akıllı sözleşmeler, durum değişikliklerine göre otomatik eylemlerde bulunan programlardır ve Ethereum da bu programın çalışmasını sağlayan bir “işlem tabanlı durum makinesi<sup>35</sup>” dir (Kasireddy, 2017). Bu makinenin nasıl çalıştığı yani Ethereum blokzincirinde akıllı sözleşme protokolünün nasıl işlediği ise aşağıda maddeler halinde özetlenmiştir (Garnett, 2023) :

- a. Taraflar, hüküm ve koşullarda anlaşır.
- b. Akıllı sözleşme oluşturulur : Bir kullanıcı veya akıllı sözleşme geliştiricisi, Solidity veya Vyper programlama dilinde bir akıllı sözleşme oluşturur. Daha sonra bu sözleşme derlenerek bytecode'a dönüştürülür. Bu bytecode da EVM'ye yüklenir.
- c. Akıllı sözleşme blokzincirde yayınlanır : Akıllı sözleşme, Ethereum blokzincirinde yayınlanır ve veri alanına akıllı sözleşme kodu dahil edilir. Bu aşama önemlidir çünkü bir sözleşme zincirde yayımlandıktan sonra değiştirilmesi veya iptal edilmesi mümkün değildir.
- d. Tetikleme koşulları gerçekleşir : Akıllı sözleşme, on-chain veya off-chain verileri izleyerek çalışmaktadır. Bu izleme sırasında sözleşme koşullarının gerçekleşmesi ile tetiklenme meydana gelir.
- e. Akıllı sözleşme yürütülür : Tetiklenme sonucunda sözleşme tarafından belirlenen eylemler otomatik olarak başlatılır. Örneğin; bir ödeme yapılabilir, bir mesaj yayınlanabilir veya başka bir akıllı sözleşme ile etkileşime geçilebilir.
- f. Madencilik ile işlem onaylanır : Yapılan durum (state) değişikliği, madenciler tarafından işleme alınıp doğrulanır.
- g. Sözleşme sonucu blokzincire kaydedilir : PoS madenciliğinin ardından söz konusu işlemi içeren blok, zincirde yayınlanır ve yeni blok diğer madenciler tarafından onaylandıktan sonra zincire kalıcı olarak kaydedilir.

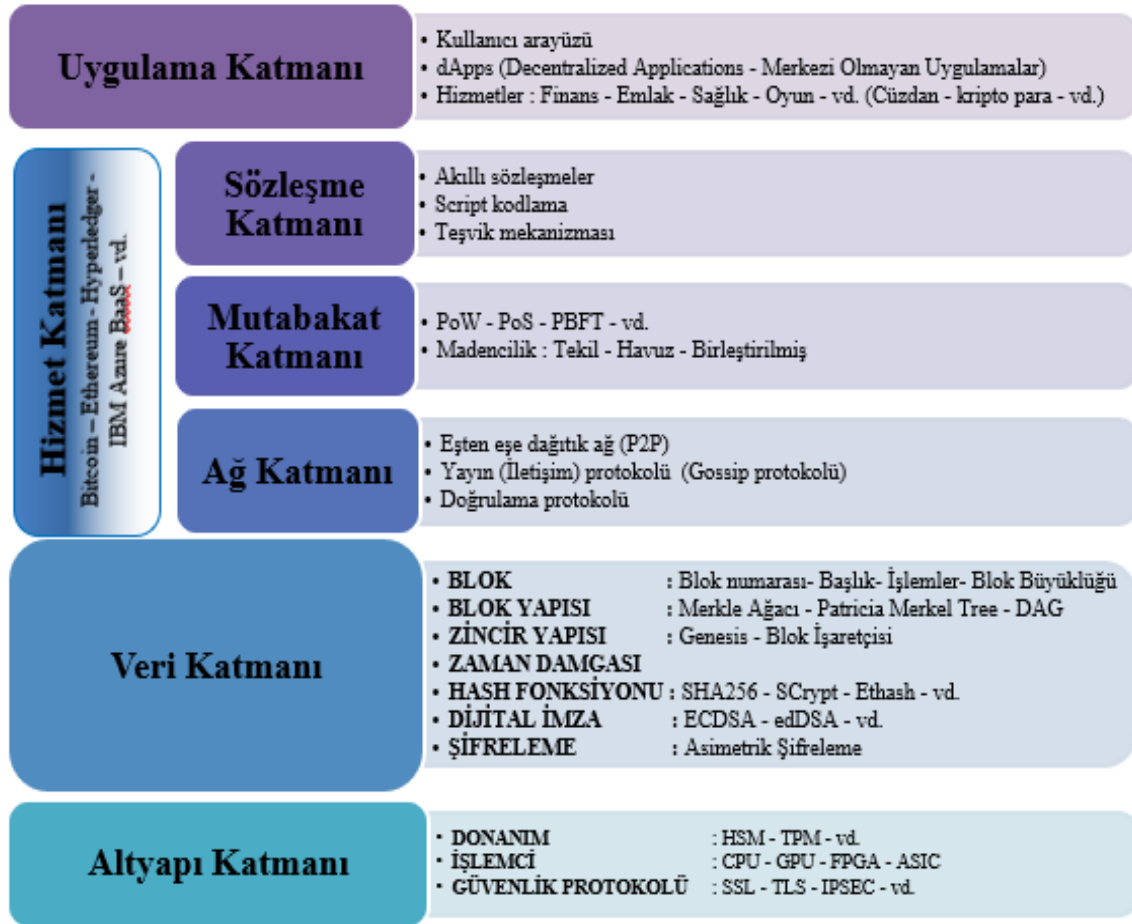
---

<sup>35</sup> Durum makinesi; bilgisayar biliminde, aldığı girdilerle yeni bir duruma geçiş yapabilen bir mekanizma olarak tanımlanmaktadır.

## 2.4 BLOKZİNCİR TEKNOLOJİSİNİN MİMARİSİ

### 2.4.1 Blokzincir Teknolojisi Katmanları

Önceki bölümlerde blokzincir teknolojisinin tanımı yapılarak bu teknolojiye ilişkin teknik kavramlar detaylı bir şekilde açıklanmıştır. Çalışmanın bu aşaması itibarıyla blokzincir teknolojisinin çalışma prensibi üzerinde durulacaktır. Bu amaçla; karmaşık olan bu sistemin işleyişinin anlaşılabilir olması için, temel bileşenlerin belirli niteliklere göre sınıflandırıldığı katmanlı bir yapı ile blokzincir teknolojisinin kavramsal mimarisi Şekil 2.21’de ortaya konulmuştur.



Şekil 2.21: Blokzincir Teknolojisi Mimari Katmanları.

[Murthy vd., 2020, s.205196; Blockchain Türkiye Platformu Teknoloji Çalışma Grubu, 2019a]’dan esinlenilerek yazar tarafından oluşturulmuştur.

Bu mimari yapıya göre blokzincir teknolojisi; en altta altyapı katmanı, sonrasında veri katmanı, ardından sırasıyla hizmet katmanının kapsadığı ağ, mutabakat ve sözleşme

katmanları ve son olarak da uygulama katmanı olmak üzere yedi katmandan oluşmaktadır. Şekil 2.21’de içerik ve uygulama örnekleri üzerinden özetlenen bu katmanların kapsamı aşağıda bölüm alt başlıklarında açıklanmıştır.

#### **2.4.1.1 Altyapı katmanı (Infrastructure layer)**

Altyapı katmanı, blokzincir sisteminin en alt katmanıdır ve donanım, sistem ve sunucu olmak üzere üç seviyede çalışmaktadır. Diğer yandan düğümler de bu katmanın bir parçasıdır (Shah vd., 2018, s.5). Dolayısıyla dağıtık ağ yapısındaki düğümleri oluşturan fiziksel veya bulut tabanlı bilgisayarlar, blokzincirin altyapısını ifade etmektedir (Dursun, 2020, s.12). Çoğu blokzincir sistemi herhangi bir özel donanım olmadan kurulabilse de mutabakat sürecini daha verimli, depolama ve hesaplama ortamını daha güvenilir hale getirmek amacıyla (Tabatabaei vd., 2023, s.5) çok çekirdekli bilgisayarlar kullanılmakta veya GPU'lar, FPGA'lar ve ASIC'ler gibi yüksek performanslı donanımlarla altyapı güçlendirilmektedir (Dursun, 2020, s.12). Ancak madencilik, ihtiyaç duyduğu aşırı güç nedeniyle yerini alternatif mutabakat yöntemlerine bıraktığından donanım gereksinimleri de yavaş yavaş ortadan kalkmaktadır (Shah vd., 2018, s.5).

#### **2.4.1.2 Veri katmanı (Data layer)**

Veri katmanı, bir blokzincir sisteminin en önemli bileşenlerinden biridir; burada verilerin, güvenli bir şekilde depolanması, değişikliklere karşı korunması ve izlenebilir hale getirilmesi sağlanmaktadır. Ayrıca bu katman verilerin kullanılabilirliğini ve dayanıklılığını sağlamaktan da sorumludur (Tabatabaei vd., 2023, s.5). Veri katmanı, veri depolamanın bütünlüğünü sağlamak için temel olarak blok veri yapısını kullanmaktadır. Ağdaki her bir düğüm, belirli bir süre boyunca alınan veri işlemlerini zaman damgalı bir veri bloğu halinde kapsüllemekte ve bloğu depolamak için mevcut en uzun ana blokzincirine bağlamaktadır (Zhai vd., 2019, s.2). Bu katman; blok depolama, zincir yapısı, hash algoritması, Merkle ağacı, zaman damgası, dijital imza ve şifreleme tekniklerini<sup>36</sup> içermektedir.

---

<sup>36</sup> İlgili kavramlar hakkında detaylı bilgi için bkz. “zincir yapısı” s.22 , “hash algoritması” s.37 , “Merkle ağacı” s.25, “zaman damgası” s.26, “dijital imza” s.36 , “şifreleme teknikleri” s.31.

### 2.4.1.3 Ağ katmanı (Network layer)

Blokzincir ağı, merkezi olmayan dağıtık bir yapıdadır<sup>37</sup>. Bu sistemde, her bir bilgisayar (düğüm) hem kaynak sağlayıcı (sunucu) hem de kaynak kullanıcı (istemci) olarak işlev görebilmektedir. Geleneksel istemci-sunucu modelinden (merkezi ağ yapısı) farklı olarak, düğümler arası iletişim bir merkeze ihtiyaç duyulmadan doğrudan gerçekleştirilebildiğinden ağdaki tüm düğümler eşittir. Dolayısıyla sistemdeki tüm veriler tüm ağ düğümlerinde (node) birebir aynı olarak bulunmakta ve herhangi bir düğüm hem veri alıp hem de veri gönderebilirken bir düğümün paylaştığı veriye diğer tüm düğümler erişebilmektedir. Bu dağıtık ağ iletişim modeline “peer to peer (P2P)” yani “eşten eşe (eşler arası)” sistemi denilmektedir.

Ağ katmanı, blokzincir ağındaki düğümler arasında bilgi transferini sağlamak için yaygın olarak Gossip protokollerinin tercih edildiği bir düzeydir (Dursun, 2020, s.12). Gossip (Dedikodu) protokolü ise dedikodunun sosyal ağlardaki mesajları yayma (kulaktan kulağa) şeklinden esinlenerek, ağın rastgele üyeleriyle periyodik veri alışverişine dayalı olarak bir ağ üzerinden içerik yayan bir P2P iletişim protokolü türüdür (Kwiatkowska, 2008, s.1). Blokzincirdeki Gossip protokolünde; her düğüm, yeni verileri tüm komşularına aynı anda ve eksiksiz bir şekilde iletmekte ve her komşu da tüm sistem senkronize olana kadar süreci taklit etmektedir (Saldamli vd., 2022, s.1915). Dolayısıyla bu protokol; verilerin hızlı bir şekilde yayılması, düğümlerin birbirlerini bulması, blokzincir verilerinin indirilmesi ve yeni blokların ağ içinde yayımlanması işlemlerini sağlamaktadır (Dursun, 2020, s.12).

Diğer yandan ağ katmanı; düğümlerin, bloklar içerisindeki işlemlerin doğruluğunu ve blokların geçerliliğini onayladıkları doğrulama protokollerini de içermektedir. Buna göre bu katmanda; “P2P ağı” dayalı olarak zincire eklenecek bloğun doğrulamasının yapıldığı “doğrulama protokolleri” ile doğrulanmış bloğun zincire eklendiğinin ağa iletilerek tüm düğümlerde senkronizasyonun yapılmasını sağlayan “yayın protokolleri” yer almaktadır.

Aynı zamanda ağ katmanı, blokzincir mimarisinin ölçeklenebilirlik sorunlarının çözülmesine yardımcı olan güvenilir bir yürütme ortamıdır. Ağın sadece bu sorununun üstesinden gelmesini sağlamakla kalmamakta, onu daha güvenli hale getirmektedir. Ayrıca

---

<sup>37</sup> “Ağ yapıları” hakkında detaylı bilgi için bkz. s.28.

verilerin ana ağdan uzakta depolanmasını sağlayarak ana ağın üzerindeki yükün bir kısmını da almaktadır (Shah vd., 2018, s.4).

#### **2.4.1.4 Mutabakat katmanı (Consensus layer)**

Adından da anlaşıldığı üzere mutabakat katmanı; blokzincir ağındaki düğümlerin, merkezi olmayan sistemdeki blok verilerinin geçerliliği ve doğruluğu konusunda bir fikir birliğine varmalarını sağlayan mutabakat algoritmalarının<sup>38</sup> yer aldığı katmandır. Mutabakat protokolleri, blokzincir ağındaki her düğüm tarafından kaydedilen verilerin tutarlılığını ve değiştirilemezliğini garanti altına alan, hileli işlemleri engelleyen en önemli bileşendir (Dursun, 2020, s.12). Mutabakat protokolleri olmayan bir blokzincir ağı bulunmamaktadır (Shah vd., 2018, s.4). Blokzincirinin kilit teknolojilerinden biri olarak, blokzinciri mimarisinin yüksek eşzamanlılığını desteklemek için verimliliği artırmaya yönelik çeşitli mutabakat protokolleri kullanılmaktadır (Wang vd., 2021, s.419). Hangi mutabakat tasarımının seçileceği, DoS saldırılarına dayanma veya bunları hafifletme becerisi de dahil olmak üzere performans, güvenlik ve gizlilik garantilerinin gücü ile ilgili farklı parametrelere bağlı olarak belirlenmektedir (Tabatabaei vd., 2023, s.5). En yaygın kullanılan türleri Nakamoto'nun PoW'u, PoS ve PBHT'dir.

#### **2.4.1.5 Sözleşme katmanı (Contract layer)**

Sözleşme katmanında, güveni uygulamak için kullanılan ve blokzincirinin programlanabilir özelliğinin temelini oluşturan akıllı sözleşme yer almaktadır. Sözleşme şartlarını otomatik olarak yürütebilen bilgisayarlı program, kod ve veri setleri şeklinde blokzincirinde saklanmaktadır. Zaman veya olaylar tarafından yönlendirilen akıllı sözleşmeler, blokzinciri düğümleri tarafından dağıtılmış bir şekilde yürütülmektedir. İlgili tüm şartlar kodlanmakta, otomatik olarak çözülmekte ve imzalar veya diğer harici veri mesajları tarafından tetiklenmektedir (Zhai vd., 2019, s.2).

Blokzinciri sistemleri, ağın katılımcıları arasında kurallar oluşturmak ve uygulamak için sözleşmeler tanımlama yeteneği sağlamaktadır. Farklı blokzinciri sistemleri, uygulama alanlarına bağlı olarak sözleşmeleri geliştirmek için çeşitli yöntemler kullanabilmektedir. Bu katman, sözleşme dahilindeki işlemlerin çağırılması ve yürütülmesinin yanı sıra

---

<sup>38</sup> “Mutabakat algoritmaları” hakkında detaylı bilgi için bkz. s.40.



programlama dilleri (Turing-tam vb. gibi) ve yürütme ortamları ile de ilgilenmektedir (Tabatabaei vd., 2023, s.5).

Akıllı sözleşmeler<sup>39</sup>, blokzincir mimarisinde veri işlemek için kullanılan araçlardan biridir ve bu unsurun blokzincir içinde kullanılabilirliğini sağlayan Sanal Makine (Virtual Machine) teknolojisidir (Blockchain Türkiye Platformu Teknoloji Çalışma Grubu, 2019, s.28). Diğer yandan gerçek dünya ile blokzincir sistemleri arasında veri etkileşimi sağlamak için de Oracle teknolojilerinden faydalanılmaktadır. Bu teknolojilerin temel görevi ise akıllı sözleşmelerde kullanılmak amacıyla fiziksel dünyaya ait döviz kuru, maç sonuçları, hava durumu, uçuş detayları vb. gibi verilere ulaşmak, gerçekliğini doğrulamak ve blokzincir sistemine entegre etmektir (Blockchain Türkiye Platformu Teknoloji Çalışma Grubu, 2019, s.29).

#### **2.4.1.6 Hizmet katmanı (Service layer) ve Uygulama katmanı (Application layer)**

Hizmet ve uygulama katmanları, blokzincir faaliyetlerinin yürütüldüğü katmanlardır (Murthy, 2020, s.205196). Hizmet katmanı, blokzincirin altında altyapısal ve protokol düzeyinde işlevleri yönetirken; uygulama katmanı, kullanıcılarla doğrudan etkileşimde bulunan ve akıllı sözleşmelerin çalıştığı katmandır.

Hizmet katmanı, uygulama katmanının oluşturulmasına ve çalıştırılmasına yardımcı olan tüm temel araçlara erişimi sağlamaktadır (Shah vd., 2018, s.4). Blokzincir uygulamaları temel katmanların üzerine doğrudan yazılabilmektedir, ancak hizmet katmanı basitlik, güvenlik ve ölçeklenebilirlik sağlayarak sistemi güçlendirmekte ve kolaylaştırmaktadır. Hizmet katmanının olmaması halinde bu işlevlerin, doğrudan uygulama katmanında etkinleştirilmesi gerekmektedir (<https://blog.bitgo.com/understanding-the-bitgo-blockchain-services-layer-2a054a5999b1>).

Dolayısıyla hizmet katmanı; blokzincirinin işlevselliğini, Yönetişim/DAO'lar (Decentralized Autonomous Organization - Merkezi Olmayan/Dağıtık Otonom Organizasyon), Oracle'lar, Cüzdanlar, Blokzinciri Monitörü vb. gibi ek hizmetlerle geliştirmektedir. Hizmet katmanı, Web3 ara bağlantısı oluşturarak engelleri ortadan kaldırmakta ve sorunsuz etkileşim sağlamaktadır (Fawole vd., 2023).

---

<sup>39</sup> “Akıllı sözleşmeler” hakkında detaylı bilgi için bkz. s.78.

Hizmet katmanı; Bitcoin, Ethereum ve Hyperledger ve benzerlerini içermektedir. Bitcoin esas olarak dijital para birimi işlemleri içindir. Ethereum, dijital para birimine dayalı merkezi olmayan uygulamalar eklemektedir. Hyperledger ise dijital para birimi işlemlerini desteklemeyen kurumsal düzeyde blokzinciri uygulamalarıdır (Zhai vd., 2019, s.2).

Uygulama katmanı ise tüm katmanların üstünde konumlanan ve doğrudan kullanıcılarla etkileşime geçen ara yüzüdür (Blockchain Türkiye Platformu Teknoloji Çalışma Grubu, 2019, s.24). Son kullanıcı için cüzdan, borç verme, stake etme gibi belirli ürünler sunan blokzincir tabanlı uygulamaları sağlamaktadır (Fawole vd., 2023). Tüm merkezi olmayan uygulamalar, merkezi olmayan ağ ile bu katmanda barındırılmaktadır. Bu katman Komut Dosyaları, Akıllı Sözleşmeler, dApp'ler ve Kullanıcı Arayüzünden oluşur. Kullanıcı, dApp kullanarak merkezi olmayan uygulamalara erişebilmekte ve ayrıca normal sörf aktiviteleri yapabilmektedir (Shah vd., 2018, s.4). Uygulama katmanı teknolojisi, blokzinciri ile gerçeklik arasındaki bağlantıyı sağlamaktadır (Wang vd., 2021, s.423).

Bu katmanda, akıllı sözleşmelerdeki talimatları adım adım yürüten ve mantıksal işlemleri gerçekleştiren sanal bir makine de bulunmaktadır. Uygulama katmanı, uygulama kullanıcıları ve uygulama operatörleri olmak üzere iki temel oyuncudan oluşmaktadır. Uygulama operatörleri; bir ya da birden çok blokzincire bağlanma yoluyla sistem kullanıcılarına, blokzincir durum görselleştiricileri, düğüm takip uygulamaları, cüzdan vb. gibi çeşitli hizmetler veren uygulamaların yönetimini sağlayan kişilerdir. Uygulama kullanıcıları ise ağ ile dolaylı olarak etkileşime geçmek için uygulama ara yüzünü kullanan kişilerdir (Blockchain Türkiye Platformu Teknoloji Çalışma Grubu, 2019a, s.24).

#### **2.4.2 Blokzincir Teknolojisinin İşleyişi**

Bir önceki bölümde blokzincir teknolojisinin kavramsal mimarisi, katmanlarına ayrılarak genel olarak ortaya konulmuştur. Bu bölümde ise söz konusu mimarinin çalışma süreci detaylı olarak açıklanacaktır. Blokzincir teknolojisinin gelişimine baktığımızda farklı özelliklere, kripto paralara ve süreçlere sahip birçok blokzincirin uygulamada olduğunu görmekteyiz. Bunların her birinin işleyişinin detaylı açıklanması mümkün olmasa da ilk ve en yaygın kullanılan Bitcoin blokzincirinin işleyişinin açıklanması genel olarak blokzincir teknolojisinin çalışma çerçevesinin anlaşılmasına yardımcı olacaktır. O nedenle bu aşamada

blokzincir teknolojisinin çalışma prensibi, Bitcoin blokzincirinin işleyişi baz alınarak açıklanacaktır.

Geleneksel sistemlerde olduğu gibi çevrimiçi işlemlerde de dolandırıcılık riskinin bertaraf edilmesi için üçüncü taraflar sürece dahil olmakta ve işleme aracılık ederek işlem güvenliğini ve doğruluğunu sağlamaktadır. Ancak bu aracılık faaliyeti de hem yüksek işlem maliyetlerini hem de bu üçüncü tarafın güvenilirliği risklerini doğurmaktadır. Bitcoin blokzinciri, internet üzerinden çevrimiçi işlemleri iki istekli taraf arasında güvenli bir şekilde gerçekleştirmek için kriptografik kanıtlar kullanarak üçüncü taraflara olan güven ihtiyacını ortadan kaldıran bir mekanizma sunmaktadır (Crosby vd., 2016, s.9).

Bitcoin blokzincirinde kullanılan temel kriptografik algoritma SHA-256 hash fonksiyonudur. Bununla birlikte Bitcoin protokolü; gizlilik, anonimlik ve merkeziyetsizlik gibi özellikleri sağlamak için çeşitli kriptografik teknolojileri de bir araya getirmektedir. Örneğin, dijital imzalar kullanılarak işlem güvenliği sağlanırken; hash fonksiyonları ile işlem bütünlüğü korunmaktadır. Ayrıca PoW mutabakat algoritmasıyla madencilik süreci merkeziyetsiz bir şekilde yönetilmekte ve blokzincirinin güvenilirliği artırılmaktadır. Bitcoin blokzincirinin karmaşık yapısı, bu kriptografik teknolojilerin birleşimiyle oluşturulmuş, güvenli ve dağıtık bir veri tabanı ve dijital ödeme sistemi sunmaktadır.

Tüm veri tabanı yönetim sistemlerinde olduğu gibi, blokzincir işlemlerinin merkezinde de verinin kendisi yer almaktadır. Kripto para birimleri için bu veri tabanına blokzinciri adı verilmektedir. Blokzinciri, her hesabın benzersiz bir adresle ilişkilendirildiği bir nevi para hesapları defteridir (Andolfatto vd., 2022, s.153). Zincirdeki en küçük birim "bloklar", deftere sırayla gönderilen, yani "zincire" eklenen işlem gruplarıdır (Swan, 2015, s.2). Blokzinciri defterine kaydedilen her blok, bir önceki bloğa dijital imzalı olarak bağlandığından kesin ve değiştirilemezdir. Diğer yandan ağa bağlanabilen herhangi biri, zincire kaydedilen verileri görebilmektedir yani defter herkese açıktır. Dolayısıyla blokzincir; iki taraf arasındaki işlemleri verimli, doğrulanabilir ve kalıcı bir şekilde kaydedebilen açık, dağıtılmış bir defterdir (Lansiti vd., 2017, s.4).

Yapılan genel açıklamaların ardından bir Bitcoin blokzinciri işlem sürecinde gerçekleşen her bir aşama aşağıda adım adım açıklanmıştır:

- a. Bitcoin Node (Düğümü) Oluşturma ve Blokzincire Erişim: Bitcoin Node kurulumu, herhangi bir bilgisayara (Windows, Linux, MacOS), “<https://bitcoincore.org/>” adresinden erişilen Bitcoin Core açık kaynak yazılımı indirilerek yapılır. Böylece Bitcoin blokzinciri ağındaki veriler ilgili cihaza indirilmiş olur. Burada veri indirimi ile ilgili (i) tüm veriler ve (ii) güncel veriler olmak üzere iki seçenek bulunmaktadır. Eğer ki sisteme katılım amacı; ağı desteklemek, blok doğrulamak ve madenci olmak ise tam düğüm (full node) olunması, yani tüm verinin indirilmesi ve saklanması gerekmektedir. Ancak amaç sadece kripto para işlemi yapmak ise o zaman hafif düğüm (lightweight node) olunması, yani sadece blok başlıklarının ve işlem köklerinin olduğu güncel verilerin indirilmesi yeterli bulunmaktadır.
- b. Bitcoin Cüzdanı Oluşturma: Her düğümün, blokzincir ağında işlem yapabilmesi için kripto cüzdanının<sup>40</sup> olması gerekmektedir. Bu nedenle Bitcoin Core yazılımı içinde “cüzdan oluştur” sekmesinden bitcoin cüzdanı oluşturulur. Cüzdan, kullanıcının belirlediği bir özel anahtar ve buna bağlı olarak hesaplanan bir genel anahtardan oluşmaktadır. Bu anahtarlar, kullanıcının işlemlerini imzalamada ve kimlik doğrulamasını sağlamada kullanılır. Genel anahtar, kullanıcının blokzincirdeki adres bilgisini gösterirken; özel anahtar ise cüzdana erişim ve işlem yapmayı sağlamaktadır. Özel anahtar kaybedilirse ilgili cüzdana bir daha erişim sağlanamaz.
- c. İşlem Oluşturma: A kişisi, B kişisine kripto para göndermek istediğinde; kendi özel şifresiyle erişim sağladığı kripto cüzdanı aracılığıyla, belirli bir miktar bitcoini, alıcı bilgisine B kişinin genel anahtarını yazarak gönderir. Böylece A kişinin dijital imzalı işlem talebi blokzincir ağındaki diğer düğümlere gönderilir.
- d. İşlem Havuzunda İşlem Taleplerinin Toplanması: Bu sırada A kişinin bu işlem talebinin yanı sıra ağdaki başka düğümler de işlem talebinde bulunmaktadır. Her bir düğüm aldığı işlem talebini doğrulayarak (gönderenin imzası, verinin gerçekliği, transfer tutarının hesaptaki mevcudiyeti gibi) komşu düğüme iletir ve ağ içerisinde yayılmasını sağlar. Böylece her düğümde eş kopyası olan bir sanal işlem havuzu oluşturulur (Dursun, 2020, s.13).

---

<sup>40</sup> “Kripto cüzdan” hakkında detaylı bilgi için bkz. s.74.

- e. Blok Oluşturma ve Madencilik: Blokzincir mekanizmasında blok oluşturma işlemini, merkeziyetsiz yapıyı ve ağın güvenliğini sağlama görevini madenci düğümler yerine getirmektedir. Madenciler, işlem havuzunda toplanan işlemler arasından blok içinde yer almasını istediklerini seçerler. Bu seçimi; işlem boyutu, işlem ücreti, işlem sırası ve öncelik sırası gibi kriterleri dikkate alarak yaparlar. Örneğin blok büyüklüğünün 1 MB olduğunu düşünelim; 1 MB'ı doldurabilecek en çok işlemi toplamaya çalışabilirler. Böylece küçük boyutlu daha çok işlem her birinden alınan işlem ücreti ile daha fazla gelir anlamına gelecektir. Ya da en yüksek işlem ücreti olan işlemlerin seçilmesi de bir başka seçenektir.
- f. Seçilen işlemler bloğun blok gövdesi bölümünde SHA-256 hash fonksiyonundan geçirilerek hash özetleri ile sıralanır ve bu işlemlerin hepsi birlikte Merkle kök hash değerini<sup>41</sup> oluşturur. Blok başlığında bulunan; hesaplanan Merkle kök hash değeri, üst blok hash değeri, zaman damgası ve gizli Nonce değeri birleştirilerek SHA-256 fonksiyonundan geçirilir ve bloğun hash değeri hesaplanır. Bloğun hash değerinin 30 adet başlangıç sıfırını içeren zorluk seviyesine<sup>42</sup> sahip olması gerekmektedir. Bu zorluk seviyesini karşılayan Nonce değeri bulmak için madenciler elektrik ve bilgisayar işlemci gücü kullanarak deneme yanılma yapar ve 10 dakika boyunca iş kanıtı bulmacasını çözmeye çalışırlar. 10 dakika sonunda uygun blok hash değerini karşılayan Nonce değeri ilk bulan madenci PoW<sup>43</sup>u üretir ve bloğu oluşturur.
- g. Bu aşamada madencilik türü; (i) yalnız, (ii) havuz veya (iii) bulut madencilik şekillerinden biri olabilir. Yalnız madencilik, madencilik için gereken donanım ve katlanılan maliyetlerinin tek başına üstlenildiği aynı zamanda madencilik ödülünün de tek başına kazanıldığı yöntemdir. Havuz madencilik, belirli sayıda madenciden oluşan bir gruba katılarak birlikte iş kanıtı üretildiği, yani daha az maliyete katlanıldığı ve blok ödülünün de paylaşıldığı yöntemdir. Bulut madencilik ise madencilik şirketlerinin sahip olduğu fiziksel donanımların kiralanması yoluyla sadece bir internet bağlantısı üzerinden madencilik yapılarak kazanç elde edilen yöntemdir.

---

<sup>41</sup> “Merkle Ağaçları” hakkında detaylı bilgi için bkznz. s.25.

<sup>42</sup> “Zorluk seviyesi” hakkında detaylı bilgi için bkznz. s.48.

<sup>43</sup> “PoW” hakkında detaylı bilgi için bkznz. s.42.

- h. Bloğun Ağda Paylaşımı: İş kanıtı bulmacasının herhangi bir madenci tarafından çözülmesiyle yeni oluşturulan blok ağdaki tüm madencilerle paylaşılır. Bu aşamada diğer madenciler artık daha fazla hesaplama yapmaya devam etmez, bulmaca çözümünü bırakırlar ve oluşturulan yeni bloğun doğrulamasını yapmaya başlarlar.
- i. Zincire Blok Ekleme (Doğrulama ve Mutabakat): Diğer madenciler, ağda paylaşılan yeni bloğun “bulunduğu iddia edilen” Nonce değerini, blok başlığına ekleyerek tekrar SHA-256 fonksiyonu uygularlar. Eğer Nonce değeri, belirlenen zorluk seviyesine uygun (30 sıfırlı) bir hash değeri üretiyorsa, bloğu doğrular ve kendi blokzincirlerine de eklerler.
- j. Ancak sistem saldırıya uğrayabilir veya rastlantısal olarak birden fazla madenci aynı anda blok oluşturabilir. Bu durumda, aynı yükseklikte birden fazla blok oluşur, yani ağda çatallanma<sup>44</sup> meydana gelir. Çatallanmanın düzeltilmesi için ise hangi bloğun kabul edileceği konusunda madencilerin %51'inin mutabakatı ile karara varılır ve zincir tekrar tek seviyeye getirilir.
- k. İşlemin Tamamlanması: Bloğun zincire eklenmesiyle birlikte A kişinin işlem talebi yerine getirilir ve A kişinin cüzdanından belirli miktarda kripto para azaltılıp, aynı miktar B kişinin cüzdanında artırılır.
- l. Ödül Alma: Son olarak iş kanıtı üreterek blok oluşturan ve bu bloğu, diğer madencilere doğrularak %51 çoğunluk mutabakatını sağlayıp blokzincirine “ilk ekleyen” madenci, güncel tutar 3.125 BTC'lik blok ödülünü kazanır. Madencilik işlemi havuz yöntemi ile yapıldıysa ödül havuzdaki madenciler arasında paylaşılır.

## 2.5 BLOKZİNCİR TEKNOLOJİSİNİN ÖZELLİKLERİ

Buraya kadar yapılan açıklamalarla blokzincir teknolojisinin çalışma prensibi ortaya konulmuştur. Bu bölümde ise blokzincir tabanlı sistemlerin genel performansının, teknolojinin kapsamının ve potansiyelinin daha iyi anlaşılabilmesi için bu yenilikçi teknolojinin temel özellikleri ve her bir özelliğin nasıl sağlandığı, bölüm alt başlıklarında detaylı bir şekilde ele alınacaktır.

---

<sup>44</sup> “Çatallanma” hakkında detaylı bilgi için bkz. s.50.

### 2.5.1 Merkeziyetsizlik (Decentralized)

Geleneksel merkezi bir ağda, işlemlerin güvenilir bir merkezi sunucu aracılığıyla doğrulanması gerekmektedir. Bu yaklaşım da tüm sistem iletişimde gecikmelerin yaşanmasına ve hesaplama maliyetlerinin artmasına neden olmaktadır (Murthy vd., 2020, s.205193). Diğer yandan güven ve gizlilik ihlalleri gibi üçüncü taraf risklerini de beraberinde getirmektedir. Blokzincir ağında ise merkezi sistemlerin aksine, herhangi bir üçüncü tarafın doğrulama yapmasına ihtiyaç duyulmadan eşler arasında (P2P) işlem gerçekleştirilebilmektedir (Monrat vd., 2019, s.5). Bu dağıtık ağa katılan tüm eşler (düğümler), internet üzerinden herkese açık olan bir defteri paylaşmakta, bu defterde kayıtlı işlem geçmişlerini saklamakta ve işlemlerin doğruluğunu kontrol ederek ağ üzerinden her bir eşteki defterin senkronizasyonunu sağlamaktadır (Zheng vd., 2019, s.3). Böylece blokzincir ile merkezi sistemlere ilişkin dezavantajlar bertaraf edilmekte; sunucu maliyetleri azaltılmakta, performans sorunları hafifletilmekte ve güven mekanizması sorunu çözümlenmektedir. (Monrat vd., 2019, s.5). Ayrıca ağa yönelik bir tehdit durumunda; merkezi sistemlerde tek bir düğüm zarar gördüğünde tüm sistem erişilemez olurken, blokzincir ağında birçok düğüm bulunduğundan ağ işlevini devam ettirmektedir (Chen vd., 2017, s.141).

Ancak dağıtık ağlarla ilgili de bir dezavantaj bulunmaktadır: düğümlerin, verileri farklı doğrulamaları dolayısıyla veri tutarlılığı sorunu ortaya çıkabilmektedir. Blokzincir ise bu riski, mutabakat algoritmaları ile çözmektedir.

Blokzincir teknolojisinin merkeziyetsiz ağ yapısı; “Dağıtık Defter Teknolojisi (Distributed Ledger Technology - DLT)” ve “Eşten Eşe Ağ (Peer to Peer Network - P2P)” bileşenleri ile sağlanmaktadır. DLT, verilerin bir merkezi otorite olmadan, birçok düğüm arasında dağıtıldığı bir veri yapısını ifade etmektedir. Bu veri yapısı, bir defterin ağdaki birçok noktada saklanması ve güncellenmesi prensibine dayanmaktadır. P2P ise her düğümün (eşin) ağda bağımsız olarak hem istemci hem de sunucu olarak işlev gördüğü bir ağ yapısını ifade etmektedir. Bu ağ yapısında düğümler, merkezi bir sunucuya ihtiyaç duymadan doğrudan birbirleriyle etkileşimde bulunabilmektedir.

### 2.5.2 Şeffaflık ve İzlenebilirlik (Transparency and Traceability)

Blokszincir; herkesin erişimine açık, tüm katılımcıların doğrulama için kayıtlarını blokszincir ağında yayınlatabildiği ve dolayısıyla bu ağda kayıtlı tüm verilerin diğer düğümler tarafından görülebilir olduğu dağıtık bir defterdir (Karakuş, 2021, s.195). Bu defterin birden fazla katılımcı arasında paylaşılıyor olması, ağdaki düğümler arasında şeffaflık sağlamaktadır (Yaga vd., 2018, s.2). Blokszincirin şeffaf yapısı; ağ genelinin onayı alınmadan yapılan veri manipölasyonlarını azaltarak sistemin bütünlüğünün korunmasına ve düğümlerin, işlem etkinliklerini izleyebilmesine katkıda bulunmaktadır (Karakuş, 2021, s.195).

Dağıtık defterde kayıtlı tüm işlemlerin düğümler tarafından izlenebilmesi ise ağın birbirine zincirlenmiş bloklardan oluşan yapısı ile mümkün olmaktadır. Blokszinciri bloklarında bulunan veriler, hash algoritmaları kullanılarak şifrelenmekte ve her blok için bir hash değeri hesaplanmaktadır. Bu hash değeri ise bir önceki bloğun hash değerini içererek hesaplanmakta ve böylece bloklar birbirine bağlanarak zincir oluşturmaktadır (Murthy vd., 2020, s.205194). Bu sayede de herhangi bir blok verisinden, başlangıç blok verisine kadar geçmiş tüm işlemlerin izlenmesi ve denetlenmesi sağlanabilmektedir.

### 2.5.3 Gizlilik ve Anonimlik (Privacy and Anonymity)

Her sistemin sahip olması gereken temel özelliklerden biri gizliliğdir. Merkezi sistemlerde, gizlilik daha kolay sağlanırken; dağıtık sistemlerde, gizliliğin sağlanması güçtür. Bunun nedeni, dağıtık sistemlerdeki şeffaflık ile gizlilik arasındaki doğal çatışmadır (Wüst vd., 2018, s.46). Blokszincir ise bu çatışmayı, asimetrik şifreleme teknikleri aracılığıyla çözmektedir.

Blokszincir ağında veriler, dijital imzalar (genel ve özel anahtarlar) ile güvence altına alınmakta ve sadece yetkili kişilerin erişimine sunulmaktadır. Bu sayede işlem detaylarına ilişkin gizlilik sağlanmaktadır. Gizliliği sağlayan dijital imzalar ise kriptö cüzdanlar aracılığıyla oluşturulmakta ve saklanmaktadır. Dolayısıyla kullanıcılar, kriptö cüzdanların bağlı olduğu adresler (açık anahtar) aracılığıyla ağ ile etkileşim kurmaktadır. Bu adresler merkezi bir otorite tarafından saklanmadığı için de kullanıcıların kimlikleri gizli kalmakta ve anonimlik sağlanmaktadır. Ayrıca ağ katılımcıları, işlem sahibinin gerçek kimliğini



bilmeden, anonim kimlik (takma ad - pseudonymity) üzerinden işlemin doğrulamasını da gerçekleştirebilmektedir.

Diğer yandan genel ve özel anahtarlar rastgele sayı dizileriyle elde edildiklerinden, matematiksel olarak bir kullanıcının genel anahtarından özel anahtarı tahmin edilememektedir (Karakuş, 2021, s.195). Bu nedenle anonim kimliklerin, gerçek dünyadaki sahiplerinin kimlikleriyle doğrudan ilişkilendirilmesi mümkün değildir (Chen vd., 2017, s.141). Böylece blokzincir ile hem şeffaflık hem de gizlilik ve anonimlik sağlanmış olmaktadır.

#### **2.5.4 Güvenlik ve Bütünlük (Security and Integrity)**

Merkezi sistemlerde; verilerin değiştirilmediğine ya da çalınmadığına ilişkin güvenceyi, veriyi saklayan aracı sağlamaktadır. Dağıtık sistemlerde ise bu güvenceyi sağlayacak bir aracı bulunmadığından, verinin güvenliği ve bütünlüğü konusunda risk söz konusudur. Blokzincir ise bu riski; dijital imzalar, kriptografik hash fonksiyonları ve mutabakat algoritmaları ile bertaraf etmektedir. Dijital imzalar ile veriye yetkisiz erişim engellenirken, hash fonksiyonları ile verideki en ufak değişikliğin tespit edilmesi sağlanmakta, mutabakat algoritmalarıyla da verinin gerçekliği ve bütünlüğü doğrulanmaktadır. Ayrıca önceki bloklara bağlanan zincirleme blok yapısı da genel olarak ağın güvenliğine ve bütünlüğüne katkı sağlamaktadır. Bu yapı sayesinde, kişisel çıkarlar doğrultusunda veri bütünlüğünün bozulması engellenmekte, veri güvenliği sağlanmakta ve merkezi bir otoriteye olan ihtiyaç ortadan kalkmaktadır (Garg vd., 2021, s.504).

#### **2.5.5 Değişmezlik ve Dayanıklılık (Immutability and Tamper Resistant)**

Geleneksel sistemlerde, verilerin değiştirilmesi için sadece veriyi saklayan merkezin manipülasyona uğraması yeterlidir. Dağıtık sistemlerde ise veri tüm düğümlerde saklandığı için, her bir düğümün değiştirilmesi gerekmektedir. Teorik olarak tüm düğümlere yapılan bir saldırı ile bu değişiklik gerçekleştirilebilmektedir. Ancak blokzincir teknolojisi bu riski, zincirleme blok yapısı, dağıtık defter (DLT) ve mutabakat algoritmaları (PoW) ile azaltarak pratikte gerçekleştirilmesi imkânsız hale getirmektedir.

Blokzincir ağına yayılan işlemler, düğümler tarafından bloklar haline getirilmekte ve bu bloklar ağın çoğunluğunun onayını alarak zincire kaydedilmektedir. Ardından da tüm

düğümünün, onaylanmış yeni bloğu kendi zincirlerine eklemesiyle düğümlerdeki defter kopyaları aynı olmaktadır. Bu nedenle düğümlerin bilgisi olmadan, zincire blok eklenmesi veya kaydedilen bloklardaki verilerin değiştirilmesi mümkün değildir (Zheng vd., 2018, s.357).

Ayrıca verilerin değiştirilmeye çalışılması halinde de bloklar hash fonksiyonlarıyla birbirlerine bağlı olduklarından, önceki tüm blokların hash verilerinin değiştirilmesi gerekir ki bu, yapılması gereken iş miktarı göz önüne alındığında astronomik derecede zor bir görev olarak kabul edilmektedir. Dolayısıyla, verilerin herhangi bir şekilde manipüle edilmesi veya tahrif edilmesi ağ tarafından tespit edilmektedir. Bu nedenle blokzinciri neredeyse kurcalamaya karşı dayanıklıdır ve değiştirilemez bir dağıtılmış defterdir (Monrat vd., 2019, s.5).

#### **2.5.6 Denetlenebilirlik ve İnkâr Edilemezlik (Auditability and Undeniability)**

Blokzincir ağında tüm işlemler, zaman damgası ve dijital imza ile birlikte ağın çoğunluğu tarafından onaylanan dağıtık deftere kaydedilmektedir. Ağ çoğunluğunun onayı işlemin geçerliliğini doğrularken, zaman damgası işlemin yapıldığı anı ve dijital imza ise işlemi gerçekleştiren kişinin kimliğini belirtmektedir. Blokzincire kaydedilen bilgiler şeffaf ve değiştirilemez olduğu için de dağıtık ağ üzerindeki herhangi bir düğüm aracılığıyla geçmiş işlem kayıtlarına erişilerek kolayca gözlem ve denetleme yapılabilmektedir (Zheng vd., 2018, s.357). Bitcoin blokzincirinde tüm işlemler yinelemeli olarak izlenebildiğinden veri denetimi kolaylıkla yapılabilmektedir. Ancak paranın hesaplar arasında dolaşıyor olması, kaynağına kadar izinin sürülmesini zorlaştırmaktadır (Monrat vd., 2019, s.5).

Diğer yandan dijital imza sistemindeki genel anahtar, işlemi doğrulamak için kullanılan anonim kimliği temsil ederken; özel anahtar, sadece kullanıcının bildiği ve işlemi yapan kişinin kimliğini kanıtlamak için kullanılan bir şifredir. İşlemler bu özel şifre ile imzalandığı için kullanıcının yapılan işlemi inkâr etmesi mümkün olmamaktadır.

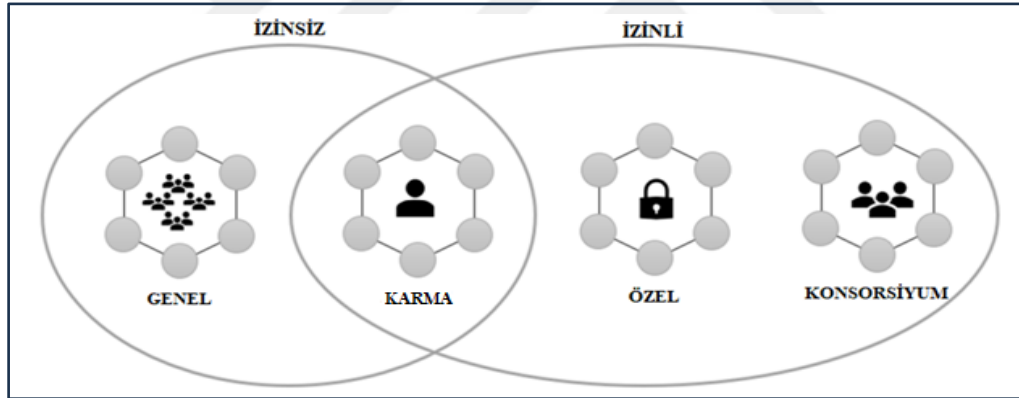
#### **2.5.7 Otonom Sistem (Autonomous System)**

Blokzincir teknolojisi; mutabakat algoritmaları, dijital imza vb. gibi birçok algoritmanın birleştiği bir işlem sürecine dayanmaktadır. Dolayısıyla böylesi bağımsız bir sistemde katılımcıların herhangi bir şekilde sürece doğrudan müdahale etmesi mümkün

olmamaktadır. Sistemde düzeltilmesi gereken bir hata ile karşılaşılması halinde ise yazılımın açık kaynak kodlu olması sebebiyle herkes yazılım yükseltme önerisinde bulunabilmekte, ancak resmi olarak uygulanabilmesi için ağdaki belirli sayıda madencilerin onayının alınması gerekmektedir. Bu mekanizma, blokzinciri sisteminde büyük değişiklikler yapılmasını sınırlandırırken, sistemin kararlı bir yapı sergilemesine katkı sağlamaktadır (Chen vd., 2017, s.141).

## 2.6 BLOKZİNCİR TÜRLERİ

Blokzincir, İnternet gibi teknolojik bir altyapıdır. Tıpkı internet üzerinde farklı protokollere sahip internet sitelerinin hizmet vermesi gibi, blokzincir teknolojisinin üzerinde de farklı protokoller kullanılarak çeşitli platformlar ve uygulama yaklaşımları geliştirilebilmektedir (Usta vd., 2019, s.32). Tüm bu platform ve uygulamalar, ağa erişim (verileri okuma) izni ve mutabakat sürecine katılım (işlem yazma) izni özelliklerine göre Şekil 2.22’de gösterildiği üzere dört ana kategoride sınıflandırılmış ve bölüm alt başlıklarında tanımlanmıştır.



Şekil 2.22: Blokzincir Türleri.

[Koç, 2022, s.34]

### 2.6.1 Genel (Public) Blokzincir

Genel blokzincir, herkesin kullanımına açık blokzincirdir. Gerekli donanıma ve internete sahip herhangi biri, hiçbir izin almadan ağa erişim sağlayıp verileri okuyabilir ve mutabakat sürecine katılıp işlem yapabilir. Tüm ağ katılımcıları (düğümler), blokzincirde kayıtlı işlemlerin yani dağıtık defterin bir eşine sahiptir. Dolayısıyla şeffaf ve değiştirilemezdir.

Diğer yandan genel blokzincir ağında katılımcı sayısı fazla olduğundan, işlemlerin tamamlanması ve blokların yayılması uzun sürmektedir. Ağ güvenliğinin sağlanması için ise

katı kısıtlamalar uygulanmaktadır. Bu nedenle genel blokzincirler, sınırlı işlem hacmine ve yüksek gecikme sürelerine sahiptir (Zheng vd., 2018, s.357). İlk blokzincir uygulaması Bitcoin, genel blokzincirlere örnektir.

### **2.6.2 Özel (Private) Blokzincir**

Özel blokzincir; herkesin kullanımına açık olmayan blokzincirdir. Ağa erişim yalnızca, mutabakat sürecini yönetenlerin izni ile sağlanabilmektedir. Mutabakat sürecini yöneten tek bir kuruluş vardır (Zheng vd., 2018, s.357) ve kendi içinde ya da diğer kuruluşlarla veri paylaşımı için blokzincir sistemini kullanmaktadır (Karakuş, 2021, s.179). Dolayısıyla erişilebilirlik, merkezi bir otoritenin iznine bağlıdır (Murthy vd., 2020, s.205194). Bu nedenle de ağı sınırlı, kimliği ve yetki düzeyi belli bir katılımcı mevcudu bulunmaktadır ve bu da verilerin değiştirilebilirlik riskini artırmaktadır. Daha çok genel ağda veri bulundurmaya sakıncalı bulan işletmeler ve organizasyonlar bu blokzinciri tercih etmektedir (Usta vd., 2019, s.34). Oylama, dijital kimlikler, servet sahipliği, tedarik zinciri yönetimi ve diğer uygulamalar için özel blokzincir kullanılmaktadır (Garg vd., 2021, s.506).

### **2.6.3 Konsorsiyum (Consortium) Blokzincir**

Konsorsiyum blokzinciri; herkesin kullanımına açık olmayan, ancak özel blokzincirden farklı olarak mutabakat sürecini ağdaki birkaç düğümün yönettiği, izinli ve kısmen merkezi olmayan bir yapıya sahip blokzincirdir. Önceden seçilen düğümler, kimlerin ağa erişebileceğini (verileri okuyacağını) ve kimlerin madencilik sürecine katılacağını (işlem yazacağını) seçme yetkisine sahiptir. Ayrıca doğrulanan blokların geçerliliği, bu düğümlerin imzalarını içermelerine bağlıdır (Tanrıverdi vd., 2019, s.206). Hatta okuma ve yazma izinlerinin sınırlı mı yoksa herkese açık mı olacağına da (Karakuş, 2021, s.179), yani seçilecek blokzincir hizmet türüne (Murthy vd., 2020, s.205194) de bu düğümler karar vermektedir. Bu blokzinciri daha çok, bankalar ve kamu kurumları tercih etmektedir (Garg vd., 2021, s.506).

### **2.6.4 Karma (Hybrid) Blokzincir**

Karma blokzincir; hem merkeziyetsiz yapıların açıklık, güvenlik ve bütünlük avantajlarından hem de merkezi yapıların gizlilik, verimlilik ve ölçeklenebilirlik avantajlarından yararlanmak amacıyla genel ve özel blokzincir altyapılarının birleştirildiği

blokzincirdir. Bu tür bir blokzincirde, ağdaki verilerin bir kısmı genel erişime açıkken, bir kısmı da sadece özel katılımcıların erişimine açıktır (Garg vd., 2021, s.506).

### 2.6.5 Blokzincir Türlerinin Karşılaştırması

Bu bölümde detaylı açıklanan genel, özel, konsorsiyum ve karma blokzincir türleri çeşitli özellikleri itibarıyla aşağıdaki Tablo 2.8’de karşılaştırılarak özetlenmiştir.

**Tablo 2.8:** Blokzincir Türlerinin Karşılaştırılması.

| Özellikleri                | Blokzincir Türleri                        |                                                       |                                               |                             |
|----------------------------|-------------------------------------------|-------------------------------------------------------|-----------------------------------------------|-----------------------------|
|                            | Genel                                     | Özel                                                  | Konsorsiyum                                   | Karma                       |
| <b>Doğası</b>              | Açık ve Dağıtık                           | Kontrollü ve Kısıtlı                                  | Kontrollü ve Kısıtlı                          | Hem Dağıtık Hem Kısıtlı     |
| <b>Katılımcılar</b>        | Anonim ve Dayanıklı                       | Tanımlı ve Güvenilir                                  | Tanımlı ve Güvenilir                          | Hem Anonim Hem Tanımlı      |
| <b>Mutabakat Belirleme</b> | Tüm madenciler                            | Bir organizasyon                                      | Seçilmiş düğümler                             | Zincir türüne göre değişken |
| <b>Merkeziyetçilik</b>     | Hayır                                     | Evet                                                  | Kısmen                                        | Kısmen                      |
| <b>Mutabakat Süreci</b>    | PoW, PoS                                  | PBFT, PoA                                             | PBFT                                          | Zincir türüne göre değişken |
| <b>Okuma/Yazma İzni</b>    | İzinsiz                                   | İzinli                                                | İzinli                                        | Hem İzinsiz Hem İzinli      |
| <b>Değiştirilemezlik</b>   | Mümkün değil                              | Değiştirilebilir                                      | Kısmen değiştirilebilir                       | Mümkün değil                |
| <b>Verimlilik</b>          | Düşük                                     | Yüksek                                                | Yüksek                                        | Yüksek                      |
| <b>Ölçeklenebilirlik</b>   | Düşük                                     | Yüksek                                                | Yüksek                                        | Yüksek                      |
| <b>İşlem Onay Sıklığı</b>  | Uzun                                      | Kısa                                                  | Kısa                                          | Zincir türüne göre değişken |
| <b>Enerji Tüketimi</b>     | Yüksek                                    | Düşük                                                 | Düşük                                         | Orta                        |
| <b>Şeffaflık</b>           | Yüksek                                    | Düşük                                                 | Düşük                                         | Orta                        |
| <b>Maliyet</b>             | Yüksek                                    | Düşük                                                 | Düşük                                         | Orta                        |
| <b>Örnekler</b>            | Bitcoin, Ethereum, Litecoin, Factom, Dash | Multichain, Blockstack, Bankchain, Hyperledger Fabric | Ripple, Hyperledger, Banking Digital Currency | Dragonchain, Corda, Quorum  |

**Kaynak :** [Monrat vd., 2019, s.6; Koç, 2022, s.39]’dan esinlenilerek yazar tarafından düzenlenmiştir.

## 2.7 BLOKZİNCİR PLATFORMLARI

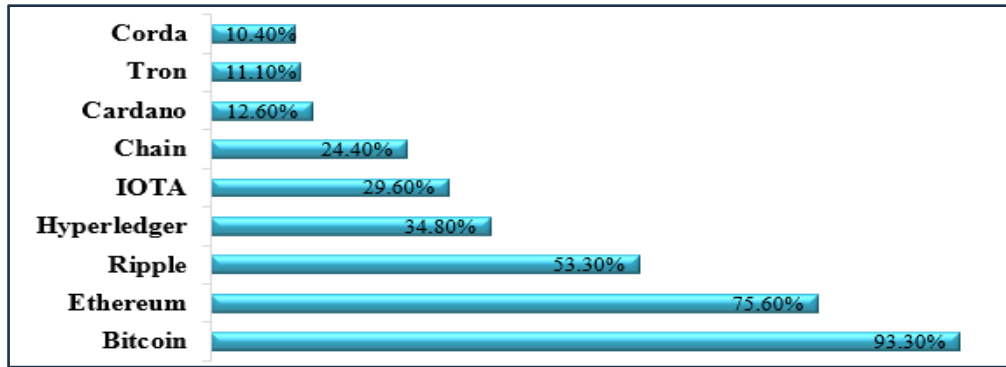
Blokzincir teknolojisinin evrimi, kripto paralardan akıllı sözleşmelere ve merkeziyetsiz uygulamalara kadar geniş bir yelpazede farklı çözümler sunarak birçok sektörde ilgi ve talep uyandırmaktadır. Bu hızlı ilerleme, teknolojinin daha fazla uygulama alanı bulmasını ve çeşitli ihtiyaçları karşılayan yeni platformların ortaya çıkmasını teşvik etmektedir. Nitekim

en çok bilinen kripto para veri platformlarından CoinMarketCap'te 28.07.2024 tarihi itibarıyla listelenen, 234'ü aktif olmak üzere toplam 315 adet blokzincir platformu ve 10.000'den fazla kripto para birimi hakkında kapsamlı bilgiye ulaşılabilmektedir. Tablo 2.9'da CoinMarketCap (<https://coinmarketcap.com/>)'te ilgili tarihte listelenen en yüksek piyasa değerine sahip ilk 10 blokzincir platformu sıralanmış ve piyasa değeri ile kripto para birimlerinin fiyatına ilişkin bilgiler verilmiştir.

**Tablo 2.9:** En Yüksek Piyasa Değerine Sahip Blokzincir Platformları.

|    | Platform Adı                                                                                  | Sembolü | Piyasa Değeri       | Fiyatı      |
|----|-----------------------------------------------------------------------------------------------|---------|---------------------|-------------|
| 1  |  Bitcoin     | BTC     | \$1,342,546,545,651 | \$68,038.21 |
| 2  |  Ethereum    | ETH     | \$393,537,260,426   | \$3,273.25  |
| 3  |  Tether USDt | USDT    | \$114,414,483,624   | \$0.9999    |
| 4  |  Solana      | SOL     | \$86,428,720,776    | \$185.98    |
| 5  |  BNB         | BNB     | \$84,813,170,701    | \$581.16    |
| 6  |  USDC       | USDC    | \$34,151,288,600    | \$0.9999    |
| 7  |  XRP       | XRP     | \$33,709,805,540    | \$0.6024    |
| 8  |  Dogecoin  | DOGE    | \$19,068,078,335    | \$0.1312    |
| 9  |  Toncoin   | TON     | \$16,485,739,731    | \$6.55      |
| 10 |  Cardano   | ADA     | \$14,788,779,437    | \$0.4119    |

**Kaynak:** [CoinMarketCap <https://coinmarketcap.com/>]



**Şekil 2.23:** Türkiye’de Bilinen Blokzincir Platformları.

[Deloitte & TUSIAD, 2018, s.12]

Bu platformlardan Türkiye’de en çok tanınırlığa sahip olanları ise Şekil 2.23’te verilmiştir. Buna göre Deloitte & TUSIAD (2018)’ın yapmış olduğu Türkiye Blokzincir Araştırması kapsamında; Türkiye’de en çok bilinen dört platformun Bitcoin, Ethereum, Ripple ve

Hyperledger olduđu gör÷lmektedir. Söz konusu platformlar Tablo 2.10'da karşılaştırmalı olarak tanımlanmıştır.

**Tablo 2.10:** Blokzincir Platformlarının Karşılaştırması.

| Özellikler                 | Bitcon                                                                                                              | Ethereum                                                                                                                    | Ripple                                                                                                                                                                | Hyperledger                                                                              |
|----------------------------|---------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| <b>Geliştiricisi</b>       | Satoshi Nakamoto                                                                                                    | Ethereum Vakfı                                                                                                              | Ripple Labs Inc.                                                                                                                                                      | Linux Vakfı                                                                              |
| <b>İlk Sürüm Tarihi</b>    | 2009                                                                                                                | 2013                                                                                                                        | 2012                                                                                                                                                                  | 2015                                                                                     |
| <b>Kripto para Birimi</b>  | BTC                                                                                                                 | ETH                                                                                                                         | XRP                                                                                                                                                                   | -                                                                                        |
| <b>Amacı</b>               | Merkezi bir otoriteye ihtiyaç duymadan güvenli ve şeffaf bir şekilde değer transferi yapabilen bir sistem sağlamak. | Merkezi olmayan uygulamaların (dApps) ve dağıtılmış uygulama platformlarının geliştirilmesini ve çalıştırılmasını sağlamak. | Finansal kurumlar ve bankalar arasında sınır ötesi ödemelerin daha hızlı (gerçek zamanlı), daha güvenli ve düşük maliyetli bir şekilde gerçekleştirilmesini sağlamak. | İşletmelerin kendilerine özel tasarlanmış blokzincir ağlarını geliştirmelerini sağlamak. |
| <b>Depolanan Veri Tipi</b> | Kripto para işlemleri                                                                                               | Kripto para, Dijital varlık, Akıllı sözleşme                                                                                | Finansal işlemler, Ödeme kanalları, Kullanıcı hesap ve bakiyeleri                                                                                                     | Chaincode, Akıllı sözleşme                                                               |
| <b>Programlama Dili</b>    | Script                                                                                                              | Solidity/Scrip EVM                                                                                                          | C++, JavaScript, Python                                                                                                                                               | Go/Java Docker                                                                           |
| <b>Blokzincir Türü</b>     | İzinsiz                                                                                                             | İzinsiz                                                                                                                     | İzinli                                                                                                                                                                | İzinli                                                                                   |
| <b>Katılım Şekli</b>       | GitHub'dan kaynak kodu alınır.                                                                                      | GitHub'dan kaynak kodu alınır.                                                                                              | GitHub'dan kaynak kodu alınır.                                                                                                                                        | Ağ üyelik hizmetlerine kimlik için kayıt olunarak kullanıcı kaynak kodu alınır.          |
| <b>Blok Ekleme Süresi</b>  | 10 dkk                                                                                                              | 12-14 sn                                                                                                                    | 3-5 sn                                                                                                                                                                | 1 sn                                                                                     |
| <b>İşlem Büyüklüğü</b>     | Ortalama 250 bayt                                                                                                   | Teoride sınır yok                                                                                                           | Yapılandırılabilir                                                                                                                                                    | Yapılandırılabilir                                                                       |
| <b>Mutabakat Yöntemi</b>   | PoW                                                                                                                 | PoW / PoS                                                                                                                   | RPCA (kendi yöntemi)                                                                                                                                                  | PBFT / SBFT                                                                              |
| <b>Merkle Ağaç Tipi</b>    | Merkle Tree                                                                                                         | Merkle Patricia Tree                                                                                                        | -                                                                                                                                                                     | Merkle Bocket Tree                                                                       |

**Kaynak :** [Aslan vd., 2022, s.58; Murthy vd., 2020, s.205195 ; Zhai vd., 2019, s.2 ; <https://ripple.com/>]'dan yararlanılarak yazar tarafından düzenlenmiştir.

Sonuç olarak, blokzincir platformlarının sayısı gün geçtikçe artmakta ve her biri farklı kullanım senaryolarına yönelik yenilikçi çözümler sunarak blokzincir ekosistemini zenginleştirmektedir.

## 2.8 BLOKZİNCİR TEKNOLOJİSİNİN KULLANIM ALANLARI

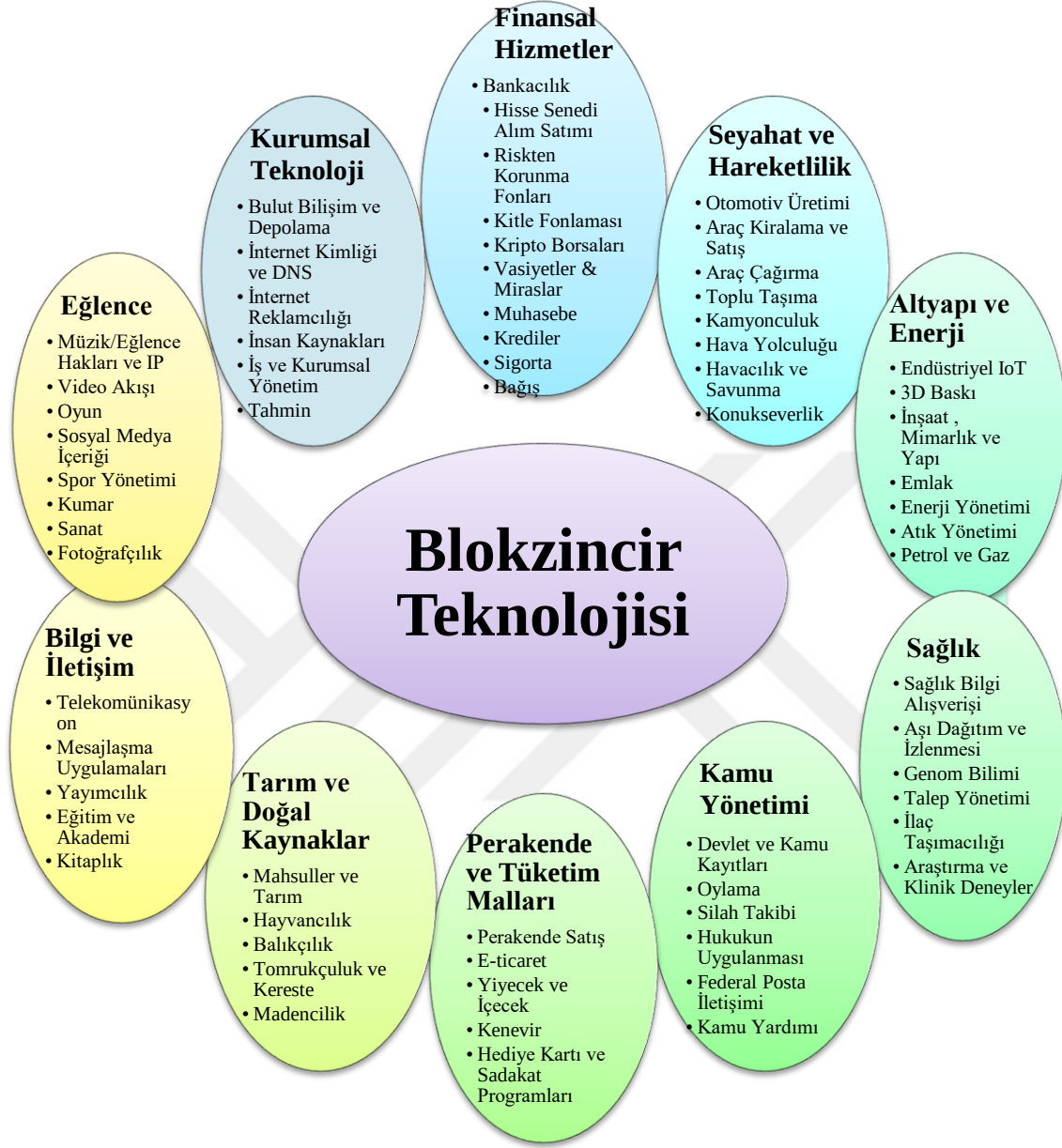
Blokzincir teknolojisi, son yıllarda dijital çağın en yenilikçi gelişmelerinden biri olarak öne çıkmaktadır. Merkeziyetsiz ve şeffaf bir veri yapısı sunarak, güvenli ve değiştirilemez veri kayıtları oluşturmaktadır. Bu temel özellikleri blokzincir teknolojisini, sadece kripto para birimi uygulamaları ile sınırlandırmayıp, birçok farklı sektörde devrim niteliğinde uygulama alanları için uygun hale getirmektedir. Finansal hizmetlerden sağlık sektörüne, tedarik zincirinden kimlik doğrulama sistemlerine kadar geniş bir yelpazede kullanım potansiyeline sahiptir. Her sektör, blokzincirin sunduğu güvenlik, şeffaflık ve verimlilik avantajlarından yararlanarak mevcut süreçleri optimize edebilmekte ve yenilikçi çözümler geliştirebilmektedir.

Deloitte & TUSIAD (2018, s.15)'ın Küresel Blokzinciri anketinde, katılımcıların beklentilerine göre küresel düzeyde blokzincir teknolojisinden en çok etkilenecek olan alanların; finans (%78.1), bilgi teknolojileri (%60.9), tedarik zinciri ve lojistik (%59.4), dijital haklar yönetimi (%53.9), ticaret (%47.7), hukuk (%41.4), nesnelerin interneti (%39.8), muhasebe (%36.7) ve kamu sektörü (%27.3) olacağı belirtilmiştir.

Gartner (2017)'in raporuna göre; 2022 yılı itibarıyla blokzincir tabanlı başarılı uygulamaların hayata geçirileceği, küresel düzeyde ekonomik katma değer 2026 yılı sonrasında yaratılacağı ve 2030 yılında blokzincirin pazar büyüklüğünün 3.1 Trilyon \$'a ulaşacağı ifade edilmiştir. Aynı raporda 2030 yılında %31'i imalat, %14'ü iletişim, medya ve hizmet, %10'u perakende, %10'u banka ve menkul kıymetler, %8'i toptan ticaret, %7'si kamu, %7 ulaşım, %5'i sağlık, %3'ü eğitim, %3'ü yardımcı programlar ve %2'si sigorta sektöründe olmak üzere blokzincir kullanımının birçok alana yayılacağı öngörülmektedir. Bu tahminlerin gerçekleşmesi halinde blokzincir kullanımına ilişkin günümüzde önemle söz ettiğimiz alanlar gelecekte blokzincir sektörünün ufak bir parçasını oluşturacaktır (İlkbahar, 2019).

Teknoloji pazarı araştırma ve analiz şirketi CB Insights'in 2022 Blokzincir Raporu'na göre ise, 65 büyük sektörde blokzincir teknolojisinin dönüşüm yaratması olasıdır. Söz konusu sektörler Şekil 2.24'te sınıflandırılmıştır.





**Şekil 2.24:** Blokzincir Teknolojisinin Kullanılabileceği Çeşitli Sektörler ve Alanlar.

[CB Insights, 2022]'den yararlanılarak yazar tarafından düzenlenmiştir.

Blokzincir teknolojisinin hali hazırda uygulama örneklerinin bazıları uygulama alanı ve kullanım amacı / sağladığı faydaları itibarıyla Tablo 2.11'de kısaca açıklanmıştır.

**Tablo 2.11: Blokzincir Teknolojisinin Uygulama Alanları.**

| Uygulama Alanı                                             | Kullanım Amacı/Sağladığı Fayda                                                                                                                                                                                                                                                                                                                                      | Uygulama Örneği                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1<br><b>Uluslararası Ödemeler ve Bankacılık Sistemi</b>    | Blokzincir ve akıllı sözleşmelere dayanan DeFi uygulamaları sayesinde finans kurumlarına duyulan ihtiyaç azaltılarak uluslararası ödemelerin yasal engellere takılmadan, düşük maliyetli ve hızlı bir şekilde yapılmasını sağlar.                                                                                                                                   | Uluslararası para transferinde Ripple'ın RippleNet ödeme ağı, büyük ölçekli bankacılık işlemlerinde J.P. Morgan Chase'in JPM Coin stablecoinini bu alana yönelik uygulamalarıdır.                                                                                                        |
| 2<br><b>Kripto Para (Dijital Para)</b>                     | Blokzincirin ilk uygulama alanıdır. Bitcoin'den sonra çok sayıda altcoin dijital para olarak ortaya çıkmıştır. Fiziksel paranın yerini alacağı düşünülmektedir. Birçok merkez bankası kendi dijital paralarını çıkarmak üzere çalışmalar yapmaktadır. Diğer yandan blokzincir üzerinden yatırım uygulamaları (hisse senedi alım/satımı gibi) da geliştirilmektedir. | BTC, ETH, USDC, USDT vb. gibi piyasaya sürülmüş birçok kripto paranın yanında Türkiye'de "Dijital Türk lirası" için çalışmalarını sürdürmektedir. Ayrıca Takasbank, dijital altın alışverişi için BİGA projesini geliştirmektedir.                                                       |
| 3<br><b>Kredi Uygulamaları ve Girişim Sermayesi Temini</b> | Blokzincir platformları, akıllı sözleşmeler aracılığıyla aracılar gerek kalmadan bireyler arasında doğrudan kredi verilmesini ve mikro kredilerin yönetilmesini sağlar. Ayrıca firmalar token ihraç ederek yatırımcılardan büyük miktarda girişim sermayesi toplayabilirler.                                                                                        | Ethereum tabanlı BankSocial, Dharma Labs ve Bloom bu alana yönelik girişimlere örnektir.                                                                                                                                                                                                 |
| 4<br><b>Muhasebe</b>                                       | Muhasebe sürecinin ihtiyaç duyduğu ticari belgeler, beyannameler ve elektronik tabloların kayıt ve takibinin blokzincir teknolojisi ve yapay zekâ kullanılarak yapılması, muhasebe sürecinin otomatikleştirilmesini ve dolayısıyla insan hatasının ve dolandırıcılığın azaltılmasını sağlar.                                                                        | PwC, kripto paralar için denetim hizmeti; Deloitte, blokzincir tabanlı yazılım; EY, dijital varlıkların incelenmesi için Blockchain Analyzer'i geliştirmiştir. KPMG ise blokzincir hakkında çeşitli proje ve programlara yatırım yapmıştır.                                              |
| 5<br><b>Tedarik Zinciri Yönetimi</b>                       | Ürünün üreticiden nihai tüketiciye ulaşana kadar gerçekleşen karmaşık süreçlerinin belgelendirme ve kontrol aşamaları maliyet ve zaman yükü yaratmaktadır. Blokzincir ve akıllı sözleşmeler ile bu süreç otomatikleştirilerek insan hatası, zaman ve maliyet azaltılır. Böylece şeffaflık artarken israfın azalması sağlanır.                                       | Blockverify (sahte ürünlere yönelik tespit ve önleme), Everledger (mücevherlerin orijinallik tespitine ve sahiplik kaydına yönelik), SyncFab (üretim süreçlerine yönelik), Shipchain ve Openport (lojistik süreçlerine yönelik izleme ve doğrulama) gibi şirketler çözüm geliştirmiştir. |
| 6<br><b>Perakende Sektörü</b>                              | Üretici ile tüketici arasında aracılık yapan mağaza ve marketlere olan ihtiyaç, blokzincir teknolojisi ve akıllı sözleşmeler ile ortadan kaldırılarak güven ve maliyet tasarrufu sağlanır.                                                                                                                                                                          | Openbazaar, ob1 gibi firmalar bu alana yönelik çalışmalar geliştirmektedir. Ayrıca Microsoft ve ConsenSys ortaklığında Louis Vuitton lüks ürünleri için Aura platformu geliştirildi.                                                                                                     |

**Tablo 2.11:** Blokzincir Teknolojisinin Uygulama Alanları (Devam).

|    | Uygulama Alanı                                 | Kullanım Amacı/Sağladığı Fayda                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Uygulama Örneği                                                                                                                                                                                                                                                                             |
|----|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7  | <b>Talep Tahmini</b>                           | Blokzincir birçok işlemin kayıt altına alındığı dağıtık bir veri tabanıdır. Dolayısıyla blokzincir ile kaydedilen veriler üzerinden istatistikî sonuçlara ulaşarak analiz ve yorum yapılabilmekte ve bu sonuçlarla müşteri gereksinimleri ve taleplerine yönelik tahminlerde bulunulabilmektedir.                                                                                                                                                                                                                                                                                                                          | Küresel piyasalara yönelik talep tahmini yapan Augur firması Ethereum blokzinciri üzerinde protokoller geliştirmektedir.                                                                                                                                                                    |
| 8  | <b>Müşteri Tanıma (Know Your Customer-KYC)</b> | Geleneksel sistemlerde çeşitli işletme ve kurumlar, müşterilerine ilişkin bilgileri birbirlerinden bağımsız olarak saklamaktadır. Bu durum hem yüksek maliyet ve verimsizliğe yol açmakta hem de müşteri bilgilerinin satılması ve çalınması riskini doğurmaktadır. Blokzincir bu riskleri ortadan kaldırarak bilgi paylaşımını müşterinin kontrolüne bırakmakta ayrıca bilgilerde değişiklik olması halinde erişim yetkisi olan kurumlara değişikliğin otomatik olarak iletilmesini sağlamaktadır.                                                                                                                        | Cambridge Blockchain, uPort, KYC-Chain, Civic ve SelfKey girişimleri bu alana yönelik çözümlerdir.                                                                                                                                                                                          |
| 9  | <b>Sağlık Uygulamaları</b>                     | Sağlık uygulamalarında blokzincir kullanılması, hasta verilerinin güvenli ve değiştirilemez bir şekilde saklanması sağlar, veri doğruluğunu artırır ve hasta bilgilerini şeffaf bir şekilde yönetir. Bu teknoloji, hasta onay süreçlerini ve veri paylaşımını kolaylaştırırken, ilaç tedarik zincirinin yanı sıra klinik araştırmaları da daha güvenilir hale getirir. Ayrıca sağlık sigortası ve faturalama işlemlerinde dolandırıcılığı azaltır ve ödemelerin doğruluğunu artırır. Diğer yandan genomik araştırmalarının saklandığı merkezi bulut veri tabanlarının manipülasyonu riski de dağıtık sistem ile azaltılır. | Doktorların çalışma lisanslarının doğrulamasında Hashed Health; Sağlık veri yönetiminde HealthVerity; DNA veri tabanı EncrypGen; Chronicled'in büyük ilaç devleriyle geliştirdiği ilaç tedarik zincirine yönelik MediLedger sağlık alanında blokzincir kullanımı örneklerinden bir kaçıdır. |
| 10 | <b>Sigorta İşlemleri</b>                       | Blokzincir teknolojisi ve akıllı sözleşmeler, sigortalama sürecini otomatikleştirerek hatalı işlem ve dolandırıcılığın önlenmesini dolayısıyla veri güvenliğinin artmasını sağlar. Ayrıca süreç daha hızlı tamamlanırken işlem maliyetlerinin azalmasına da katkıda bulunur.                                                                                                                                                                                                                                                                                                                                               | Oracle, genel olarak sigortacılık sektörüne yönelik Aeternity çözümünü; EY ise, Guardtime şirketi ile birlikte deniz sigortasına yönelik Insurwave platformunu geliştirmiştir.                                                                                                              |
| 11 | <b>Emlak Sektörü</b>                           | Mülk alım satımı sırasında ve sonrasında karşılaşılan şeffaflık eksikliği, çok miktarda evrak işi (bürokrasi), olası dolandırıcılık ve kamu kayıtlarındaki hatalar blokzincir teknolojisi kullanılarak bertaraf edilebilir. Böylece kayıt tutma ihtiyacı ve işlem maliyetleri azalırken işlem hızının artması sağlanır. Arazi tapuları, mülkiyet senetleri, hacizlerin doğrulanması ve devir işlemleri güvenle yapılabilir.                                                                                                                                                                                                | Akıllı sözleşme platformu Propy, güvenli ev satın alma çözümü; Ubitquity ise tapu ve ipotek şirketleri için yazılım çözümü sunmaktadır.                                                                                                                                                     |

**Tablo 2.11:** Blokzincir Teknolojisinin Uygulama Alanları (Devam).

| Uygulama Alanı                                    | Kullanım Amacı/Sağladığı Fayda                                                                                                                                                                                                                                                                                                                          | Uygulama Örneği                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12 <b>Endüstriyel Nesnelerin İnterneti (IIoT)</b> | Blokzinciri ağı, çok sayıda cihazın birbiri ile iletişimini sağlamak için bir merkeze ihtiyaç duymayan genel bir kayıt defteri görevi üstlenebilir. Bu sayede tüm cihazlar, yazılım güncellemelerini, hatalarını veya enerji kullarımlarını yönetmek için birbirleriyle otonom bir şekilde iletişim kurabilirler.                                       | Helium ve NetObjex, internet altyapısı ve akıllı şehir ulaşımında IoT cihazları için blokzincir ağı başlatmıştır. Xage, endüstriyel cihazlar için veri güvenliğinde blokzincir kullanmaktadır. Hyundai Merchant Marine ve Samsung SDS ortaklığında geliştirilen blokzincir sistemi ile gemi varış/kalkış, konşimento ve kargo takibinde BC kullanılan deneme seferi düzenlemiştir. |
| 13 <b>Enerji Yönetimi</b>                         | Geleneksel uygulamalarda enerji kaynaklarının, üreticiden tüketiciye ulaşabilmesi için bir kamu kurumu aracılığına ihtiyaç duyulmaktadır. Blokzincir bu merkeziyet ihtiyacını ortadan kaldırarak üreticinin doğrudan tüketiciye, hatta kişiden kişiye (örneğin komşusuna), enerji satımını gerçekleştirebilmesini sağlar.                               | LO3 Energy'nin Energy Web Chain'i üzerinde çalışan Pando ürünü, Ethereum üzerinde çalışan TransactiveGrid ve yenilenebilir enerjiye erişime yönelik İspanyol Acciona Energy ile Iberdrola bu alana yönelik girişimlerdir.                                                                                                                                                          |
| 14 <b>Özel Taşımacılık Sektörü</b>                | Akıllı sözleşme ile araç kiralama ve araç çağırma işlemleri aracısız olarak hızlı ve güvenli gerçekleştirilebilir. Ayrıca ikinci el araba alımlarında, aracın geçmişine (kaza, bakım-onarım, km bilgisi, ipotek ve mülkiyet durumu vb. gibi) ilişkin veriler blokzinciri kayıtlarından ulaşılabilir ve değiştirilemez olduğundan güvenilir alım sağlar. | Visa'nın araç kiralamaya yönelik DocuSign girişimi; ikinci el araba alım-satımına yönelik Estonya girişimi carVertical; araç çağırma yönelik Arcade City girişimi bu alana örnektir.                                                                                                                                                                                               |
| 15 <b>Bulut Bilişim ve Veri Depolama</b>          | Merkezi bir sunucuya dayanan geleneksel veri depolama sistemi siber saldırılara, insan hatalarına ve veri kayıplarına karşı savunmasızdır. Blokzincir tabanlı bulut depolama sistemi, bu riskleri ortadan kaldırarak güvenli, dayanıklı ve düşük işlem maliyetli bir çözüm sağlamaktadır.                                                               | Dosya depolama için Airbnb olarak adlandırılan Filecoin; bulut depolamaya yönelik Storj ve Siacoin bu alana yönelik örneklerdir.                                                                                                                                                                                                                                                   |
| 16 <b>Müzik ve Telif Hakları</b>                  | Müzik sektöründe, blokzincir ve akıllı sözleşmelerin kullanılmasıyla müzisyenler dinleyicilerden direkt kazanç elde edebilirken; eserlerin telif hakkı ödemelerinin de otomatik ve adil yapılması sağlanır.                                                                                                                                             | Binance ile ortak olan müzik akış platformu Muzika; merkeziyetsiz medya kütüphanesi Mediachain; Mycelia ve ujo girişimleri bu alana örnektir.                                                                                                                                                                                                                                      |
| 17 <b>Kamu Yönetimi</b>                           | Kamu hizmetlerinin ağır ve yolsuzluğa açık yapısı, blokzincir kullanılarak bürokrasisi düşük, şeffaf ve verimli bir sürece dönüştürülebilir. Böylece işgücü ve para tasarrufu yapılarak vatandaşların hayat kalitesi ve mutluluk düzeyi artırılabilir.                                                                                                  | İsveç Tapu Dairesi'nin arazi kaydı ve mülk satışları için blokzincir ve akıllı sözleşme kullanımına yönelik girişimleri bulunmaktadır. Diğer yandan Birleşik Arap Emirlikleri de blokzincir firması Consensus'den bu alana yönelik danışmanlık almaktadır.                                                                                                                         |

**Tablo 2.11:** Blokzincir Teknolojisinin Uygulama Alanları (Devam).

| Uygulama Alanı                                 | Kullanım Amacı/Sağladığı Fayda                                                                                                                                                                                                                                                                                                                                                                        | Uygulama Örneği                                                                                                                                                                                                                                                                        |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 18<br><b>Oy Kullanma</b>                       | Seçim sürecinin gerektirdiği kimlik doğrulama, kullanılan oyun anonimliği, mükerrer oy kullanılmaması ve doğru oy sayımı nitelikleri blokzincir kullanımı ile sağlanabilir. Böylece hükümetler ve seçmenler doğrulanabilir olduğundan, oylar değiştirilemediğinden veya silinemediğinden güvenilir ve adil bir seçim süreci sağlanır. Ayrıca seçim çevrim içi yapıldığından sonuçlar hemen açıklanır. | Agora platformu, 2018 Sierra Leone seçiminde test edilerek resmi sayımlara yakın sonuçlar verdi. Ayrıca Follow My Vote ve Democracy.Earth bu alanda geliştirilen çözümlerdir.                                                                                                          |
| 19<br><b>Vergi Toplama</b>                     | Blokzincir ve akıllı sözleşmeler ile tüm işlemler dijital olarak yapıldığından vergi, doğru ve gerçek zamanlı olarak hesaplanıp tahsil edilebilir. Tüm sürecin dijital olarak yürütülmesi vergi kaçırılması riskini azaltarak kayıt dışı ekonomi önlenir ve vergi toplama süreci düşük maliyetle daha hızlı tamamlanır.                                                                               | Estonya, e-estonia platformu blokzincir teknolojisine dayanan ilk devlettir ve tüm vatandaşlık hizmetleri dolayısıyla vergi toplama işlemleri de blokzincir aracılığıyla gerçekleştirilir. Ayrıca Dubai'de 2020 yılı itibarıyla devlet işlerinde blokzincir kullanma hedefi koymuştur. |
| 20<br><b>Dijital Kimlik</b>                    | Geleneksel bir yapıda dijital kimlik bilgileri, merkezi otoritelerde saklanır ve dış servisler ile bu merkezlerin kontrolünde paylaşılır. Blokzincir ile merkezi yapı ortadan kaldırılarak kişisel kimlik paylaşımı ve kontrolü kimlik sahibine bırakılır. Böylece kişisel gizlilik sağlanır. Ayrıca blokzincirin değiştirilemezliği de sahte kimlik ve kimlik hırsızlığı riskini azaltır.            | IBM'in IBM Verify Credentials'ı, blokzincir tabanlı bir kimlik yönetim aracıdır. Ayrıca mobil dijital kimlik yönetimine yönelik Turkcell de bir çözüm geliştirmiştir.                                                                                                                  |
| 21<br><b>Bağış Toplama ve Sosyal Yardımlar</b> | Blokzincir kullanılarak yapılan bir bağış sürecinde; araçlar dolayısıyla yapılan kesinti, bağışın yerine ulaşmasında geçen uzun süre ve kaynak aktarımının gerçekleşip gerçekleşmediğine ilişkin güven sorunları bertaraf edilir. Böylece şeffaf, gerçek zamanlı, güvenilir, izlenebilir ve verimli bir bağış süreci gerçekleştirilir.                                                                | BitGive ve devlet sosyal yardımlarına yönelik İngiltere hükümeti ile Barclays bankası girişimi olan GovCoin bu alana yönelik örneklerdendir.                                                                                                                                           |
| 22<br><b>Bahis ve Şans Oyunları</b>            | Blokzincir teknolojisi merkeziyetsiz, adil, manipüle edilemeyen ve anonim bir oyun alanı sağlar. Ayrıca çok fazla belge ve doğrulama olmadığından evrensel olarak kumarın erişilebilirliğini artırır.                                                                                                                                                                                                 | Güvensiz bahis fikriyle oynatılan Wager sitesi blokzincir teknolojisi üzerine kurulu bir bahis platformudur.                                                                                                                                                                           |
| 23<br><b>Noter İşlemleri</b>                   | Noterlerin, işlemlerin ve belgelerin gerçekliğini doğrulama görevi blokzincir ağı aracılığıyla merkeziyetsiz, güvenilir, hızlı ve düşük maliyetli bir şekilde yerine getirilebilir.                                                                                                                                                                                                                   | Tüm blokzincir ağları farklı şekillerde doğrulama işlevini yerine getirdiğinden noter mesleği gelecekte yok olma riski altındadır.                                                                                                                                                     |

**Tablo 2.11:** Blokzincir Teknolojisinin Uygulama Alanları (Devam).

| Uygulama Alanı                         | Kullanım Amacı/Sağladığı Fayda                                                                                                                                                                                                                                                                                                                             | Uygulama Örneği                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 24<br><b>Tarım ve Doğal Kaynaklar</b>  | Tarımda ve doğal kaynak yönetiminde blokzincir kullanımı, ürünlerin ve kaynakların izlenebilirliğini artırır, böylece üretim süreçleri daha şeffaf ve verimli hale gelir. Ayrıca bu teknoloji, kaynakların sürdürülebilir kullanımını sağlamak ve tedarik zincirindeki her aşamayı gerçek zamanlı olarak takip etmek için kullanılır.                      | Tahıl alım-satımı ve depolamasının dijitalleştirilmesine yönelik AgriDigital; hayvan genomik profili, tıbbi geçmişi ve yediği yem bilgilerine yönelik Ripe Technology; World Wildlife Fund'un ConsenSys ve SeaQuest Fiji ortaklığında ton balığının nasıl, ne zaman ve nerede yakalandığının doğrulamasına ilişkin girişimleri bu alana yönelik örneklerdendir. |
| 25<br><b>Askeri Güvenli Haberleşme</b> | Askeri haberleşmenin şifreli yapıldığı dikkate alındığında, bilgi iletiminde bütünlük, gizlilik, doğruluk ve inkâr edilemezliğin kriptografi kullanılarak güvence altına alındığı blokzincir teknolojisinin kullanılması, askeri iletişim sistemlerinin güvenliğini artırarak veri manipülasyonu veya yetkisiz erişim gibi tehditlere karşı koruma sağlar. | U.S. Department of Defense (DoD), askeri haberleşme ve veri paylaşımında blokzincir kullanımına yönelik araştırmalar yapmaktadır.                                                                                                                                                                                                                               |

**Kaynak :** [Kılıç, 2020, s.16-20; CB Insights, 2022; Usta vd., 2019, s.55-65]\*dan yararlanılarak yazar tarafından düzenlenmiştir.

## 2.9 BLOKZİNCİR TEKNOLOJİSİNİN AVANTAJ VE DEZAVANTAJLARI

Blokzincir teknolojisinin, dijital verilerin güvenli ve şeffaf bir şekilde saklanması sağlayarak birçok sektörde devrim yaratacağından ve sağladığı faydaları dolayısıyla yaygın bir kullanım alanı bulacağından önceki bölümlerde detaylı bir şekilde bahsedilmiştir. Ancak bu teknoloji, sağladığı faydaların yanında bazı teknik olumsuzlukları da barındırmaktadır. Dolayısıyla blokzincir teknolojisinin potansiyeli ve sınırlamalarının daha net ortaya konulması amacıyla blokzincirin avantajları ve dezavantajları aşağıda maddeler halinde özetlenmiştir.

Avantajları :

- Dağıtık ağ yapısı sayesinde bir merkezi sunucunun manipülasyona uğraması ile karşılaşılan veri güvenliği ve bütünlüğü riski engellenir.

- b. Verilerin ağ katılımcılarının tümü tarafından erişilebilir olması sistemin şeffaf olmasını sağlar. Böylece veriler izlenebilir ve herkes tarafından veri denetimi yapılabilir.
- c. Dijital imzalar ile kimliklerin anonimliği sağlanarak kişisel mahremiyet korunur. Böylece verinin, kiminle ne kadar paylaşılacağı bir merkezin değil işlem sahibinin kontrolünde gerçekleşir.
- d. Kriptografi, mutabakat algoritmaları ve zincir yapısı ile veri güvenliği sağlanır. Bu nedenle ağ üzerindeki verilerin sahte veya hatalı olması, değiştirilmesi ya da silinmesi mümkün değildir.
- e. Güvenilir üçüncü taraflar olmadan işlem yapılabilirdiğinden aracılık maliyetleri yoktur.
- f. Bankacılık sisteminin aracılığı olmadan, bankalardan hizmet alamayanlar da dahil herkesin, finansal işlem yapabileceği bir ortam yaratılır.
- g. Blokzincir teknolojisi; mesai saati, hafta tatili veya resmî tatil gibi bekleme sürelerine bağlı kalmadan, işlemlerin her zaman anında gerçekleşmesini sağlar.
- h. İşlemler dijital ortamda ve dağıtık ağ aracılığıyla yapıldığından, fiziksel evrak ve bürokrasi sürecini azaltarak işlemleri daha hızlı ve verimli hale getirir.
- i. Akıllı sözleşmeler ve algoritmalar aracılığıyla işlemler otomatikleştirilerek insan hatası riski ortadan kaldırılır.

Dezavantajları (Shah vd., 2018, s.10) :

- a. Yüksek Enerji Tüketimi: Blokzincirde kullanılan PoW mutabakat protokolü yüksek enerji sarfiyatına sebep olmaktadır. Buna çözüm olarak farklı mutabakat yöntemleri<sup>45</sup> geliştirilmiş olsa da en yaygın kullanılan Bitcoin blokzinciri, PoW mekanizmasını kullanmaktadır. Diğer yandan her bir katılımcı sistem güvenliğini sağlamak için mutabakat sürecine katıldığından yüksek enerji maliyetlerinin yanı sıra kaynakların israf edilmesi de söz konusudur.

---

<sup>45</sup> “Mutabakat Yöntemleri” için bkznz. s.40.



- b. Yüksek Maliyet: Gelişen madencilik süreci özel ve yüksek performanslı donanımlara hatta madencilik merkezlerine ihtiyaç duymaktadır. Dolayısıyla bu durum madencilik faaliyetlerini pahalı hale getirmektedir<sup>46</sup>.
- c. Yavaş İşlem Süreci: Blokzincirde verilerin doğrulanması için işlemlerin ağ katılımcılarına dağıtılması gerekmektedir. Blokzincir ağına erişim herkese açık olduğundan katılımcı sayısı ve işlem miktarı arttıkça işlem süreci yavaşlamakta dolayısıyla daha yüksek kapasite bir ağ bağlantısı ve ayrıca depolama alanına ihtiyaç duyulmaktadır (Karahana vd., 2019, s.62).
- d. Ölçeklendirme Zorluğu: Ölçeklenebilirlik, bir sistemin hacmindeki veya boyutundaki değişikliklere rağmen işlevlerini aynı şekilde sürdürebilme yeteneğidir. Blokzincirin zincir yapısı dolayısıyla işlem miktarı ve kullanıcı sayısı arttıkça, defter boyutu büyümekte ve işlem hızı yavaşlamaktadır. Diğer yandan bitcoinin 10 dakikalık blok oluşturma süresi de saniyede 7 işlem yapabilmesine neden olmakta ve ölçeklenebilirlik sorununu daha da derinleştirmektedir. Özel blokzincirler ile saniyede binlerce işlem yapılabilmesine olanak sağlanarak eş zamanlı veri işleme yapılmasıyla bu sorun çözümlenmeye çalışılmaktadır.
- e. Veri Değiştirilemezliği Sorunu: Blokzincirin en önemli avantajı değiştirilemezlik, herhangi bir verinin yanlış kaydedilmesi halinde düzeltme yapılmasına imkân vermemesi sebebiyle pratik uygulamalarda kısıt olarak karşımıza çıkmaktadır. Diğer yandan bireylerin adli kayıtları, kimlik bilgileri vb. gibi kişisel bilgileri blokzincire bir kez kaydedildi mi unutulma hakkı uygulanarak kayıtların silinmesi de mümkün olmamaktadır. Ayrıca bu bilgilerin genel ağlarda herkesin erişimine açık olması da kullanıcıların mahremiyetini riske atabilmektedir (Karahana vd., 2019, s.61).
- f. Öz Takip Sorunu: Blokzincirde işlem yapmak için gerekli olan açık ve özel anahtarlardan özel anahtar sadece sahibinin bildiği bir anahtardır ve güvenli bir şekilde korunması sahibinin yükümlülüğündedir. Dolayısıyla özel anahtarın unutulması veya kaybolması halinde anahtar sahibinin doğrulanmasının ya da anahtarın koruduğu verilere ve fonlara

---

<sup>46</sup> “PoW Mutabakat Yönteminin Dezavantajları” için bkz. s.66.



erişimin imkânı kalmamaktadır. Böylece ilgili varlıklar kaybedilmektedir (Usta vd., 2019, s.98).

- g. Olgunlaşmamış Sektör: Blokzincir hali hazırda karmaşık ve çok yeni bir teknolojidir. Vadettiklerini sunabilmesi ve belirli bir standarda erişmesi için uzun bir süreç gerekmekte ve henüz çok erkendir. Diğer yandan bu teknoloji hakkında teknik bilgi ve deneyime sahip yazılım uzmanı yetersizdir. Bu nedenle blokzincir teknolojisine dayanan uygulamaların geliştirme maliyetleri yüksektir. Ayrıca blokzincir, karmaşık kavramlar ve süreçleri barındırması sebebiyle sıradan bir insan için anlaşılması zor bir teknolojidir. Bu nedenle de ana akım kullanım için henüz hazır değildir (Sarmah, 2018, s.27).
- h. Hukuki Sistemle Entegrasyon Sorunu: Blokzincir teknolojisi birçok hukuki alanı da etkilediğinden yasal düzenlemelere ve standartlara ihtiyaç duymaktadır. Ancak henüz küresel çapta genel kabul görmüş bir regülasyon getirilmemiştir. Bunun yanı sıra ülkeler, doğrudan teknolojiye yönelik değil ama blokzincir uygulama alanları (kripto para, akıllı sözleşmeler, dijital kimlik vb. gibi) üzerinden düzenlemeler getirerek olası risklere karşı piyasaları ve insanları korumaya çalışmış ve blokzincir pazarının büyümesine yönelik bir mevzuat çerçevesi oluşturmaya çalışmışlardır. Düzenlemeler çoğunlukla, kripto para birimleri, kara para aklama ile mücadele ve müşteri tanıma (KYC) alanları üzerinde yoğunlaşmıştır. Fakat teknolojinin hızla gelişmesi ve teknolojinin küresel düzeyde etki alanının olması, yapılan yerel düzenlemelerin ihtiyacı karşılamada yetersiz ve geç kalması riskini taşımaktadır (Blockchain Türkiye Platformu, 2019, s.11). Örneğin akıllı sözleşmeler ve dijital kimlik üzerine somut düzenleme çalışmaları henüz yeteri kadar gündem oluşturmamaktadır. Buna göre, akıllı sözleşmelerin mahkemede delil olarak kullanılıp kullanılamayacağı gibi hukuki bağlayıcılığına ilişkin belirsizlikler mevcuttur (Karahana vd., 2019, s.62).
- i. Sistemler Arası Çalışabilirlik Sorunu: Sistemler arası çalışabilirlik, veri senkronizasyonu ve tutarlılığı gerektirir. Bu nedenle blokzincir uygulamaları, eski sistemler ve zincir dışı veriler ile bütünleştirilememektedir (<https://kriptomat.io/tr/blockchain/blok-zinciri-teknolojisinin-artilari-ve-eksileri/>). Ayrıca blokzincirlerin farklı protokol ve standartları, veri yapıları, mutabakat mekanizmaları, kullandıkları akıllı sözleşme dilleri gibi özellikleri dolayısıyla diğer blokzincir platformları ile de entegre olmaları zordur. Diğer yandan blokzincirler arası etkileşimler için standartların ve düzenlemelerin eksikliği,

alışabilirlik sorunlarını artırmaktadır. Uluslararası ve sektörel standartların olmaması, farklı blokzincirlerin ve sistemlerin uyumlu alışmasını zorlaştırmaktadır.

- j. Yasadışı Faaliyet Riski: Blokzincir teknolojisi, ağı kullanıcılarının anonimliğini ve veri gizliliğini sağlarken ne yazık ki yasadışı faaliyetlerin ve ticaretin yapılmasına da zemin hazırlamaktadır. Yasal otoritelerin en büyük eleştirilerinden biri bu konudur. Blokzincirin merkeziyetsiz yapısı, finansal kurumların üstlendikleri, işlemi yapan tarafın şüpheli listesinde olup olmadığına ilişkin kimlik doğrulaması görevini yapamamalarına yol açmaktadır. Diğer yandan finansal sisteme erişemeyen bu şüpheli kişilerin nakit yerine dijital ortamda kolaylıkla faaliyette bulunmasına olanak sağlamaktadır. Blokzincirin yasadışı faaliyetlerde kullanımına yönelik en bilindik örneğı Şubat 2011’den kapatıldığı Ekim 2013’e kadar faaliyette bulunan darkweb pazarı Silk Road’tur (Hayes, 2024).

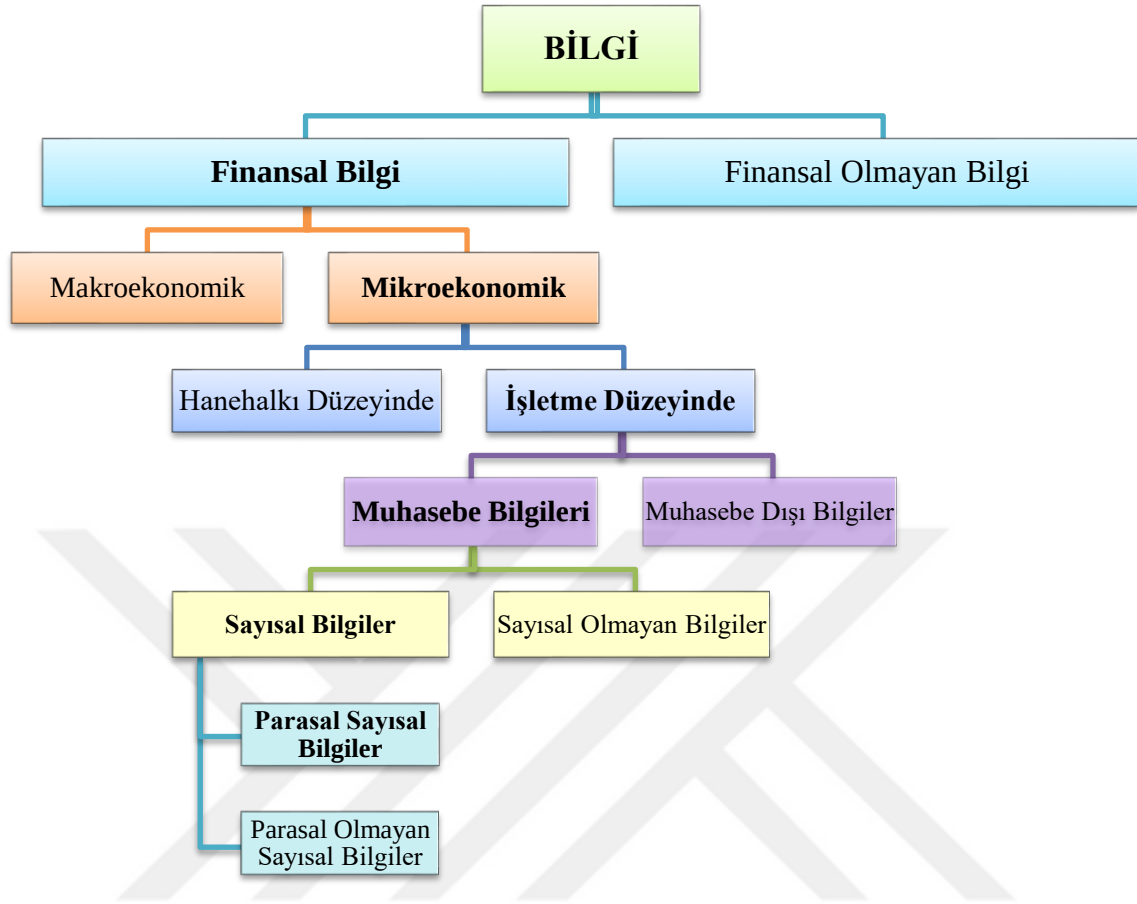
### **3. FİNANSAL BİLGİ MANİPÜLASYONU (MUHASEBE HİLELERİ)**

#### **3.1 FİNANSAL BİLGİ VE MANİPÜLASYONU**

Literatürde çok çeşitli bilgi sınıflandırmaları yapılmış olmasının yanı sıra çalışma konusu kapsamında bilgi, finansal bilgi ve finansal olmayan bilgi olarak yapılan ayırım üzerinden ele alınmaktadır. Bu ayrıma göre finansal bilgi; ekonomi, muhasebe ve finans bilim dalları kapsamında ilgililerin, karar almada başvurdukları bir kaynağı; finansal olmayan bilgi ise, bunun dışındaki her türlü bilgi kaynağını ifade etmektedir (Özdemir, 2013, s.160). Araştırma konusu özelinde sadece finansal bilgi kavramı üzerinde durularak, finansal bilgi manipülasyonun tanımı yapılacaktır.

##### **3.1.1 Finansal Bilgi**

Finansal bilgi, Şekil 3.1’de görüldüğü üzere; genel iktisat teorisi kapsamında ihtiyaç duyulan bilginin kullanım alanına göre “makroekonomik finansal bilgi” ve “mikroekonomik finansal bilgi” olarak iki boyutta değerlendirilmektedir. Makroekonomik finansal bilgi; ekonomik büyüme, cari işlemler dengesi, enflasyon, kamu bütçe dengesi, döviz kurları, faiz oranları gibi genel ülke ve dünya ekonomisine ilişkin finansal bilgileri içermektedir. Mikroekonomik finansal bilgi ise ekonomideki tüketici ve üretici birimlerin iktisadi ve mali durumunu etkileyen veya gelecekte etkileme ihtimali bulunan olayların araştırılarak veya gözlemlenerek tablo, grafik vb. gibi bilgi iletim araçlarının oluşturduğu bilgi kaynağını içermektedir. Ancak hanehalkının finansal bilgi üretme zorunluluğunun olmaması sebebiyle mikroekonomik finansal bilgi denildiğinde sadece işletme düzeyindeki bilgi kastedilmektedir. Diğer yandan işletme düzeyinde mikroekonomik finansal bilgi, geniş anlamı ile hem muhasebe hem de muhasebe dışı bilgileri kapsarken; dar anlamı ile sadece muhasebe bilgileri anlamında literatürde kullanılmaktadır (Özdemir, 2013, s.161). Muhasebe bilgileri, muhasebe bilgi sisteminin üretmiş olduğu kayıtlar ve finansal tabloları ifade ederken; muhasebe dışı bilgiler ise, müşteri memnuniyeti, ürün geliştirme süreçleri, yönetim tahminleri, iş gücü verimliliği, sosyal ve çevresel sorumluluklar gibi muhasebe bilgi sisteminin üretmediği finansal bilgileri ifade etmektedir.



**Şekil 3.1:** Finansal Bilginin Sınıflandırılması.

[Özdemir, 2013, s.163]

Dolayısıyla genel olarak finansal bilgi denildiğinde; işletmelerinin muhasebe bilgi sistemlerinin ürettiği bilgiler kastedilmekte ve bir firmanın belirli bir dönemdeki faaliyetlerine ilişkin finansal tabloları aracılığıyla açıklanan tüm nicel veya nitel verileri (Landu vd., 2024, s.2), finansal bilgi olarak tanımlanmaktadır.

Muhasebe bilgileri de “sayısal” ve “sayısal olmayan” muhasebe bilgileri olmak üzere iki kategoriye ayrılmaktadır. Finansal tablolarda yer alan bilgiler aktif/pasif büyüklüğü, birikmiş amortisman tutarı, net satış tutarı gibi değerler sayısal finansal bilgi iken; tabloların dipnotlarında yer alan amortisman yöntemi, stok değerlendirme yöntemi gibi muhasebe politikalarına ilişkin bazı bilgiler sayısal olmayan finansal bilgilerdir. Ayrıca sayısal finansal bilgiler, “parasal” ve “parasal olmayan” olarak da sınıflandırılmaktadır. Bu ayrıma göre mali tablolardaki tüm veriler parasal sayısal bilgiler iken; stok miktarı, senet miktarı, nakit miktarı, ortaklık payları veya personel sayısı gibi bilgiler parasal olmayan sayısal bilgilerdir.

Muhasebede bir mali işlemin dikkate alınabilmesi için mutlaka parasal bir değer ile ifade edilebilir olması gerekmektedir. Dolayısıyla muhasebe bilgileri içindeki hem sayısal olmayan hem de parasal olmayan bilgiler parasal bilgilerin hesaplanmasında yardımcı olan bilgilerdir. Bu nedenle finansal bilgi literatürde yaygın olarak; bir işletmenin muhasebe bilgi sistemi ve dış raporlama sistemi aracılığıyla üretilen, işletmenin finansal durumunun, faaliyetlerinin ve faaliyet sonuçlarının, parasal bir ölçü birimi ile mali tablolar ve raporlar üzerinden ilgililere sunulduğu (Küçüksözen, 2004, s.14) sayısal veriler olarak tanımlanmaktadır.

Sonuç olarak; finansal bilginin çok daha kapsamlı bir anlamı olmakla birlikte muhasebe bilgisi, finansal bilginin bir alt kümesi yani türüdür. Geniş kitlelere hitap eden bu kavramın tanımlanmasında genel eğilim muhasebe bilgisi anlamında kullanılmasına yöneliktir (Özdemir, 2013, s.173). Bu çalışmada da genel eğilim doğrultusunda muhasebe bilgisinin yerine kullanılacaktır.

Finansal muhasebe bilgileri, bir şirketin finansal durumunu, finansal durumundaki değişiklikleri, performansını ve risklerini belirlemek için kullanılmaktadır. Geçmiş ve mevcut durum hakkında bilgi sahibi olmak ve ekonomik herhangi bir karar için gerekli arka plan verilerini sağlamak finansal rakamların işlevidir (Socea, 2012, s.51). Dolayısıyla finansal bilgilerin, karar alıcılar tarafından hızla ve en verimli şekilde kullanılabilmesi için bazı özelliklere sahip olması gerekmektedir. Bu özellikler 1 No.lu Muhasebe Sistemi Uygulama Genel Tebliği (MSUGT), Türkiye Muhasebe Standartları (TMS) Kavramsal Çerçeve ve TMS 1 Finansal Tabloların Sunuluşu'nda sıralanmıştır. Buna göre finansal bilgi; (i) güvenilir, (ii) ihtiyaca uygun, (iii) anlaşılabilir, (iv) karşılaştırılabilir (v) doğrulanabilir, (vi) gerçeğe uygun olmalı ve (v) zamanında hazırlanarak sunulmalıdır. Ayrıca finansal bilgi, sadece geçmiş olaylar hakkında değil, aynı zamanda gelecekteki nakit yükümlülükleri ve sırasıyla ödenecek ve alınacak kaynakları da kapsamaktadır (Landu vd., 2024, s.2).

Son olarak, finansal bilgileri karar almada kullanacak taraflara değinecek olursak; muhasebe bilgi kullanıcıları temelde işletme içi ve işletme dışı kullanıcılar olmak üzere iki kategoride ele alınmaktadır. İşletme içi kullanıcılar; işletme sahibi ve ortakları, yöneticiler ve çalışanlardır. İşletme dışı kullanıcılar ise alıcı ve satıcılar, borç verenler, yatırımcılar, devlet, sendikalar, toplum ve diğer işletmelerdir. Anlaşıldığı üzere geniş bir kitleye finansal bilgi sağlanmaktadır. Her bir kullanıcı farklı motivasyonlarla finansal bilgiye ihtiyaç duymaktadır

ve sağlayabilecekleri bilgi düzeyi de değişkenlik göstermektedir. İşletme sahipleri, ortakları, yöneticileri ve devlet tam bilgiye, bunların dışında kalanlar ise sınırlı bilgiye erişebilmektedir.

### 3.1.2 Finansal Bilgi Manipülasyonunun Tanımı

Fransızca kökenli Manipülasyon (İngilizce Manipulation) kelime anlamı olarak; Cambridge Sözlükte “birini veya bir şeyi, genellikle haksız veya dürüst olmayan bir şekilde, kendi yararınıza kontrol etmek”, Türk Dil Kurumu’na göre ise “yönlendirme”, “seçme, ekleme ve çıkarma yoluyla bilgileri değiştirme” şeklinde tanımlanmaktadır.

Sermaye Piyasaları Kurulu (SPK)’na göre manipülasyon; “piyasa dolandırıcılığı” olarak tanımlanmakta ve Sermaye Piyasası Kanunu Md. 107’de, “sermaye piyasası araçlarının fiyatlarına, fiyat değişimlerine, arz ve taleplerine ilişkin olarak yanlış veya yanıltıcı izlenim uyandırmak amacıyla alım veya satım yapma, emir verme, emir iptal etme, emir değiştirme veya hesap hareketleri gerçekleştirme” şeklinde açıklanan dolandırıcılık eylemleri suç kapsamında dikkate alınmaktadır.

Association of Certified Fraud Examiners (ACFE)’a göre dolandırıcılık, İngilizce “Fraud” kelimesi ile karşılık bulmakta ve “başkalarını kandırmak için tasarlanmış, mağdurun bir kayba uğramasına ve/veya failin bir kazanç elde etmesine neden olan herhangi bir kasıtlı eylem veya ihmâl” olarak tanımlanmaktadır (COSO & ACFE, 2023, s.8).

Dolayısıyla dolandırıcılık kavramı; İngilizce karşılık olarak sermaye piyasalarında “manipulation”, muhasebe sisteminde ise “fraud” olarak kullanılmaktadır. Diğer yandan ACFE’nin Türkiye temsilcisi olan USİUD, “fraud” kelimesinin Türkçe’de “dolandırıcılık, yolsuzluk, rüşvet, irtikap, zimmet, usulsüzlük, hile” vb. gibi çok geniş anlamları ifade eden bir kavram olması dolayısıyla Türkçe karşılığının “suistimal” olarak kullanımını benimsemiştir (Yılmaz, 2014). Ayrıca muhasebenin ürettiği finansal bilgilerde ortaya çıkan yanlışlıkların “hata ve hile” olarak ikiye ayrılması sebebiyle, kasıt ve suç teşkil eden “hile” kelimesinin “fraud” kavramına karşılık kullanımı Türk yazınında daha yaygındır.

Özetle; ilgili yazında manipülasyon, hile ve suistimal kelimeleri çoğunlukla aynı anlamı taşımakta ve birbirleri yerine kullanılmaktadır. Finansal bilgi manipülasyonu ise literatürde; muhasebe hileleri, muhasebe suistimalleri, muhasebe manipülasyonu, finansal tablo hileleri,

finansal tablo manipölasyonu gibi ifadeler ile yazarlar tarafından ele alınmakta ve açıklanmaktadır.

Buna göre muhasebe hileleri; Kamu Gözetim Kurumu (KGK) – Bağımsız Denetim Standardı 240 (BDS 240)’ta, “yönetimden, üst yönetimden sorumlu olanlardan, çalışanlardan veya üçüncü taraflardan bir veya birden fazla kişinin, haksız veya yasalara aykırı bir menfaat elde etmek amacıyla yaptığı aldatma içeren kasıtlı eylemler” olarak tanımlanırken benzer bir şekilde SPK – Bağımsız Denetim Standardı Hakkında Seri X, 22 No.lu Tebliğ’de “işletme yönetimindekiler ile yönetimden sorumlu kişilerin, işletme çalışanlarının veya üçüncü şahısların kasıtlı olarak adil veya yasal olmayan bir menfaat sağlamak amacıyla aldatma içeren davranışlarda bulunmaları” ifadesi ile açıklanmaktadır.

American Institute of Certified Public Accountants (AICPA), Statements on Auditing Standards (SAS) No.99 md.6’ya göre finansal bilgi manipölasyonu;

- a. “Finansal tabloların hazırlanmasında kullanılan muhasebe kayıtlarının veya destekleyici belgelerin tahrif edilmesi veya değiştirilmesi,
- b. Olayların, işlemlerin veya diğer önemli bilgilerin finansal tablolarda yanlış beyan edilmesi veya kasıtlı olarak ihmal edilmesi,
- c. Tutarlar, sınıflandırma, sunum şekli veya açıklamalara ilişkin muhasebe ilkelerinin kasıtlı olarak yanlış uygulanması”

şeklindeki faaliyetleri kapsamaktadır.

### 3.2 FİNANSAL BİLGİ MANİPÜLASYONU YAPILMASININ NEDENLERİ

Hileli bir eylemin doğmasına sebep olan ve bireyleri hile yapmaya iten, Amerikalı sosyolog ve kriminolog Donald Ray Cressey’in 1953 yılında “Other People’s Money: A Study in the Social Psychology of Embezzlement (Başkalarının Parası: Zimmete Para Geçirmenin Sosyal Psikolojisi Üzerine Bir Çalışma)” isimli çalışması ile ortaya koyduğu ve daha sonra 2001 yılında ACFE’nin kurucularından Joseph T. Wells tarafından “Hile Üçgeni (Fraud Triangle)” olarak isimlendirilen teoriye göre; (i) teşvik veya baskı (incentive or pressure), (ii) fırsat (opportunity) ve (iii) haklı gösterme (rationalize) unsurlarının gerçekleşmesidir.

### 3.2.1 Teşvik veya Baskı

Çalışanlar, finansal veya finansal olmayan özellikli teşvik veya baskılar dolayısıyla hile eylemine yönelmektedirler. Baskı unsuru; (i) mali içerikli baskı, (ii) kötü alışkanlıklardan kaynaklanan baskı ve (iii) işle ilgili baskılar olmak üzere üç kategoriye ayrılmaktadır. Maddi güçlük yaşanması, yüksek kredi kartı veya kredi borcu altında olunması, plansız sağlık harcamalarının ortaya çıkması vb. gibi finansal özellikte olanlar mali içerikli baskılardır. Diğer yandan çalışanın alkol, kumar veya madde bağımlılığı gibi finansal olmayan nitelikte olan baskı türü, kötü alışkanlıklardan kaynaklanan baskıdır. Son olarak yine finansal olmayan nitelikli; yüksek performans beklentisi altında çalışılması, takdir edilmeme, terfi alamama ve düşük ücret düzeyi gibi nedenler de işle ilgili baskılardır (Kazan, 2021, s.249).

### 3.2.2 Fırsat

Çalışanı hileye teşvik eden bir unsurun ortaya çıkması, hile eyleminin gerçekleşmesi için yeterli değildir. Teşvik ile birlikte aynı zamanda bunu yapabilecek koşulların veya ortamın da oluştuğu bir fırsat yakalanmalıdır. Bu fırsat, kontrollerin olmadığı ya da etkin olmayan kontrollerin varlığı veya kontrollerin geçersiz kılınabilmesi gibi örgütsel koşullar sayesinde yaratılabilmektedir (AICPA SAS No:99). Bu ortam koşullarına; zayıf iç kontrol sisteminin olması, muhasebe standartlarının karmaşık olması, kurumsal yönetimin eksik olması, hilekarlara uygulanan disiplin cezalarının yetersiz olması, bağımsız denetim komitesinin olmaması veya etkin faaliyet göstermemesi örnek olarak gösterilebilir (Kaya vd., 2018, s.726).

Ayrıca hile fırsatını kullanabilmek için genel bilgi ve teknik beceri de gereklidir. Genel bilgi, çalışanın sahip olduğu güveni ihlal etmesi iken; teknik beceri, ihlali gerçekleştirebilme yeteneğidir. Esasen bu koşullar çalışanın en başta işletmedeki pozisyonuna ulaşması ve onu koruması için ihtiyaç duyduğu becerilerdir. Dolayısıyla işletmede hileleri tespit etmek ve önlemek için uygun kontrol mekanizmaları sağlanmadığı takdirde en çok güvenilen çalışanların dahi hile fırsatı yakalayarak bunu kullanmaları mümkündür (Kazan, 2021, s.249).



### 3.2.3 Haklı Gösterme (Rasyonelleştirme)

Rasyonelleştirme; bir çalışanın, şahsi dürüstlüğü veya ahlaki muhakemesi sebebiyle hileli tutumuna veya davranışına mazeret bulma ve onu meşrulaştırma çabasıdır. Cressey'e göre haklı gösterme, suç eyleme dönüşmeden önce ortaya çıkan bir bileşendir. Suç gerçekleştikten sonra ise haklı gösterme bahaneleri tekrar edilerek yapılan eylemin yanlışlığına ilişkin düşünce değiştirilmekte ve böylece davranış alışkanlığı dönüştürülmektedir (Ataman vd., 2017, s.7; Kazan, 2021, s.250).

Bazı bireyler sahip oldukları karakter veya etik değerler neticesinde bilerek ve isteyerek dürüst olmayan eylemlerde bulunmaktadır. Diğer yandan dürüst olan bireyler dahi, üzerlerinde yeterli baskı oluşturan bir ortamda sahtekarlık yapabilmektedirler. Teşvik veya baskı ne kadar fazla olursa, bireyin sahtekarlık yapmayı kabul edilebilmesini haklı gösterme olasılığı da o kadar fazla olmaktadır (AICPA SAS No:99). Dolayısıyla haklı gösterme; çalışanın üstündeki baskıyı azaltmak amacıyla yakaladığı fırsatı, hile yapmada kullanmak için kendisini ikna ettiği bir motivasyon kaynağıdır.

Ancak Cressey'nin hile üçgeni unsurlarının bir araya gelmesinin, çalışanların hile yapmaya yönelmesi için yeterli olmadığına ilişkin eleştirileri dolayısıyla David T. Wolfe ve Dana R. Hermanson, 2004 yılında "The Fraud Diamond: Considering the Four Elements of Fraud (Hile Elması: Suistimalin Dört Unsurlarını Dikkate Almak) isimli çalışmaları ile hile yapılabilmesi için "yetenek (*capability*)" unsurunun da dikkate alınması gerekliliğini ortaya koymuşlar ve bu dört unsurun bütününe "Hile Elması" adını vermişlerdir.

Hile elması teorisine göre (Wolfe vd., 2004, s.38); *"fırsat, dolandırıcılığa giden kapıyı aralamakta; teşvik ve haklı gösterme ise, kişiyi buna doğru çekmektedir. Ancak kişinin açık kapıyı bir fırsat olarak görmesi ve sadece bir kez değil, defalarca kez bu kapıdan geçerek bundan faydalanabilmesi için bunu yapabilme kabiliyetine sahip olması gerekmektedir."*

### 3.2.4 Yetenek

Çalışanların işletme içindeki görevlerini başarılı bir şekilde yerine getirmelerini sağlayan kişisel beceriler ve yetkinliklerdir. Wolfe ve Hermanson'a göre; baskı, fırsat ve haklı gösterme nedenleri olsa bile çalışan, yapabilme ve saklayabilme becerisinin olup olmadığını değerlendirerek hile eylemine geçmektedir (Kazan, 2021, s.251). Bu doğrultuda hilekarların

sahip olduđu kişisel özellikler ve yetenekler altı unsurda sınıflandırılmıştır (Wolfe vd., 2004, s.39-40):

- a. Pozisyon: Kurum içinde uygun pozisyonunda olmak ve işleve sahip olma,
- b. Zekâ, deneyim ve yaratıcılık: İşlem ve kontrol sürecine hâkim, iç kontrol sistemindeki zayıflıkları anlayan ve bunu menfaatine kullanma becerisine ve yetkisine sahip olma,
- c. Ego ve özgüven: Güçlü bir egoya ve hilenin tespit edilmeyeceğine dair büyük bir özgüvene veya yakalandığı takdirde kolayca kurtulabileceğine dair bir inanca sahip olma,
- d. İkna kabiliyeti ve zorbalık: Baskı ve korkutma ile başkalarını iş birliğine ikna edebilme,
- e. Tutarlı yalan söyleyebilme: Yalanı, inandırıcı söyleme ve takip etme becerisine sahip olma,
- f. Stresle başa çıkabilme: Tespit edilme riskine ve hileyi gizlemeye çalışma stresine dayanma.

Yapılan açıklamalar çerçevesinde; işletme yöneticilerini ve çalışanlarını, finansal bilgi manipölasyonu yapmaya iten nedenler aşağıda maddeler halinde açıklanmıştır (Küçüksözen, 2004, s.124; Dereköy, 2020, s.93; Ertikin, 2017, s.77):

- a. Şirketlerin zayıf yönetim yapılarının olması,
- b. Yöneticilerin, beklenen mali performans düzeyini sağlamak, kendi kişisel kazançlarını artırmak ve menfaatlerini korumak amacıyla işletmenin finansal durumunu olumlu gösterme eğiliminde olmaları,
- c. İşletmede, gelir artışı sağlanması, belirli bir büyüme oranının elde edilmesi veya bütçe hedeflerine ulaşılması gibi koşullara bağlı ödül, ikramiye ve promosyon kazanılması veya üst düzey yöneticilerden firma ile ilgili makul olmayan beklentilerde bulunulması,
- d. İşletmelerde zayıf iç denetim sistemi ve zayıf bağımsız denetim komitelerinin olması veya bağımsız denetim komitesinin hiç olmaması,

- e. Finansal bilginin, gerçek zaman yerine periyodik esas baz alınarak finansal tablolarda raporlanması,
- f. Periyodik finansal raporlama neticesinde doğan finansal analistlik mesleği ve bunların tahminlerinin işletme yönetimi üzerinde beklentileri karşılama baskısı yaratması,
- g. Muhasebe standartlarındaki; gerçekleşme, tahakkuk ve tahsis kavramları dolayısıyla işletmeye iktisadi sonuç yaratan işlem ve olayların kayıt tarihi (gerçekleşme), tutarı (tahminleri de içeren değerlendirme) ve raporlanmasına yönelik muhasebe sisteminin esneklik sağlaması,
- h. İşletme ile bağımsız denetçiler arasındaki menfaat ilişkisi dolayısıyla bağımsız denetçilerin, müşterisi olan işletmeyi tatmin edecek bir finansal görünüm sunmak amacıyla muhasebe kurallarını kendi lehlerine olacak şekilde yorumlaması.

KPMG (2020, s.15)'nin “Bir Suistimalcinin Profili” adlı araştırmasında suistimallerin ortaya çıkma nedenleri Tablo 3.1’de verilmiştir.

**Tablo 3.1: KPMG Raporuna Göre Hile Nedenleri.**

|   | <b>HİLE NEDENLERİ</b>                      | <b>2020 YILI</b> |
|---|--------------------------------------------|------------------|
| 1 | Zayıf iç kontroller                        | 69%              |
| 2 | Etkin olmayan gözetimler                   | 53%              |
| 3 | Sınırsız yetkiler                          | 43%              |
| 4 | Yetkilerin ayrılığı ilkesine uyulmaması    | 41%              |
| 5 | Teknoloji kullanımında görülen yetersizlik | 20%              |
| 6 | İç kontrolleri atlatan iş birlikleri       | 20%              |

Diğer yandan KPMG (2020, s.24)'nin aynı çalışmasında, dünya geneliyle benzer düzeyde Türkiye’deki suistimalcilerin hile motivasyonları Tablo 3.2’de sıralanmıştır.

**Tablo 3.2:** KPMG Raporuna Göre Hile Motivasyonları.

|   | HİLE MOTİVASYONU                        | 2020 YILI |
|---|-----------------------------------------|-----------|
| 1 | Maddi gelir/Kişisel fayda sağlama       | 83%       |
| 2 | Yapabilirim güdüsü                      | 29%       |
| 3 | İşini kaybetmemek için bütçeyi tutturma | 14%       |
| 4 | Ek kazanç için hedef tutturma           | 12%       |
| 5 | Yüksek borç yükü                        | 12%       |
| 6 | Kötü alışkanlıklar                      | 10%       |
| 7 | Şirketi korumak için hedef tutturma     | 10%       |
| 8 | Organizasyon yapısı ve kültürü          | 7%        |

Dolayısıyla hilekârlar çoğunlukla, “kişisel fayda sağlama” güdüsü ile hareket ederek, iç kontrol sistemi zayıf olan işletmelerde finansal bilgi manipülasyonu eyleminde bulunmaktadır.

### 3.3 FİNANSAL BİLGİ MANİPÜLASYONU TÜRLERİ

Literatürde farklı kategorilere ayrılmış manipülasyon sınıflandırmaları mevcuttur. Bunlardan bazıları bu bölüm başlığı altında maddeler halinde verilecek ve ardından da alan yazında genel kabul görmüş sınıflandırmaya ilişkin tanımlamalar yapılacaktır.

KPMG (2020, s.13)’nin “Bir Suistimalcinin Profili Araştırması”na göre suistimal ile karşılaşılacak alanlar ve karşılaşma oranları Tablo 3.3’te verilmiştir.

**Tablo 3.3:** KPMG Raporuna Göre Suistimal Türleri.

|   | SUİSTİMAL TÜRÜ               | 2020 YILI |
|---|------------------------------|-----------|
| 1 | Varlıkların kötüye kullanımı | 49.02%    |
| 2 | Zimmet / Şahsi menfaat       | 49.02%    |
| 3 | Satın alma suistimalleri     | 43.14%    |
| 4 | Çıkar çatışması              | 31.37%    |
| 5 | Yolsuzluk                    | 29.41%    |
| 6 | Siber suistimal              | 9.80%     |
| 7 | Finansal tablo suistimali    | 7.84%     |

Diğer yandan PwC (2022, s.13)’nin “Küresel Ekonomik Suç ve Hile Araştırması”na göre; işletmelerin finansal ve ekonomik suç ve hile davranışı gösterdiği alanlar daha geniş kapsamlı olarak Tablo 3.4’te sınıflandırılmıştır.

**Tablo 3.4:** PwC Raporuna Göre Finansal ve Ekonomik Suçlar ve Hileler.

|    | SUÇ VE HİLE TÜRÜ                       |
|----|----------------------------------------|
| 1  | Muhasebe/ Finansal tablo hileleri      |
| 2  | Varlıkların kötüye kullanımı           |
| 3  | Rüşvet ve yolsuzluk                    |
| 4  | Müşteri hileleri                       |
| 5  | İnsan kaynakları hileleri              |
| 6  | Kara para aklama                       |
| 7  | İhale yolsuzluğu                       |
| 8  | Vergi kaçakçılığı                      |
| 9  | İçerden öğrenenlerin yetkisiz ticareti |
| 10 | Siber Suçlar                           |
| 11 | Aldatıcı iş uygulamaları               |
| 12 | Fikri mülkiyet hırsızlığı              |
| 13 | Rekabete aykırı davranış               |

SPKn (Md.107)’na göre piyasa dolandırıcılığı; (i) İşlem Bazlı Piyasa Dolandırıcılığı ve (ii) Bilgi Bazlı Piyasa Dolandırıcılığı olmak üzere ikiye ayrılmaktadır. İşlem bazlı piyasa dolandırıcılığı, sermaye piyasası araçlarının fiyatlarının güvenilir bir şekilde oluşmasını engelleyen manipülatif alım-satım işlemleridir. Bilgi bazlı piyasa dolandırıcılığı ise sermaye piyasası araçlarının fiyatlarını ve yatırımcıların kararlarını yönlendirmek amacıyla yanlış veya yanıltıcı haber, bilgi, söylenti yaymak veya rapor düzenlemektir.

KGK Bağımsız Denetim Standardı 240’a göre; denetçiler, kasıtlı yanlışlık bulunan (i) hileli finansal raporlamadan ve (ii) varlıkların kötüye kullanılmasından kaynaklanan hile türleri ile ilgilenmektedir.

Bir başka muhasebe hileleri gruplandırması ise; (i) çalışan hileleri, (ii) yönetim hileleri, (iii) yatırımcı hileleri, (iv) satıcı hileleri ve (v) müşteri hileleri olmak üzere yapılan sınıflandırmadır (Kılıç vd., 2018, s.60).

Görüldüğü üzere çok çeşitli hile kategorileri olmakla birlikte, hile eyleminde bulunan insan yaratıcılığının bir sınırının olmaması sebebiyle her geçen gün yeni kategorilerin ortaya çıkma riski bulunmaktadır. Buna rağmen tüm sınıflandırmalar incelendiğinde hem alan

yazını doğrudan ilgilendirmesi hem de en genel kapsamı yansıtmaması dolayısıyla ACFE'nin hile suistimal kategorileri, literatürde yaygın kabul edilen hile sınıflandırması olarak kullanılmaktadır.

ACFE, dünya genelinde suistimal vakalarına ilişkin, maliyet, hile kategorisi ve hilekâr profili bazında analizlerini, ilk kez 1996 yılında yayınladığı ve iki yılda bir aynı içerikle birlikte incelemeye tabi tuttuğu ülke sayısını artırarak güncellediği “Occupational Fraud: A Report to Nations (Uluslar için Mesleki Suistimaller Raporu) araştırması ile yapmaktadır. Bu çalışmada (ACFE, 2024, s.11), hileler kategorilere ayrılarak “*Hile Ağacı (Fraud Tree)*” adı verilen bir şemada gösterilmektedir. Buna göre muhasebe hileleri, (i) *Yolsuzluk*, (ii) *Varlıkların Kötüye Kullanılması* ve (iii) *Finansal Tablo Hileleri* olmak üzere üç ana kategoriye ayrılmaktadır.

### **3.3.1 Varlıkların Kötüye Kullanılması (Çalışan Hileleri)**

Varlıkların kötüye kullanılması vakaları; bir çalışanın, işveren kuruluşun kaynaklarını çalmasını veya kötüye kullanmasını içermektedir. Bu tür, en yaygın karşılaşılan ancak maliyet açısından en düşük kayba yol açan mesleki suistimal kategorisidir (ACFE, 2024, s.10).

Varlıkların kötüye kullanımı, (i) nakit hileleri ve (ii) nakit dışı hileler olmak üzere iki şekilde yapılmaktadır. Nakit hileleri; doğrudan nakit hırsızlığı, nakdin bir kısmını çalma (satışlar, alacaklar ve iadeler üzerinden kayıt dışı veya fazla/eksik nakit alma) ve hileli harcama (hayalet çalışan, sahte maaş, olmayan/fazla gider, çoklu ödemeler, sahte çek cirosu, alacaklı değiştirme, yanlış iade vb. gibi) yollarıyla uygulanmaktadır. Nakit dışı hileler ise nakit olmayan stok ve diğer tüm varlıkların şahsi kullanımı ve hırsızlığı şeklinde uygulanmaktadır (ACFE, 2024, s.11).

Bu tür hileye başvuran çalışanlar, genellikle işletmede uzun çalışma kıdemine sahip olup işletme yönetiminin ve ortaklarının güvenini kazanmış kişiler olmaktadır. Bu kişiler, kendilerini daha önce kanıtladıklarından sahip oldukları güveni kullanarak üzerlerindeki şüphe ve denetim riskinden sıyrılmakta ve fark edilmeden manipülasyonda bulunabilmektedirler (Ataman vd., 2017, s.5). Ayrıca diğer çalışanlara yakalanma riski

düşük olduğundan mesaiye erken gelip geç çıkma ve vekaleten yerine kimse bakmasın diye zorunlu olmadıkça izne çıkmama eğilimine sahiptirler (Ertikin, 2017, s.77).

### 3.3.2 Yolsuzluk

Avrupa Konseyi Yolsuzluğa Karşı Özel Hukuk Sözleşmesi (Md.2)'nde yolsuzluk; *"...doğrudan veya dolaylı yollardan yasadışı bir çıkar sağlayan kişinin sahip olduğu görevlerin yasalara uygun olarak yerine getirilmemesine yol açan rüşvet veya her türlü yasadışı menfaatin talep edilmesi, teklif edilmesi, sunulması ve alınıp verilmesi"* ifadesi ile tanımlanmaktadır (Ataman vd., 2017, s.5). Bu tür, %48 gibi bir oran ile en yaygın karşılaşılan ikinci suistimal kategorisidir (ACFE, 2024, s.10)

Yolsuzluk vakaları; (i) çıkar çatışmaları, (ii) rüşvet, (iii) yasadışı hediyeler ve (iv) haraç olmak üzere dört şekilde yapılmaktadır. Çıkar çatışmaları, satın alma ve satış işlemleri ile; rüşvet ise ihaleye fesat karıştırma gibi yollarla gerçekleştirilmektedir (ACFE, 2024, s.11).

### 3.3.3 Finansal Tablo Hileleri (Yönetim Hileleri)

Finansal tablo hileleri; işletmelerin, Genel Kabul Görmüş Muhasebe İlkeleri (GKGMI<sup>47</sup>)'ndeki standart raporlamaya ilişkin esnekliklerden faydalanmaları veya bu esneklik limitlerini aşarak, mali durum ve faaliyet sonuçlarını gerçekte olduğundan farklı göstermek amacıyla finansal tablolarda sunulan bilgiler üzerinde değişiklik yapmaları şeklinde gerçekleştirilmektedir (Küçüksözen, 2004, s.49). Bu hileler; finansal bilgi kullanıcılarını aldatmaya yönelik olarak GKGMI'ye aykırı kasıtlı yanlış beyanlar, tutar veya açıklama eksiklikleridir (AICPA SAS No.99 md.6). Bu tür, en az karşılaşılan ancak maliyet açısından en büyük kayba yol açan mesleki suistimal kategorisidir (ACFE, 2024, s.10).

Hileli finansal raporlamaya, literatürde ağırlıklı olarak standartların yorumlanması (tahakkuk düzeyine ilişkin kararların farklı yorumu vb. gibi) üzerinden karşılaşılmaktadır. Diğer yandan manipülasyon önceden planlanmış da olabilir, yani işlemler istenen bir muhasebe uygulamasına izin verecek şekilde tasarlanabilmektedir. Örneğin; bir finansal kiralama sözleşmesi, kiralanan ekipmanın aktifleştirilmeyeceği şekilde yazılabilmektedir (Stolowy vd., 2000, s.3). Ancak her zaman büyük bir planın sonucu olması gerekmekte

---

<sup>47</sup> Genel Kabul Görmüş Muhasebe İlkeleri'nin İngilizce karşılığı, Generally Accepted Accounting Principles (GAAP)'tir.

ve daha sonra düzeltilmek üzere geçici süreyle finansal tabloların yanlış beyan edilmesi şeklinde makul gösterilmeye de çalışılabilmektedir (AICPA SAS No.99 md.6).

Finansal tablo hileleri; zamanlama farklılıkları, gelirler, yükümlülükler ve giderler, yanlış varlık değerlemeleri, yanlış açıklamalar yollarıyla net değer (net gelirin) fazla veya eksik beyan edilmesi şeklinde yapılmaktadır (ACFE, 2024, s.11).

### **3.4 FİNANSAL BİLGİ MANİPÜLASYONUNUN AMAÇLARI**

İşletmeler, faaliyet gösterdikleri sektör veya büyüklükleri ne olursa olsun finansal bilgi paylaşımı konusunda tedirginlik hissetmektedirler. Bu durum paylaşılan sayısal bilgilerin işletme üzerinde yaratacağı olası etkilerden kaynaklanmaktadır. Öyle ki, işletmenin imajı ve buna bağlı olarak da sermaye maliyeti üzerindeki etki çok büyük olabilmektedir. Piyasa fiyatları yükselirken borç sahiplerinin güveni artmakta ve tersi durumda piyasa fiyatları düşerken borç sahiplerinin güveni azalmaktadır. Diğer yandan muhasebe bilgileri; çalışanların, işletmenin kar elde etmesine bağlı gelecek planlarını veya genel müdürün, tazminat seviyesini de etkilemektedir (Stolowy vd., 2000, s.2).

Bu nedenle yöneticiler kendi çıkarları doğrultusunda işletmenin görünümünü daha iyi veya daha kötü göstermek üzere finansal tabloları manipüle etmektedirler. Karını yüksek göstererek borçlanma maliyetlerini düşürmeyi hedefleyen dolayısıyla işletmenin durumunu olduğundan iyi göstermek üzere manipülasyon yapan işletmeler büyük ölçekli ve halka açık işletmeler olurken; daha az vergi ödeme odaklı işletmeyi olduğundan kötü göstermek amacıyla manipülasyon yapan işletmeler orta ve küçük ölçekli işletmeler olmaktadır (Bozkurt, 2000, 15-22).

İşletmelerin projeleri için gereken finansmanı düşük maliyetle elde edebilmesi, yatırımcıların işletmeye ilişkin algıladıkları risk düzeyine bağlıdır. Yatırımcıların risk algılarını yönlendiren ise işletmenin beyan ettiği finansal tablo bilgileri olmaktadır. Buna göre bir yatırımcının kararını etkileyen temelde iki risk unsuru bulunmaktadır. Bunlar; (i) beta katsayısı ile ölçülen, işletmenin hisse senedi getirisinin, piyasa getirisine göre değişimi olan sistematik risk ve (ii) finansal kaldıraç oranı ile ölçülen, işletmenin borç ödeme yeterliliğini gösteren borç-öz kaynak dengesi olan sistematik olmayan risktir. Dolayısıyla finansal bilgi manipülasyonu ile amaçlanan; bu iki risk unsurunu yani hisse başına kazanç ve borç-öz kaynak dengesini çıkarlar doğrultusunda değiştirmektir (Stolowy vd., 2000, s.3).



Hisse başına kazanç üzerinde manipölasyon; (i) net gelirin (gelir veya giderlerin eklenmesi veya çıkarılması şeklinde) ve (ii) hesap sınıflandırmasının (kardan önce veya sonra bir kalem sunulması şeklinde) deęiştirilmesi şeklinde iki yolla yapılmaktadır. Borç-öz kaynak üzerinde manipölasyon ise; yine (i) hesap sınıflandırmasının deęiştirilmesi ve farklı olarak (ii) bilanço dışı finansman sağlanması yollarıyla yapılmaktadır (Stolowy vd., 2000, s.62).

Muhasebe bilgi kullanıcılarının algılarını ve kararlarını yönlendirmek üzere yapılan finansal tablo manipölasyonları ile hedeflenen başlıca amaçlar aşağıda maddeler halinde özetlenmiştir (Küçüksözen, 2004, 172-203; Küçükkocaoğlu vd., 2005, s.163; Yaman, 2008, s.168):

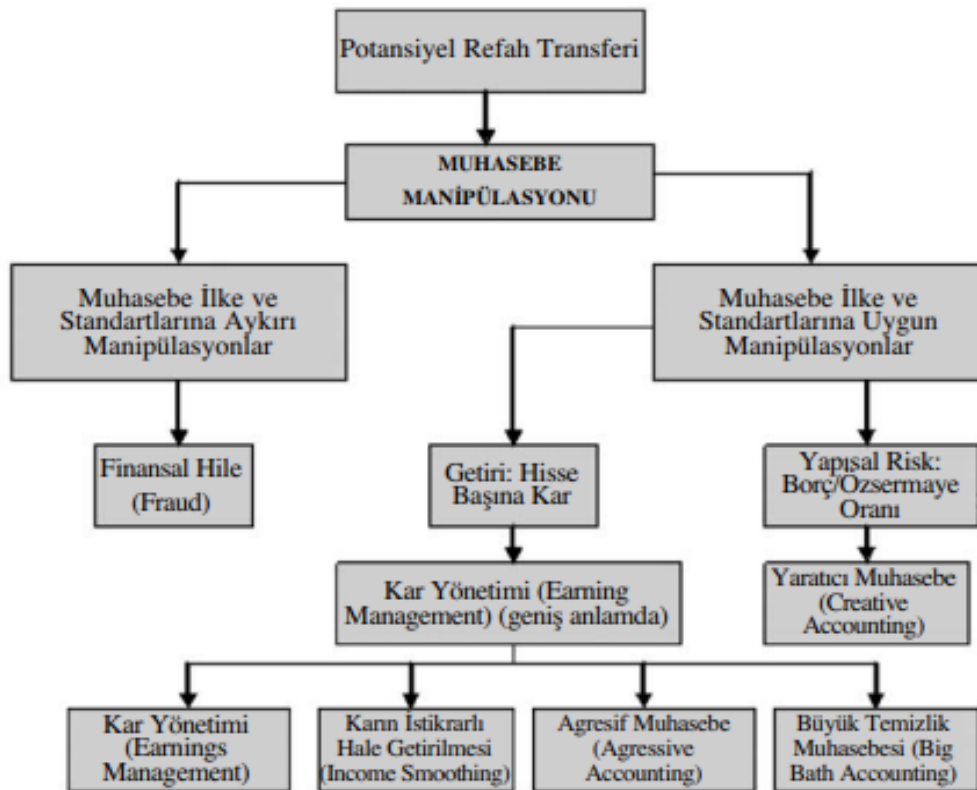
- a. İşletmenin hisse senedi fiyatını ve riskini etkilemek,
- b. Yatırımcıların işletme ile ilgili algıladıkları riski azaltmak,
- c. Borç sözleşmelerindeki finansal koşulları sağlamak,
- d. Ödenecek vergiyi azaltmak veya vergi kaçırmak,
- e. Yöneticilerin ücret ve primlerini artırmak,
- f. Siyasal veya yasal düzenlemelerden doğabilecek risklerden kaçınmak,
- g. Sermaye arttırımı veya halka açılma ile elde edilebilecek fon tutarını artırmak,
- h. İşletmenin performansının gelecekte daha iyi olacağına ilişkin piyasaya olumlu mesaj göndermek,
- i. Çalışanlar, yatırımcılar ve borç verenlerle ilişkileri iyi tutmak,
- j. Karı uzun vadede istikrarlı hale getirmek,
- k. İçerden öğrenenlerin ticareti,
- l. Yöneticilerin şirketi ele geçirmesinde (management buy-out), ele geçirme maliyetini düşürmek,
- m. Zimmete geçirilen varlıkları gizlemek,
- n. Hissedarların birbirlerini yanlış yönlendirme istekleri,

- o. Dağıtılacak karı azaltmak,
- p. Yolsuzlukları saklamak,
- q. Haksız teşviklerden yararlanmak.

### 3.5 FİNANSAL BİLGİ MANİPÜLASYONU YÖNTEMLERİ

Finansal bilgi manipülasyonu yöntemleri üzerine literatürde ortak bir görüşe varılamamış olmasına rağmen; (i) kar yönetimi, (ii) karın istikrarlı hale gelmesi, (iii) agresif muhasebe, (iii) büyük temizlik muhasebesi, (iv) yaratıcı muhasebe ve (v) hileli finansal raporlama olmak üzere beş kategori tanımlanmıştır (Stolowy vd., 2000, s.63; Mulford vd., 2002, s.3).

Demir (2007) ise bu tanımlamaları ve Stolowy ve Breton (2004)'nın sınıflandırmasını genişleterek Şekil 3.2'de gösterilen sınıflandırmayı ilgili yazına kazandırmıştır. Geniş kapsamlı ve anlaşılır olması dolayısıyla Türk alan yazınında çokça bu sınıflandırma şeması kullanılmaktadır. Dolayısıyla bu çalışmada da ilgili şemaya yer verilmiştir.



Şekil 3.2: Finansal Bilgi Manipülasyonu Yöntemleri.

[Stolowy vd., 2020, s.63; Demir vd., 2007, s.110]

Buna göre; finansal tablo manipölasyonları, muhasebe ilke ve standartlarına uygun ve aykırı olmak üzere iki ana kategoriye ayrılmaktadır. Muhasebe ilke ve standartlarına aykırı gerçekleştirilen manipölasyonlar, “Finansal Hile (Hileli Finansal Raporlama)” olarak adlandırılmaktadır. Muhasebe ilke ve standartlarına uygun gerçekleştirilen manipölasyonlar ise hisse başına kar elde etmek ve borç-özsermaye oranını düzenlemek amaçlarına göre ikiye ayrılmaktadır. Borç-özsermaye oranını etkilemek için uygulanan manipölasyon yöntemi, “yaratıcı muhasebe” olarak adlandırılırken; hisse başına kar elde etmek için uygulanan manipölasyon yöntemleri, genel adıyla “kazanç (kar) yönetimi” olarak adlandırılmakta olup dört farklı hedefe yönelik gerçekleştirilebilmektedir. Bu kazanç yönetimi yöntemleri de “dar anlamıyla kazanç yönetimi”, “karın istikrarlı hale getirilmesi”, “agresif muhasebe” ve “büyük temizlik muhasebesi” olmak üzere dört gruba ayrılmaktadır.

### **3.5.1 Kazanç Yönetimi (Earnings Management)**

Kazanç yönetimi; karın, önceden belirlenmiş bir hedefe yönelik aktif olarak manipüle edilmesidir. Bu hedef; yönetim tarafından belirlenmiş, analistler tarafından tahmin edilmiş veya istikrarlı bir kar akışı düzeyini sağlayan bir miktarı ifade etmektedir (Mulford vd., 2002, s.25).

Literatürde kar yönetimi kavramı; muhasebe ilkelerine, standartlarına ve yasal düzenlemelere uygun şekilde bunlardaki esnekliklerden faydalanarak, işletme yöneticilerinin amaçlarına yönelik, karın değiştirilmesi olarak tanımlanmaktadır. Ancak bu esnekliğin, finansal bilgi kullanıcılarını yanıltmak amacı ile kötüye kullanılıp kullanılmadığı hususunu belirlemek oldukça zordur. Örneğin; amortisman/itfa yöntemi veya stok-değerleme yönteminin değiştirilerek ya da satış taleplerine özellikle cevap verilmeyerek karın etkilenmesi şeklinde yapılan kazanç yönetimi, GKGMİ çerçevesinde uygun ve yasaldir. Bunun yanı sıra gider kayıtları sonraki döneme ertelenerek veya gelecek dönemin hasılatı erken kaydedilerek ya da stoktaki malların başka yere taşınması ile satıldı görünümü vererek karın etkilenmesi şeklinde yapılan kazanç yönetimi ise GKGMİ’ye aykırı ve yasal değildir. Bu durumda kazanç yönetimi, hileli finansal raporlamaya dönüşmektedir. Kazanç yönetimi; her ne kadar GKGMİ, muhasebe standartları ve yasal düzenleme sınırları içinde gerçekleştiriliyor olsa da finansal tabloların makul ve doğru sunumundan uzaklaşarak bilgi kullanıcılarının yanlış kararlar almasına sebep olmakta ve onlara zarar vermektedir (Ocak vd., 2014, s.131-132).

### 3.5.2 Karın İstikrarlı Hale Getirilmesi (Income Smoothing)

Döviz kurları, faiz oranları, vergi oranları, mal ve hizmet talebindeki değişimler, enflasyon, ekonomik kriz vb. gibi hem yerel hem de küresel ekonomi politikaları ve makroekonomik koşullarda ortaya çıkan değişimler sebebiyle işletmelerin yıllık performans sonuçları olumlu veya olumsuz olarak etkilenecek yıllar itibarıyla karlarında dalgalanmalar gerçekleşmektedir. Bu dalgalanmalar da işletmede kontrolsüz bir yönetim (iyi yönetilemeyen) imajı yaratmakta ve işletmenin, yatırımcılar açısından yüksek riskli olarak görülmesine neden olmaktadır (Toplu vd., 2021, s.18). Risk düzeyinin yüksekliği de işletme değerinin düşmesine ve sermaye maliyetinin artmasına yol açmaktadır.

Dolayısıyla işletmeler bu olumsuz imajın oluşmaması için belirli bir hedef düzeyinde karı dengelemek üzere manipülasyon yapmaktadırlar. Karın istikrarlı hale getirilmesi veya kar düzleştirme olarak adlandırılan bu manipülasyon yöntemi; normal bir kazanç serisindeki iniş ve çıkışları ortadan kaldırmak üzere iyi yıllarda elde edilen kârları, az kar edilen yıllarda kullanmak üzere “azaltma” ve “depolama” adımlarını içeren bir kazanç yönetimi türüdür (Mulford vd., 2002, s.3) ve sürekli büyüyen bir kar akışı üretmeyi ifade etmektedir. Bu tür bir manipülasyonun var olabilmesi için, firmanın gerektiğinde akışı düzenlemek amacıyla karşılık yaratacak kadar büyük karlar elde etmesi gerekmektedir (Stolowy vd., 2020, s11). Böylece yüksek kar elde edildiği dönemlerde düşük, düşük kar elde edildiği dönemlerde ise yüksek gösterilerek kar dalgalanmaları önlenmektedir.

Karın etkin bir şekilde istikrarlı hale getirilmesi üç şekilde gerçekleştirilebilmektedir (Ronen vd., 1975, s.133-134 Akt: Demir vd., 2007, s.113) :

- a. Tahakkuk: Yönetici kararları doğrultusunda gelir tahakkuklarının zamanını ayarlayarak,
- b. Zamana dağıtım: Gelir ve/veya giderleri ait oldukları dönem dışında farklı dönemlerde kaydederek ya da kur farklarını kar/zarar olarak kaydetmeyip aktifleştirme veya pasifleştirme suretiyle zaman içinde kar/zarara aktararak,
- c. Sınıflandırma: Yönetici kararları doğrultusunda gelir tablosu hesaplarını farklı sınıflandırarak (örneğin; olağan geliri, olağan dışı gelire kaydetmek).

### 3.5.3 Büyük Temizlik Muhasebesi (Big Bath Accounting)

Her maliye bakanı veya hükümet değişiminde olduğu gibi; işletme yönetiminin değişiminde de yeni yönetim, kendisine devredilen finansal performansın çok daha kötü olduğu imajı ve kendi yönetimine güven sağlamak üzere sürekli bir gelir akışı yaratmak için hesapları temizlemektedir. Göreve geldiği dönemin gelirlerini ertelemek veya gelecek dönemlerde yazılabilecek zararları hızlandırmak gibi ihtiyari muhasebe politikaları uygulamak yoluyla cari kazançların azaltılması şeklinde uygulanan bu manipülasyon “büyük temizlik” olarak adlandırılmaktadır (Stolowy vd., 2000, s.22).

Diğer yandan; yönetimin değişmediği ancak işletmelerin hali hazırda zarar ettiği ve daha fazla zarar açıklamanın ek maliyet oluşturmadığı dönemlerde de gelecek dönemlerde daha fazla kar elde ediliyormuş izlenimi yaratmak için bir fırsat olarak değerlendirilerek, bu strateji kullanılmaktadır (Küçüksözen vd., 2005, s.91).

Büyük temizlik muhasebesi; GKGMİ, muhasebe standartları ve yasal düzenleme sınırları içerisinde gerçekleştirilen bir kazanç yönetimi uygulamasıdır. Bu kazanç yönetiminde işletmeler, aşağıdaki uygulama teknikleri ile büyük temizlik yaparak rahat bir nefes almaktadırlar (Küçüksözen vd., 2005, s.92) :

- a. Verimsiz veya zarar eden bölümlerin ve kısımların kapatılmasıyla,
- b. Bilanço aktifinde yer alan henüz ömrünü tamamlamamış maddi veya maddi olmayan duran varlıkların topluca giderleştirilmesiyle,
- c. Yeniden yapılanma uygulamaları ile proje maliyetlerinin dönem gideri olarak kaydedilmesiyle.

### 3.5.4 Agresif Muhasebe (Aggressive Accounting)

Agresif muhasebe; GKGMİ, muhasebe standartları ve yasal düzenlemeler ile uyumlu olup olmadığına bakılmaksızın özellikle daha yüksek cari dönem karı elde etmek amacıyla zorlayıcı ve kasıtlı bir şekilde muhasebe politikalarının seçilmesi ve uygulanmasıdır (Mulford vd., 2002, s.3). Agresif kelimesi TDK’da “saldırgan” kelimesi ile tanımlanmaktadır. Dolayısı ile işletme performansını olduğundan çok daha iyi göstermek

amacıyla muhasebe politikaları seçiminde sınırları zorlayarak saldırgan davranmayı ifade etmektedir.

Agresif muhasebede, finansal tablolar ile bilgi kullanıcılarına sunulan karı fazlasıyla şişirmek ve varlıkları fazlasıyla yüksek göstermek için GKGMİ'ye uygun olarak aşağıdaki teknikler uygulanmaktadır (Ocak vd., 2014, s.128):

- a. Şüpheli alacaklara çok düşük karşılık ayırma,
- b. İlk giren ilk çıkar (FİFO) stok değerleme yöntemini kullanma,
- c. Pazarlama ve satış harcamalarını (ihtiyari olduğundan) aktifleştirme,
- d. Azalan bakiyeler amortisman yöntemini kullanma,

Agresif muhasebe uygulamalarının tam tersi yani karın ve varlıkların fazlasıyla düşük gösterilmesi ise literatürde “muhafazakâr muhasebe” olarak tanımlanmaktadır. Muhafazakâr muhasebede uygulanan teknikler ise aşağıda sıralandığı gibi agresif yöntemlerin tam tersi olmaktadır (Ocak vd., 2014, s.128) :

- a. Şüpheli alacaklara çok yüksek karşılık ayırma,
- b. Son giren ilk çıkar (LİFO) stok değerleme yöntemini kullanma,
- c. Pazarlama ve satış harcamalarını (ihtiyari olduğundan) giderleştirme,
- d. Normal amortisman yöntemini kullanma,

### **3.5.5 Yaratıcı Muhasebe Uygulamaları (Creative Accounting Practices)**

Yaratıcı muhasebe kavramı; herhangi bir teoriden değil, piyasa profesyonelleri ve gazete yorumcularının gözlemleri ile geliştirilmiş bir ifadedir. “Muhasebe el çabukluğu (accounting sleight of hand)”, “hesapları vitrine koyma/hesapları makyajlama (window dressing the accounts)”, kozmetik/makyajlı raporlama (cosmetic reporting)”, “defterlerle oynama (fiddling the books)” gibi kavramlar yaratıcı muhasebe uygulamalarını tanımlamak için kullanılmaktadır (Stowoly vd., 2000, 24).

Diğer yandan teknik bilgi ve beceri gerektirdiğinden; “defterleri pişirme sanatı (cooking the books)”, bilanço sunma sanatı (the art of presenting a balance sheet), kendi karını hesaplama

sanatı (the art of computing its profit) gibi ifadeler ile sanatsal bir eylem olarak da görülmektedir. (Stowoly vd., 2000, 24). “Yaratıcı veya yaratıcılık” kelimelerinin anlamı dolayısıyla bu kavramda sözü edilen ise muhasebe ilkelerine uygun bir şekilde, standartlaştırılmamış bir işlem ve olayın varlığında, boşluktan faydalanarak belirli hedefler doğrultusunda farklı yorumlama yaparak gerçekte olmayan bir görünümün yaratılmasıdır.

Buradan hareketle yaratıcı muhasebe; bilgi kullanıcılarının, işletmenin finansal durumu ve performansı, nakit akışı, risk düzeyi hakkındaki algılarının pozitif olmasını sağlamak için, GKGMİ, muhasebe standartları ve yasal düzenlemelere uygun ancak bunlardaki mevcut esnekliklerden ve boşluklardan (eksikliklerden) faydalanılarak finansal tabloları (bilanço, gelir tablosu, nakit akış tablosu gibi) olduğundan daha iyi göstererek, makul ve doğru finansal tablo sunumundan uzaklaşılmasına sebep olan uygulamalardır (Ocak vd., 2014, s.128).

Yaratıcı muhasebe uygulamaları, muhasebe ilkelerinin agresif bir şekilde seçilmesi ve uygulanmasına yönelik hileli finansal raporlama ve kazanç yönetiminin tüm yöntemleri dahil her türlü manipülasyon tekniklerini kapsamaktadır (Mulford vd., 2002, s.3). Bunun yanı sıra hileli finansal raporlama yöntemine kıyasla daha az riskli veya zararlı olarak değerlendirilmektedir. Bunun sebebi de yaratıcı muhasebe ile hile arasındaki farktır. Yaratıcı muhasebede, muhasebe ilke ve standartlarına uyularak bunlardaki boşluklardan yararlanılmaktayken; hileli finansal raporlamada, yasal olmayan ve muhasebe ilke ve standartlarına tamamen aykırı bir şekilde davranılmaktadır (Çıtak, 2009, s.86).

Diğer yandan kazanç yönetiminden farklı olarak; sadece raporlanacak kar etkilenmeye çalışılmamakta, genel itibarıyla nakit yaratma gücü, borç-özkaynak oranı gibi finansal analizde kullanılan oranlar üzerinden işletmenin görünümü daha iyi gösterilmeye çalışılmaktadır. Bir diğer farkı ise kazanç yönteminde kar sadece yüksek değil düşük de gösterilebilmekteyken; yaratıcı muhasebe uygulamalarında işletmenin genel durumunu iyi göstermek için kar sadece yüksek gösterilmektedir (Ocak vd., 2014, s.132).

GKGMİ’ne uygun olarak yapılan yaratıcı muhasebe uygulama teknikleri aşağıda sıralanmıştır: (Mulford vd., 2002, s.14; Küçüksözen, 2004, s.90):

- a. Gelirin erken yani tahakkuk etmeden muhasebeleştirilmesi veya fiktif (olmayan) gelir yaratılması,

- b. Agresif aktifleştirme yapılması veya amortisman faydalı ömrünün uzatılması,
- c. Varlık ve yükümlülüklerin yanlış bildirilmesi,
- d. Gelir Tablosu kalemleri sınıflandırmasının değiştirilmesi,
- e. Nakit Akım Tablosunda, nakit sınıflandırmalarının değiştirilmesi (yatırımlardan sağlanan nakdin faaliyetlerden sağlanıyormuş gibi gösterilmesi).

### **3.5.6 Hileli Finansal Raporlama (Fraudulent Financial Reporting)**

Hileli finansal raporlama; finansal tablo kullanıcılarını aldatmak amacıyla GKGMİ'ne, standartlara ve yasal düzenlemelere aykırı olarak kasıtlı yapılan, yanlış beyanlar, finansal tablolardaki tutarlar veya açıklamaların ihmal edilmesine yönelik her türlü uygulamadır (Mulford vd., 2002, s.3).

Literatürde muhasebe usulsüzlükleri (accounting irregularities) ifadesi ile de kullanılan hileli finansal raporlama kavramı; işletmenin finansal durumu ve performansı hakkında finansal bilgi kullanıcılarının gerçeğe aykırı ve yanlış bilgilendirilmesine sebep olan tüm manipülasyon yöntemlerinin, muhasebe ilkeleri sınırlarını aşan bir birleşimdir (Küçüksözen, 2004, s.101).

Hileli finansal raporlamada; satışları yüksek göstermek için sahte fatura düzenlemek, kayıtlı işlemleri silmek, belgeler üzerinde tahrifat yapmak, fiktif işlem kaydetmek veya önemli bilgi ve belgeleri yok etmek vb. gibi uygulamalar suç tanımı içerisinde yer almakta ve idari merciler tarafından tespit edilmesi halinde yaptırım uygulanmaktadır.

### **3.6 FİNANSAL BİLGİ MANİPÜLASYONUNUN TESPİT EDİLMESİNDE VE ÖNLENMESİNDE UYGULANAN YAKLAŞIMLAR**

Hilenin tespit edilmesi ve önlenmesinde, yönetim ve üst düzey yöneticiler birincil sorumlulardır. Bu nedenle işletmede, etik ve dürüst davranış kültürünü yerleştirmeleri ve hile girişimi ihtimaline yönelik caydırıcı bir tutum sergilemeleri gerekmektedir. Diğer yandan bu hususta denetçilerin sorumluluğu ise denetim sürecini, bağımsız denetim standartlarına uygun gerçekleştirmek ve finansal tablolarda hata veya hileler nedeniyle meydana gelen önemli yanlışlıkların yer almadığı konusunda makul güvence sağlamaktır. Bunun yanı sıra bağımsız denetim standartlarına uygun gerçekleşen bir denetim sürecine



rağmen yapısal kısıtlamalar dolayısıyla hata ve hilelerin denetçiler tarafından tespit edilememe riski kaçınılmazdır (KGK, BDS 240, md.4 ve 5).

Her ne kadar hilenin tespit edilmesi ve önlenmesi sorumluluğu yönetime ait olsa da geçmişte yaşanan büyük skandallar, yönetim tarafından gerçekleştirilen finansal bilgi manipölasyonlarına örneklerdir. Bu tür manipölasyonlar, bağımsız denetime rağmen ortaya çıkarılamayabilmekte ve yarattıkları finansal maliyet oldukça yüksek olmaktadır. Nitekim Tablo 3.5'te görüldüğü üzere karşılaşma sıklığı en düşük olan finansal tablo hileleri (yönetici hileleri), işletmelere ve ekonomiye en yüksek zararı vermektedir.

Bu durum bağımsız denetime tabi tutularak sunulan finansal tablolara duyulan güvenin sarsılmasına neden olmuş ve klasik hile tespit yöntemlerinin yanı sıra alternatif olarak, hile yapılmasını önlemeye yönelik erken uyarı mekanizmaları ihtiyacını ortaya çıkarmıştır (Uğurlu vd., 2015, s. 65-66).

**Tablo 3.5:** Yıllar İtibarıyla Türlerine Göre Suistimal Gerçekleşme Oranları ve Maliyetleri.

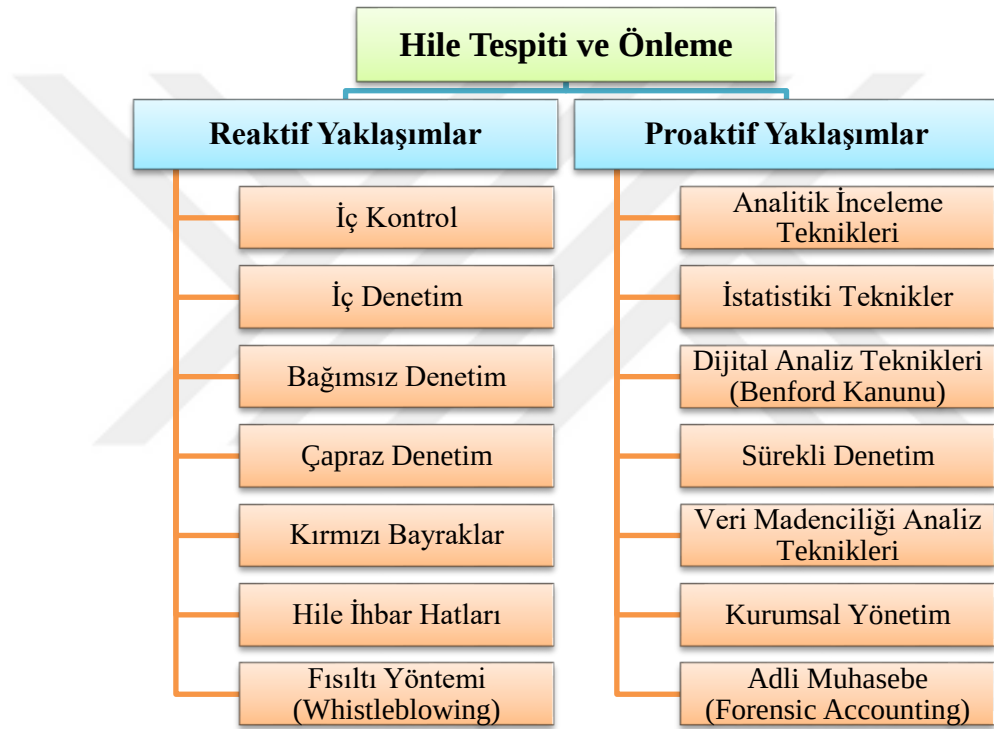
| SUİSTİMAL TÜRLERİ               | 2018 YILI      |                        | 2020 YILI      |                        | 2022 YILI      |                        | 2024 YILI      |                        |
|---------------------------------|----------------|------------------------|----------------|------------------------|----------------|------------------------|----------------|------------------------|
|                                 | Vaka Oranı (%) | Ortalama Maliyeti (\$) | Vaka Oranı (%) | Ortalama Maliyeti (\$) | Vaka Oranı (%) | Ortalama Maliyeti (\$) | Vaka Oranı (%) | Ortalama Maliyeti (\$) |
| Varlıkların Kötüye Kullanılması | 89%            | 114,000                | 86%            | 100,000                | 86%            | 100,000                | 89%            | 120,000                |
| Yolsuzluk                       | 38%            | 250,000                | 43%            | 200,000                | 50%            | 150,000                | 48%            | 200,000                |
| Finansal Tablo Hileleri         | 10%            | 800,000                | 10%            | 954,000                | 9%             | 593,000                | 5%             | 766,600                |

**Kaynak:** [ACFE, 2018; 2020; 2022; 2024]

Dolayısıyla literatürde hile tespit ve önlemede kullanılan çok çeşitli yöntem ve modeller geliştirilmiştir. Bu yöntemler, teknolojik temelli - teknolojik temelli olmayan (Bozkurt, 2011), geleneksel – gelişmiş/çağdaş (Kandemir vd., 2012a; 2012b), tahakkuk esaslı – karma – alternatif (Küçükkocaoğlu vd., 1997), reaktif – proaktif (Abdioğlu, 2007) gibi farklı sınıflandırmalar altında açıklanmaktadır. Bu çalışmada ise, hile gerçekleştikten sonra (tespite yönelik) ve gerçekleşmeden önce (önlemeye yönelik) uygulanan yöntemler esas alınarak yapılan Şekil 3.3'te görülen reaktif – proaktif sınıflandırması dikkate alınmakta ve ardından bu yöntemler kısaca açıklanmaktadır.

Reaktif yaklaşımda; hile belirtilerinin gözlenmesi veya hile yapıldığına dair bir şikâyet alınması halinde, şüpheli alan ile ilgili inceleme yapılarak hile tespit edilmeye çalışılmaktadır. Proaktif yaklaşımda ise herhangi bir hile belirtisi bulunmuyorken, işletmede ortaya çıkabilecek hile riski analiz edilerek, olası hileleri önlemeye yönelik teknikler uygulanmaktadır (Ertikin, 2017, s.78).

Reaktif yöntemler; küçük veri setlerinin hile denetiminde ve çoğunlukla manuel olarak uygulanan yöntemler iken; proaktif yöntemler, büyük veri setlerinin hile denetiminde uygulanan bilgisayar destekli yöntemlerdir (Onocak, 2022, s.218).



**Şekil 3.3:** Finansal Bilgi Manipülasyonunun Tespitinde ve Önlenmesinde Uygulanan Yaklaşımlar.

Dolayısıyla hile tespit ve önleme yönteminin seçimini, veri setlerinin büyüklüğü ve karmaşıklığı etkilemektedir. Diğer yandan hangi yöntemlerin daha etkili ve uygulanabilir olduğunu, işletmenin süreç ve faaliyetlerinin hileye ne kadar açık olduğunu gösteren “hile risk değerlendirmesi” sonuçları belirlemektedir. Ancak bu değerlendirme aynı zamanda, etkili iç kontrol sistemlerinin hangi alanlarda yoğunlaştırılacağını belirlemenin zorluğuna da işaret etmektedir. Çünkü gereğinden fazla kontrol, maliyetleri artırmakta ve süreçleri yavaşlatmaktadır (Yılmaz, 2019, s.89). Ayrıca mevcut teknolojik altyapı ve teknolojik yetkinlik, işletmenin organizasyon yapısı, kültürü, bütçesi, insan kaynakları ve yasal

gereklilikler de hile tespit ve önleme yönteminin uygunluğunu belirlemede önemli rol oynamaktadır.

Bu etkenlerin yanı sıra, PwC (2003)'nin Küresel Ekonomik Suç Araştırması (Global Economic Crime Survey)'na göre; suistimal mağduru olmamış işletmeler, davranış kuralları veya suistimal raporlama politikaları gibi soyut önleme araçlarına yani proaktif yöntemlere daha fazla güvenme eğilimindeyken; suistimale maruz kalmış olanlar, ihbar politikaları ve suistimal önleme ve tespit eğitimleri gibi daha somut önlemler yani reaktif yöntemler uygulamaktadır (Bierstaker vd., 2006, s.523)

ACFE (2024)'nin araştırma sonuçlarına göre ise proaktif tespit yöntemleri ile, reaktif tespit yöntemlerine göre çok daha hızlı bir şekilde hile tespitinde bulunulmakta ve suistimali aktif bir şekilde araştırmayan (reaktif) yöntemler kullanan işletmeler, çok daha uzun süre devam eden ve daha yüksek maliyet yaratan suistimallerle karşılaşmaktadırlar (ACFE, 2024, s.24). Dolayısıyla proaktif yöntemler, hile belirtisi veya ihbarını beklemeden hilelerin erkenden tespit edilmesini ve hile kaynaklı maddi kayıpların asgari düzeye indirilmesini sağlamaktadır (Mert vd., 2022, s.69).

**Tablo 3.6:** KPMG ve ACFE Raporlarına Göre Suistimal Tespit Yöntemleri ve Vaka Oranları.

|    | SUİSTİMAL TESPİT<br>YÖNTEMLERİ                    | KPMG              |                   | SUİSTİMAL TESPİT<br>YÖNTEMLERİ           | ACFE<br>Küresel<br>(2024) |
|----|---------------------------------------------------|-------------------|-------------------|------------------------------------------|---------------------------|
|    |                                                   | Küresel<br>(2016) | Türkiye<br>(2020) |                                          |                           |
| 1  | İhbar hattı dışında bildirim                      | 24%               | 24%               | İhbar                                    | 43%                       |
| 2  | Yönetim incelemesi                                | 22%               | 38%               | İç denetim                               | 14%                       |
| 3  | İhbar hattı                                       | 20%               | 29%               | Yönetim incelemesi                       | 13%                       |
| 4  | İç denetim                                        | 14%               | 36%               | Belge incelemesi                         | 6%                        |
| 5  | Tesadüfen                                         | 14%               | 7%                | Hesap mutabakatı                         | 5%                        |
| 6  | Şüphelenilen amir                                 | 10%               | 16%               | Tesadüfen                                | 5%                        |
| 7  | Üçüncü taraf durum<br>değerlendirme               | 7%                | 11%               | Bağımsız denetim                         | 3%                        |
| 8  | Proaktif suistimal odaklı veri<br>analitiği       | 3%                | 9%                | Veri izleme                              | 3%                        |
| 9  | İtiraf                                            | 3%                | -                 | Gözetim                                  | 2%                        |
| 10 | Müşteri veya tedarikçi şikâyeti                   | -                 | 22%               | Kamu / Kolluk<br>kuvvetleri aracılığıyla | 2%                        |
| 11 | Teknoloji kullanımı / Proaktif<br>data analizleri | -                 | 9%                | Diğer                                    | 2%                        |
| 12 | Kamu / Kolluk kuvvetleri<br>aracılığıyla          | -                 | -                 | İtiraf                                   | 1%                        |

**Kaynak :** [KPMG, 2020, s.16; ACFE, 2024, s.24]

Buna rağmen; KPMG (2020) ve ACFE (2024)'nin Tablo 3.6'da özetlenen suistimal raporlarına göre; suistimal vakalarının tespitinde en çok, özellikle de ihbar yöntemi olmak üzere, reaktif yöntemler etkili olmaktadır, proaktif yöntemler neredeyse yok denecek kadar az kullanılmaktadır.

### 3.6.1 Reaktif Yaklaşımlar

Reaktif yaklaşımlarda, geleneksel veya klasik hile tespit yöntemleri kullanılmakta ve pasif bir yaklaşım izlenmektedir. Pasif yaklaşım ile kastedilen ise iç kontrol sisteminin, yönetimin beklentisini karşılayacak şekilde gerçekleşip gerçekleşmediğinin değerlendirilmesidir. Bu değerlendirme, tarafsız ve tesadüfi örnek seçimine göre yapılmaktadır. Ayrıca hile tespit süreci, yalnızca ihbar, şikâyet veya hile belirtisi olması halinde başlamaktadır ve araştırılan iddiaların açıklığa kavuşturulmasını hedeflemektedir (Bozkurt, 2011, s. 174; Pehlivanlı, 2011, s.16).

Reaktif yaklaşımda uygulanabilecek yöntemler; (i) iç kontrol, (ii) iç denetim, (iii) bağımsız denetim, (iv) çapraz denetim, (v) kırmızı bayraklar, (vi) hile ihbar hatları ve (vii) fısıltı yöntemi olarak sınıflandırılmaktadır.

#### 3.6.1.1 İç kontrol

Çalışanları hile yapmaya iten nedenlerden “fırsat” unsuru, işletmenin kontrol altına alabileceği yegâne unsurdur. Hileye uygun ortam yaratılmasını sağlayan olası fırsatların azaltılması, ancak işletmede dürüstlük ve etik değerlerin hâkim olması ve etkin bir iç kontrol sisteminin varlığı ile mümkün olabilmektedir (Kocameşe vd., 2010, s.29).

İç kontrol, 5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'nun 55. maddesinde; *“idarenin amaçlarına, belirlenmiş politikalara ve mevzuata uygun olarak faaliyetlerin etkili, ekonomik ve verimli bir şekilde yürütülmesini, varlık ve kaynakların korunmasını, muhasebe kayıtlarının doğru ve tam olarak tutulmasını, mali bilgi ve yönetim bilgisinin zamanında ve güvenilir olarak üretilmesini sağlamak üzere idare tarafından oluşturulan organizasyon, yöntem ve süreçle iç denetimi kapsayan mali ve diğer kontroller bütünüdür”* şeklinde tanımlanmıştır. 2003 tarihli bu kanun maddesi 1985 yılında kurulan COSO (Committee of Sponsoring Organisations - Sponsor Kuruluşlar Komitesi)'nin yapmış olduğu iç kontrol tanımının bir benzeridir.

İç kontrol, kurumsal risk yönetimi ve suistimal caydırıcılığı alanlarında standartlar geliştiren ve gönüllü bir özel sektör girişimi olan COSO<sup>48</sup> tarafından 1992 yılında yayınlanan “İç Kontrol Bütünleşik Çerçeve (Internal Control Intergated Framework)<sup>49</sup>”de, iç kontrol kavramı ve etkin bir iç kontrolün sağlanması için entegre bir şekilde birlikte çalışması gereken beş unsur ve her bir unsura ait ilkeler tanımlanmıştır. Bu bileşenler; (i) kontrol ortamı, (ii) risk değerlendirmesi (iii) kontrol faaliyetleri, (iv) bilgi ve iletişim ve (v) izlemedir (McNally, 2013, s.2-5). Çerçeveye göre; her bir bileşenin işletmede mevcut ve işler olması halinde iç kontrol sistemi, sistemde ortaya çıkabilecek birkaç eksikliğe rağmen risklerin önlenmesi açısından yöneticilere makul bir güvence sağlamaktadır (İbiş vd., 2012, s.117).

Söz konusu beş unsurdan kontrol ortamı, iç kontrol sisteminin başarılı bir şekilde işlemesi için gereken en temel bileşendir (İbiş vd., 2012, s.101). IIA (The Institute of Internal Auditors - İç Denetçiler Enstitüsü) iç kontrolü; üst düzey yönetim ve yönetim kurulunun, işletme içindeki kontrol sistemine verdikleri önemi gösteren tavır ve davranışları olarak tanımlamış ve kontrol ortamının, iç kontrolün amaçlarına ulaşmada gereken disiplini ve çevreyi sağlaması gerekliliğini ifade etmiştir. Ayrıca kontrol alanında düzenlenmesi gereken unsurların; dürüstlük ve etik ilkeler, organizasyon yapısı ve bu yapıdaki yetki ve sorumlulukların tespit edilmesi, yönetim felsefesi ve şekli, insan kaynakları politikaları ve personel yeterliliğinden oluştuğunu belirtmiştir (Yılmaz, 2018, s.95).

İç kontrol sistemi, işletme yönetiminin belirlemiş olduğu politika ve kurallara riayet edilmesini ve finansal raporların gerçeğe uygun, tam zamanında ve eksiksiz bir şekilde hazırlanmasını sağlamaktadır. Ayrıca iç kontrol birimlerinden alınan verilerin bağımsız denetim birimi tarafından tekrar denetime tabi tutulmasıyla muhasebe bilgi sisteminin sağladığı hesaplara ve finansal raporlara güvenilirlik de temin edilmektedir (Yıldız vd., 2014, s.7). Dolayısıyla iç kontrol sisteminin mevcut olması, işletmelere ve ilgililere sundukları finansal tablolara olan güvenin temel altyapısını oluşturmaktadır. İç kontrol sisteminin etkin olması da denetim sürecinde gözden kaçırılabilir hata ve eksiklikleri en aza indirerek denetim kalitesini yükseltmektedir. Diğer yandan denetim sürecinin daha kısa

---

<sup>48</sup> COSO organizasyonunun oluşumuna beş kâr amacı gütmeyen kuruluş sponsor olmuştur. Bu kuruluşlar: AAA (American Accounting Association), AICPA (American Institute of Certified Public Accountants), FEI (Financial Executives International), IIA (Institute of Internal Auditors) ve IMA (Institute of Management Accountants)’dır.

<sup>49</sup> 1992 yılında yayınlanan İç Kontrol Bütünleşik Çerçeve, 2013 yılında SOX (Sarbanes-Oxley Yasası) kapsamında güncellenmiştir.

sürede tamamlanmasını ve bu sayede denetim maliyetlerinin azalmasını sağlamaktadır (İşgüden Kılıç vd., 2018, s.63).

Özetle; iç kontrol sisteminin mevcudiyeti, işletme yönetiminin görev ve sorumluluklarını artırmakla birlikte hilelerin tespit edilmesi ve önlenmesine katkı sağlamaktadır (Yıldız vd., 2014, s.7).

### **3.6.1.2 İç denetim**

İç kontrol bileşenlerinden “izleme ve gözetim” unsuru, iç denetim faaliyetleri çerçevesinde gerçekleştirilmektedir (Kandemir vd., 2012a, s.48). Dolayısıyla “iç kontrol” daha geniş bir kavram olup; “iç denetim”, iç kontrol sisteminin etkin ve yeterli olup olmadığını incelemek ve değerlendirme fonksiyonu görmektedir (Blackstone ve William, 1994, s.20 Akt. İbiş vd., 2012, s.99).

IIA’ya göre iç denetim; “işletme faaliyetlerinin geliştirilmesi ve onların değerlerini arttırmak amacı ile yapılan bağımsız ve objektif bir güvence ve danışmanlık alma işlemi”dir (Öztoprak, 2017, s.118). Bununla birlikte iç denetim sürecini yürüten iç denetçilerin görevi ise işletme yönetimine bağlı olarak iç kontrol sisteminin, işletmenin hedeflerine, ilkelerine, kurallarına ve mevzuata uygunluğunun denetlenmesi, riskli alanların belirlenmesi ve hile ve suistimallerin araştırılması faaliyetlerinde bulunmaktır (İşgüden Kılıç vd., 2018, s.62). Dolayısıyla iç denetçiler, işletmede tam zamanlı çalışarak, finansal raporlama sürecine aktif bir şekilde dahil olup, edindikleri bilgileri bağımsız denetim komitesine (audit committee)<sup>50</sup> doğrudan iletme fırsatına sahiptirler (Young, 2002, s.17).

İç denetçilerin, işletmenin her türlü bölümlerine, işlevlerine, kayıtlarına, personeline ve varlıklarına sınırsız erişim hakkına sahip olmaları, denetim sürecinin zaman sınırlaması olmadan daha kolay gerçekleştirilmesini sağlamaktadır. Bu ayrıcalıklı konumları sebebiyle de işletmede güvenlik birimi olarak algılandıklarından iç denetim, hile tespit ve önlemede yüksek etki yaratmaktadır. Diğer yandan işletme personeli olarak istihdam edilmeleri, bilgi toplama maliyetlerini düşürürken, yöneticilerle iş birliği yapılarak hileli işlemlerin yapılması

---

<sup>50</sup> Bağımsız denetim komitesi; şirket yönetim kurulunda bulunan ancak icracı olmayan bağımsız üyelerdir (Küçüksözen, 2004, s.130).

riskini artırmaktadır. Dolayısıyla iç denetimin etki düzeyi organizasyon yapısındaki yerine, hiyerarşik ilişkilerine ve yönetimin verdiği öneme bağlıdır (Kandemir vd., 2012a, s.48-51).

Nitekim KPMG (2020)'nin raporuna göre (Tablo 3.1), hilelere ilk yol açan %69 ile zayıf iç kontrol sistemleri iken; ACFE (2024) raporuna göre (Tablo 3.6), iç denetim, %14 ile en sık kullanılan ikinci suistimal tespit yöntemi olarak bu tür hileleri ortaya çıkarmaktadır.

### 3.6.1.3 Bağımsız denetim

Bağımsız denetim; bir dış denetim türüdür ve işletmelerin finansal bilgilerinin ve hazırlamış oldukları finansal tablolarının, kendi iç denetim birimleri dışında, genel olarak güvenilir kabul edilen bağımsız kuruluşlar tarafından denetlenmesini ifade etmektedir.

Sermaye Piyasası Bağımsız Denetim Standartları Seri X No 22 Md. 4/b'de bağımsız denetim, *“işletmelerin kamuya açıklanacak veya Kurulca (SPK) istenecek yıllık finansal tablo ve diğer finansal bilgilerinin, finansal raporlama standartlarına uygunluğu ve doğruluğu hususunda, makul güvence sağlayacak yeterli ve uygun bağımsız denetim kanıtlarının elde edilmesi amacıyla bağımsız denetim standartlarında öngörülen gerekli tüm bağımsız denetim tekniklerinin uygulanarak, defter, kayıt ve belgeler üzerinden denetlenmesi ve değerlendirilerek rapora bağlanması”* şeklinde tanımlanmıştır. Bağımsız denetim faaliyetlerini gerçekleştiren her kademdeki denetim elemanları ise bağımsız denetçi olarak adlandırılmaktadır.

İşletmelerde bağımsız denetime ihtiyaç duyulması; iç denetçilerin, işletme personeli olarak istihdam edilmeleri dolayısıyla yönetime bağımlılıklarının olası bir yönetim hilesi durumunda iş birliğine zorlanmalarına sebebiyet vermesinden kaynaklanmaktadır. Buna karşılık iç denetimin üzerindeki bir bağımsız dış denetim baskısı, işletme yönetimi ve iç denetçiler arasındaki iş birliğinin engellenmesini sağlamaktadır (Kandemir, 2012a, s.51).

Söz konusu avantajına rağmen ACFE (2024, s.38)'nin suistimal raporları göstermektedir ki, suistimal mağduru işletmelerin %84'ü mali tablolarını bağımsız denetime tabi tutmuşlar<sup>51</sup> ancak tüm hile vakalarının yalnızca %3'ü (Tablo 3.6) bağımsız denetim aracılığıyla tespit edilebilmiştir. Dolayısıyla işletmelerin hile tespitine ve önlemeye yönelik ikinci en çok

---

<sup>51</sup> ACFE (2024, s.38) raporuna göre; dış denetim dışında işletmelerin hile tespiti ve önlemede en çok kullandığı yöntemler birinci sırada %85 ile davranış kuralları, üçüncü sırada ise %80 ile iç denetimdir.

kullandıkları yöntem bağımsız denetim iken bu yöntemin etki derecesi, yaygınlığına rağmen diğer yöntemlere göre düşük kalmaktadır. Bunun nedeni bağımsız denetimlerin belirli bir zaman diliminde ve sınırlı kaynaklarla gerçekleştiriliyor olmasıdır.

Diğer yandan Bağımsız Denetim Standartları'na göre (BDS No:240 ms.5); hata ve hilelerin tespitinde birincil sorumlu işletme yönetimidir ve bağımsız denetçinin sorumluluğu, mali tabloların geneline yönelik önemli hata ve hilelerin olmadığına dair makul güvence vermektir. Yönetimin bağımsız denetçiler tarafından denetiminin, bu sınırlandırılmış kapsamı dolayısıyla gerekli dikkat ve özen gösterilse dahi bazı önemli hata ve hileler engellenemeyebilmektedir. Bununla birlikte işletme çalışanlarının denetleniyor olmaları sebebiyle hile yapmaktan kaçınmalarını sağlamakta böylece hilelerin önlenmesi konusunda caydırıcı olmaktadır (İşgüden Kılıç vd., 2018, s.63).

#### **3.6.1.4 Çapraz denetim tekniği**

Çapraz denetim tekniği; muhasebe hesaplarının işleyiş kuralları itibarıyla, GKGMİ'ne aykırı olarak karşılıklı çalışmaması gereken hesapların belirlendiği bir hile tespit yöntemidir. Bu teknikte öncelikle karşılıklı çalışması gereken hesaplar belirlenmekte ardından yevmiye maddeleri taranmaktadır. Eğer ki karşılıklı çalışması şüpheli olan kayıtlara rastlanırsa, yevmiye kayıtları incelenmeye alınmaktadır. Ayrıca hesapsal uygunluğun yanı sıra tutarsal denklige de dikkat edilmektedir (Çankaya vd., 2009, s.100).

Çapraz denetim tekniğinin işleyişinde; “Karşı Hesaplar Tablosu” ve “Artışlar Azalışlar Tablosu” olmak üzere iki tablo düzenlenerek aykırılıklar tespit edilmeye çalışılmaktadır. Karşı hesaplar tablosu, belirli bir dönemde hesap bakiyelerinde değişim olan hesap kalemlerinin gösterildiği bir tablodur. Artışlar azalışlar tablosu ise denkleştirme formülü aracılığıyla belirli bir dönemde hesap bakiyelerinde gerçekleşen artış ve azalışların gösterildiği dinamik bir tablodur. Bu tabloda denkleştirme sağlanamaması, hile riskinin mevcudiyetini göstermektedir. Bu yöntem, 100.000 adedin üzerinde yevmiye maddesinin olması ve kayıtların elektronik ortamda tutulmaması durumlarında kullanıma elverişli değildir (Kara vd., 2023, s.78-79).



### 3.6.1.5 Kırmızı bayraklar

Kırmızı bayraklar, işletme çalışanları ve yöneticilerin tutumlarında ortaya çıkan anormallikler olarak ifade edilen hile belirteçleridir, yani hilenin parmak izleridir (Onocak, 2022, s.219). Hilenin keşfi, hile belirteçlerinin ortaya çıkarılması ile başlamaktadır. Dolayısıyla bu belirteçlerin; yöneticiler, denetçiler ve araştırmacılar tarafından iyi bilinmesi gerekmektedir. Bununla birlikte bu belirteçler kesin bir hile kanıtı değildir. Hile belirtecinin fark edilmesi halinde gizli tutulmalı ve kesin sonuca ulaşılan kadar araştırmaya devam edilmelidir. Hile belirteçlerinin etkin bir şekilde izlenmesi ile, hilelerin erken dönemde yakalanma ihtimali artmaktadır (Arzova, 2003, s.121).

İşletmelerde karşılaşılan potansiyel hile belirteçleri, altı grupta sınıflandırılmaktadır: (i) muhasebe ile ilgili anormallikler, (ii) iç kontrol zayıflıkları, (iii) analitik anormallikler, (iv) aşırı yaşam biçimleri, (v) olağan olmayan davranışlar ve (vi) şikayetler, uyarılar, imalar (Albrecht vd., 1995, s.53-55 Akt. Arzova, 2003, s.121).

**Tablo 3.7:** ACFE 2024 Raporuna Göre Kırmızı Bayrak Belirteçleri.

|   | KIRMIZI BAYRAK BELİRTEÇLERİ                          | 2024 YILI |
|---|------------------------------------------------------|-----------|
| 1 | İmkânların ötesinde yaşamak                          | 39%       |
| 2 | Finansal zorluklar                                   | 27%       |
| 3 | Satıcı/müşteri ile alışılmadık derecede yakın ilişki | 20%       |
| 4 | Kontrol sorunları, görevleri paylaşmada isteksizlik  | 13%       |
| 5 | Sinirlilik, şüphecilik veya savunmaya geçme          | 12%       |
| 6 | Kurnaz davranışlar                                   | 12%       |
| 7 | Zorbalık veya Sindirme                               | 11%       |
| 8 | Boşanma/Ailevi problemler                            | 10%       |

ACFE (2024, s.66-68)'nin suistimal araştırmasında; en sık görülen kırmızı bayrak belirteçleri ise Tablo 3.7'de gösterildiği üzere sekiz kategoride tanımlanmaktadır. Bu kategoriler içinde en yaygın davranışsal tehlike işareti, faillerin %39'u tarafından sergilenen “imkanlarının ötesinde bir yaşam tarzının” olması, ikincil olarak “finansal zorluklar” yaşamak (%27) ve üçüncü olarak ise bir “satıcı veya müşteriyle alışılmadık derecede yakın bir ilişki” içinde olmak (%20)'tir. Ayrıca vakaların %84'ünde failler bu sekiz belirteçten en az birini sergilerken; vakaların yarısından fazlasında (%52) birden fazla belirteç gözlenmiş; %16'sında ise hiçbir belirteç gözlenmemiştir.

### 3.6.1.6 Hile ihbar hatları

İhbar hatları; işletme ile ilgili hile konusunda bilgi ve haber sağlamak için özel olarak ayrılmış, direkt telefon hatlarıdır. Telefon hatlarının yanı sıra mektup, faks, elektronik posta gibi diğer iletişim kanalları da bu amaçla kullanılmaktadır. Böylece ne kadar çok ve çeşitli iletişim aracı kullanılabilirse elde edilen önemli bilgilerin çokluğu da o kadar fazla olmaktadır (Kandemir vd., 2012b, s.48).

ACFE'nin iki yılda bir yapmış olduğu hile araştırmaları sonuçlarına göre; suistimallerin ortaya çıkarılmasında yıllar itibarıyla kullanılan en etkili ve yaygın yöntem, ihbar yöntemidir. 2024 yılı raporuna göre (Tablo 3.6) tüm vakaların %43'ü ihbar ile tespit edilmiştir. İhbarların, %30'u telefon, %37'si e-posta ve %40'ı web tabanlı iletişim yollarıyla yapılmıştır. Diğer yandan tüm ihbarların, yarısından fazlası (%52) kurum içindeki çalışanlar tarafından yapılmışken; müşteriler (%21), satıcılar (%11) ve rakipler gibi dış kaynaklar tarafından yapılan ihbarlar toplamda üçte birini oluşturmuştur. Ayrıca ihbar hattı olan kuruluşların, ihbar hattı olmayan kuruluşlara kıyasla suistimal tespit etme olasılığı ise neredeyse iki kat daha fazla gerçekleşmiştir. Dolayısıyla suistimal tespitinde ihbarlar, oldukça önemli bir rol üstlenmektedir (ACFE, 2024, s.23).

İhbar yönteminin etkili bir şekilde işlemesi için ise bazı özelliklerin var olması gerekmektedir. Bu özellikler aşağıda maddeler halinde özetlenmiştir (Kandemir vd., 2012b, s.50-53) :

- a. İhbarcılarının kimlikleri gizlenerek, anonimlikleri korunmalıdır.
- b. İhbarlar önemslenerek geçekliği araştırılmalıdır.
- c. Herhangi bir şekilde kimliklerinin ifşa olması halinde, misillemeye karşı ihbarcılarının korunabileceği, diğer yandan asılsız ihbarlara karşı da cezalandırılabilceği bir sistem oluşturulmalıdır.
- d. İhbar hatlarına yurt içinden ve dışından erişim, kesintisiz (7 gün 24 saat), kolay ve ücretsiz olmalıdır.
- e. İhbar hatlarında, işletme personeli dışında bağımsız ve telesekreter yerine canlı görevli personel çalışmalıdır.

- f. İşletmede ihbar hatlarına ilişkin bilgilendirmeler sağlanarak, kurum kültürü olarak ihbarlar çeşitli ancak sınırlı (hilenin belirli bir yüzdesi vb. gibi) ödüllendirmelerle teşvik edilmelidir.

Diğer yandan ihbar hattı oluşturulması işletmeye masraf ve çok sayıda asılsız ihbar araması sebebiyle artı sorumluluklar yükleyebilmektedir. Ancak avantajları daha baskın gelmektedir. Öyle ki ihbar hatları daha güçlü kurumsal ilişkiler ve iç denetim yapısı sağlamaktadır. Düşük maliyetle hem işletme içi hem de işletme dışı kaynaklardan hileler tespit edilebilmekte ve bu durum çalışanlar tarafından bilindiği için de hile eylemine geçmede caydırıcı olabilmektedir (Abdioğlu, 2007, s.132).

#### **3.6.1.7 Fısıltı yöntemi (Bilgi ifşası -Whistleblowing)**

İngilizce’de “düdük/ıslık çalmak” anlamına gelen “whistleblowing”, literatürde ihbarcılık veya ifşacılık anlamında kullanılmaktadır. Bu kullanım, İngiliz polisinin suç işleme potansiyeline sahip kişileri engellemek amacıyla düdük çalarak uyarması şeklindeki müdahaleden esinlenilmiştir. Dolayısıyla yasalara ve etik değerlere aykırı tutum ve davranışların, bir düdük (ifşa) vasıtasıyla durdurulmaya çalışılması, ilgili kavramın temel prensibini açıklamaktadır (Sayğan, vd., 2013, s.5).

Buradan hareketle whistleblowing veya bilgi ifşası; *“bir organizasyon içerisinde yasa-dışı ve etik değerlere uygun olmayan davranış ve eylemlerin organizasyon içi ve/veya organizasyon dışı başka kişilere veya kurumlara zarar vermemesi için enformasyon sahibi kişiler (çalışanlar veya paydaşlar) tarafından sorunları çözme güç ve yetkisine sahip iç ve dış otoritelere bildirilmesi”*dir (Aktan, 2015, s.23).

Ayrıca bilgi ifşası, literatürde “principled organizational dissent (prensiplere dayalı organizasyonel ihtilaf)” terimi ile de kullanılmaktadır. Bu yöntemde; işletmedeki “malpractice”, “organizational wrongdoing/misconduct” gibi terimlerle ifade edilen “örgütteki yanlış uygulamalar” hakkında bilgi sahibi olan kişi, gönüllü olarak kimliği gizli veya açık, sözlü veya yazılı biçimde, işletme içindeki yönetim birimlerine veya işletme dışı kanallara bu durumu bildirmektedir (Uyar vd., 2015, s.86).

Fısıltı yönteminde, ifşacılar (whistleblowers) ihbar hattı mekanizmasını kullanmadan gayri resmi şekilde ihbarda bulunmaktadırlar. ACFE (2024, s.27) suistimal raporuna göre (Tablo 3.8); bu yöntemle ihbarcılarının en çok bildirim yaptıkları taraf birim amirleridir (%29). İkinci

sırada yöneticilere (%16) ve üçüncü sırada iç denetçilere (%14) bildirimde bulunmaktadırlar. En az bildirimde bulundukları ise dış denetçiler (%1)'dir.

**Tablo 3.8:** ACFE 2024 Raporuna Göre İhbarcıların İlk Raporlama Birimleri.

|    | RAPORLAMA BİRİMİ                  | 2024 YILI |
|----|-----------------------------------|-----------|
| 1  | Birim Amiri                       | 29%       |
| 2  | Yönetici                          | 16%       |
| 3  | İç denetim                        | 14%       |
| 4  | Hile İnceleme Ekibi               | 13%       |
| 5  | Diğer                             | 11%       |
| 6  | İş arkadaşı                       | 8%        |
| 7  | Denetim Komitesi Kurulu           | 8%        |
| 8  | İnsan Kaynakları                  | 7%        |
| 9  | Kanun uygulayıcı veya düzenleyici | 5%        |
| 10 | İşletme sahibi                    | 4%        |
| 11 | Kurum içi danışman                | 2%        |
| 12 | Dış denetim                       | 1%        |

Bilgi ifşası sadece finansal bilgi manipölasyonlarını değil; üretimde sağlığa zararlı maddeler kullanımı veya üretimin ekolojiye zarar vermesi, insan hakları ihlalleri, taciz, şiddet vb. gibi genel topluma zarar veren etik ve yasal olmayan konuları da kapsamaktadır (Uyar vd., 2015, s.87). ABD’de politik kültürün bir parçası olarak yaygın şekilde kullanılan fısıltı yöntemi birçok büyük skandalın da ortaya çıkma sebebidir. Enron skandalında genel müdür yardımcısı Sherron Watkins muhasebe hilelerini genel müdüre bildirmesiyle pasif göreve alınmış ardından işten ayrılarak resmi makamlara bildirmiştir. Worldcom skandalında mali denetçi ve başkan yardımcısı Cynthia Cooper, yolsuzluğu denetim firması Arthur Anderson’a bildirmiş, durumun görmezden gelinmesiyle hükümete bildirmiştir. FBI ajanı Coleen Rowley, 11 Eylül saldırılarından FBI’nın önceden haberdar olduğunu ortaya çıkarmıştır. Türkiye’de Roche ilaç devinin yöneticilerinden Veysi Mungan, NeoRecormon isimli kanser ilacının yüksek fiyatla satıldığı ve iç denetimin rekabet kurallarına aykırı raporlandığını ihbar etmiştir (Mercan vd., 2012, s.170). Tüm bu skandallar, yasa dışı ve etik olmayan davranışların tespitinde whistleblowing’in ne derece önemli olduğunu ortaya koymaktadır.

Fısıltı yönteminin etkin işlemesi için; işletmeler, çalışanların gözlemledikleri hileleri bildirmeleri için cesaretlendirecek ve bununla birlikte asılsız iddiaların da önüne geçilecek politikalar izlemelidirler. Öyle ki etkin işleyen bir fısıltı yöntemine ilişkin işletmede bir

bilincin oluşması, çalışanların yakalanma risklerinin yüksek olduğu düşüncesiyle hile yapmaktan kaçınmalarını sağlayacaktır (Onocak, 2022, s.220).

### **3.6.2 Proaktif Yaklaşımlar**

Proaktif yaklaşım, işletmede zayıf iç kontrol yapısı ya da herhangi bir hile ihbarı olmadan hile yapılıp yapılmadığının araştırılmasıdır. Reaktif yaklaşımın aksine hile belirtisi veya ihbarın olması beklenilmeden her zaman işletmede hile gerçekleşebileceği beklentisi ile hareket edilmektedir. Bu yaklaşımda denetim, ihbar üzerine şüpheli alanlardan rastgele örneklem seçimi ile değil; işletmenin bütün veri tabanı üzerinden yapılmaktadır (Pehlivanlı, 2011, s.16).

Hilelerin önlenmesine yönelik yöntemleri kapsayan proaktif yaklaşımda, veri tabanı üzerinde hile analizi yapılması için bilgi teknolojileri kullanılmaktadır. Böylece zaman maliyetine katlanılmadan kolaylıkla analiz yapılabilmektedir (Çalış vd., 2014, s.96).

Proaktif yaklaşımda uygulanabilecek yöntemler; (i) analitik inceleme teknikleri, (ii) istatistiki yöntemler, (iii) dijital analiz teknikleri: Benford Kanunu, (iv) bilgisayar destekli denetim teknikleri: sürekli denetim, (v) veri madenciliği analiz teknikleri, (vi) kurumsal yönetim ve (vii) adli muhasebe olarak sınıflandırılmaktadır.

#### **3.6.2.1 Analitik inceleme teknikleri (Mali analiz)**

Analitik inceleme teknikleri AICPA SAS No: 56 Md.2'de; *“hem finansal hem de finansal olmayan veriler arasındaki makul ilişkilerin incelenmesi yoluyla yapılan finansal bilgi değerlendirmeleri”* olarak tanımlanmıştır. Bu yöntemin temel prensibine göre; veriler arasında makul bir ilişki bulunmaktadır ve bilinen koşulların olmadığı durumda dahi, veriler arasındaki makul ilişki devam etmektedir. Diğer yandan veriler arasında makul bir ilişkinin bulunmaması halinde; bu durum, muhasebe değişikliklerinden, belirli olağandışı işlemler veya olaylardan, rastgele dalgalanmalardan, iş değişikliklerinden veya yanlış beyanlardan kaynaklanmaktadır. Dolayısıyla analitik inceleme teknikleri ile denetçi, işletme ve işletmenin faaliyet gösterdiği sektör hakkında sahip olduğu bilgiler ile elde ettiği analitik inceleme sonuçlarını karşılaştırarak verilerin makul olup olmadığı hakkında muhakemede bulunmaktadır (SAS No:56, Md.2-3).

Bir başka deyişle; bir hilenin gizlenmesi için manipüle edilen hesaplar, manipüle edilmeyen diğer hesaplarla olağandışı ilişkiler göstermektedir. Ayrıca hilekarın yakalanmamak için sadece ara sıra hile faaliyetlerinde bulunduğu dikkate alındığında, bu durum periyodik hesap bakiyelerinde düzensiz modeller de ortaya çıkarmaktadır. Dolayısıyla muhasebe hileleri, finansal tablo oranları ve eğilimlerini etkilediğinden, beklenmeyen mevcut ilişkiler veya mevcut olması beklenen ilişkilerin yokluğu mali analiz ile ortaya çıkarılabilmektedir (Bierstaker vd., 2006, s.523). Mevcut olması beklenen ilişkinin yokluğu da olası bir hile uyarısı olarak kabul edilmektedir (Onocak, 2022, s.218).

Nitekim 1990'lı yıllardan bu yana, gelişmiş ülkelerde etkili bir denetim yöntemi olarak mali analiz diğer bir adıyla analitik inceleme teknikleri kullanılmaktadır. Bu tekniklerin etkin kullanımı, denetçileri rutin işlemlerden kurtarmakta, denetimin kısa sürede ve düşük maliyetle gerçekleşmesini sağlamaktadır (Abdioğlu, 2007, s.128).

Literatüre ve denetim standartlarına göre; analitik inceleme, işletme verilerinin; (i) önceki yıllara ait benzer veriler, (ii) işletmenin bütçe ve tahminleri, (iii) denetçinin beklenti sonuçları, (iv) sektör verileri ve (v) finansal olmayan faaliyet verileri ile karşılaştırılması yollarıyla uygulanmaktadır. Bu karşılaştırmaların yapılabilmesi için çeşitli teknikler kullanılmaktadır. Bu teknikler aşağıda sıralanmıştır (Dönmez vd., 2011, s.123-126) :

- a. Oran (Dikey) Analizi
- b. Trend (Yatay) Analizi
- c. Karşılaştırmalı Tablolar Analizi
- d. Ussallık Testleri
- e. Regresyon Analizi
- f. Zaman Serisi Analizleri
- g. Benford Kanunu
- h. Yapay Sinir Ağları

Söz konusu analitik inceleme tekniklerinin uygulanması, gelişen teknoloji ve bilgisayar programları aracılığıyla oldukça kolay hale gelmektedir. Bu programlar ile işletme verilerine direkt bağlantı sağlanabilmekte, böylece daha etkin bir denetim sağlanarak hata ve hileler tespit edilip önlenabilmektedir.

### 3.6.2.2 İstatistiki yöntemler

Hile tespitinde; çoğunlukla tek bir tekniğin kullanılmasından ziyade, birden fazla tekniğin bir arada kullanılması gerekmektedir. Diğer yandan geleneksel yöntemlerle, milyonlarca işlemin arasından en küçük bir hileyi dahi tespit etmek kolay olmamaktadır. Bu nedenle veri toplama, analiz ve raporlama programları, hilelerin önlenmesi ve tespit edilmesinde önemli bir role sahiptir (Kandemir vd., 2012a, s.72).

Hile denetiminde uygulanan bütün proaktif yöntemler, istatistiksel yöntemlere dayanmaktadır ve hile denetiminde, regresyon analizi gibi basit istatistiksel yöntemlerin yanı sıra gelişmiş bilgisayar yazılımları da kullanılabilmektedir (Çalış vd., 2014, s.96).

Ayrıca akademik yazında, finansal bilgi manipülasyonundan şüphelenilen alanları, işletmelerin kamuya açıkladıkları finansal tablolar ve bilgiler üzerinden istatistiksel yöntemlerle test ederek, bu tür manipülasyonların mevcut olup olmadığı hakkında tahminler yapmak için istatistiki yöntemler sıklıkla kullanılmaktadır (Küçükkoçoğlu vd., 2005, s.165). Bu doğrultuda literatürde birçok model geliştirilmiştir. Tablo 3.9'da gösterilen bu modeller; yaklaşımları itibarıyla (i) tahakkuk esaslı, (ii) karma ve (iii) alternatif modeller olmak üzere üç kategoride sınıflandırılmaktadır.

**Tablo 3.9:** Finansal Bilgi Manipülasyonu Tespitinde Kullanılan İstatistiki Modeller.

| Tahakkuk Esaslı Modeller                                                                         | Karma Modeller                                                                                       | Alternatif Modeller                                                                                                |
|--------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| - Healy Modeli (1985)<br>- De Angelo Modeli (1986)<br>- Jones Modeli (1991)<br>- Endüstri Modeli | - Beneish Modeli (1999)<br>- Spathis Modeli (2002)<br>- Spathis, Doumpos ve Zopounidis Modeli (2004) | - Yapay Sinir Ağları<br>- Regresyon Modeli<br>- Karar Ağacı Modeli<br>- Genetik Algoritma<br>- Diskriminant Analiz |

**Kaynak :** [Güner vd., 2020, s.202]

Finansal bilgi manipülasyonunun işletmelerde çok yaygın bir şekilde uygulandığı düşüncesine rağmen bu durumun kanıtlanması oldukça zordur. Bunun sebebi manipülasyon öncesi işletmenin gerçekleşmesi gereken faaliyet sonuçlarının tahmin edilmesindeki güçlülüdür. Bu bağlamda araştırmacılar iki problem ile karşılaşmaktadırlar: (i) yöneticilerin, manipülasyonla ulaşmak istedikleri amaçları belirlemek ve (ii) yöneticilerin, muhasebe politikası seçimlerinin veya beklenmedik ihtiyari tahakkuk uygulamalarının etkilerini ölçmek (Küçüksözen, 2004, s.250). İkinci problemin çözümüne ilişkin yani beklenmedik tahakkuk uygulamalarının etkilerinin ölçülmesine yönelik geliştirilen modeller, “tahakkuk esaslı modeller” sınıflandırmasında yer almaktadır.

Literatürde ilk tahakkuk esaslı modeli geliştiren Healy (1985)'dir. Healy modelinde; cari dönemdeki ihtiyari tahakkukların, önceki yıla ait toplam tahakkukların bir bileşeni olduğu varsayılmaktadır. Bu varsayım altında ihtiyari tahakkukların, sıfır olması beklenmektedir. Eğer bir işletmenin ihtiyari tahakkukları sıfır değilse, bu durum işletmenin kar yönetimi stratejilerini uyguladığını göstermektedir. Yani ihtiyari tahakkuklar sıfırdan düşükse, işletme karlarını artırma yönünde; sıfırdan büyükse, karlarını düşürme yönünde manipülasyon yapıyor olduğu kabul edilmektedir (Aren, 2003, s.34).

Ardından Healy'nin tahakkuk modelini, DeAngelo (1986) ve Jones (1991) farklı araştırma alanlarında kullanarak, farklı hesaplama yöntemleri ile ölçerek geliştirmişler ve finansal bilgi manipülasyonu ölçüm araçları olarak literatüre kazandırmışlardır (Küçükkocaoğlu vd., 1997, s.4).

Karma modeller ise toplam tahakkukları içermekle birlikte, genellikle finansal bilgi manipülasyonlarında kullanılan muhasebe hesaplarını çeşitli finansal oranlara ve endekslere dönüştürerek manipülasyonların tespit edildiği modellerdir. Bu modellerde, tahakkuklardaki değişimleri tespit etmek için doğrusal regresyonlar kullanıldığı gibi, ilave olarak probit ve logit modelleri gibi farklı değişkenler içeren yöntemler de finansal bilgi manipülasyonu tespitlerinde kullanılmaktadır (Küçükkocaoğlu vd., 1997, s.6).

Karma modeller, Beneish (1997)'in yaklaşımı öncülüğünde gelişmiştir. Beneish modeli, finansal tablolardaki birtakım oranlar kullanılarak manipülasyon riskinin ölçüldüğü bir probit modeldir. Hem ihtiyari tahakkukları tespit etmek hem de kazanç yönetimini belirlemek için kullanılmaktadır. Bu modelde, manipülasyon yaptığı tespit edilen işletmelerin finansal tablo verileri ile kontrol firmalarının (diğer firmaların) bu verileri arasındaki sistematik benzerlikler incelenerek bulgular elde edilmektedir (Toplu vd., 2021, s.19). Model, çeşitli analiz oranları ile işletme verileri baz alınarak belirlenen sekiz değişkenden oluşmaktadır ve bunlara göre kazançların değişim derecelerini gösteren bir M-Skoru hesaplanmaktadır (Kıllı vd., 2017, s.74). M-skoru; her bir değişken için, manipülatör işletmeler ile kontrol işletmelerinin verilerinin probit analize tabi tutulmasıyla hesaplanan bir katsayıyı ifade etmektedir. İşletmenin manipülasyon yapıp yapmadığı ise bu M-skorunun 0 ile 1 arası aldığı değere göre belirlenmektedir. Buna göre, M değeri 1'a yakın ise işletmenin manipülasyon yaptığı; 0'a yakın ise manipülasyon yapmadığı şeklinde yorumlanmaktadır (Küçükkocaoğlu vd., 1997, s.7).



Daha sonra Beneish'in karma modelini, Spathis (2002) logit modeli ile yorumlamış ve bu model Spathis, Doumpos ve Zopounidis (2004) tarafından çok kriterli karar verme tekniği (UTADIS) kullanılarak genişletilmiştir (Toplu vd., 2021, s.19).

Son olarak alternatif modeller, finansal bilgi manipölasyonunu ortaya çıkarmaya yönelik olarak herhangi bir araştırmacı tarafından geliştirilmemiş olan ve bilgisayar teknolojilerindeki gelişmelerin bir sonucu olarak kullanılabilen ileri düzey istatistik ve analiz modelleridir (Toplu vd., 2021, s.20). Yapay sinir ağları, regresyon analizleri, karar ağacı modeli, diskriminat analizi ve genetik algoritma alternatif modellere örneklerdir.

### **3.6.2.3 Dijital analiz teknikleri : Benford Kanunu**

Benford Kanunu'nun temeli, fizikçi Simon Newcomb tarafından 1881 yılında yayınlanan "Note on the Frequency of Use of the Different Digits in Natural Numbers (Doğal Sayılarda Farklı Rakamların Kullanım Sıklığı Üzerine Not)" makalesinde bahsettiği, sayılar içindeki rakamların ortaya çıkma sıklıklarını hesapladığı teorisi ile atılmıştır. İlk olarak Newcomb'un ortaya koyduğu bu rakamların görülme sıklıkları, Frank Benford'un 1938 yılında yayınlanan "The Law of Anomalous Numbers (Anormal Sayılar Yasası)" isimli makalesinde daha kapsamlı veri kümeleri ile yapmış olduğu analizleriyle doğrulandığından bu kavram literatüre Benford Kanunu olarak geçmiştir (Çalış vd., 2014, s.97).

Newcomb'un yaşadığı dönemde hesap makineleri henüz icat edilmediğinden logaritmik tablolar aracılığıyla hesaplamalar yapılmaktaydı. Newcomb, logaritma tablolarının ilk sayfalarının son sayfalara göre daha yıpranmış, kirli ve sık kullanılmış olduğunu gözlemlemiştir. Buna göre "1" ile başlayan sayıların hesaplamalarda daha fazla yer aldığı sonucuna ulaşmıştır. Bu gözlemlerinden hareketle, sayıların ilk basamağındaki rakamların kullanım sıklığının eşit olmadığı ve küçük rakamlarla başlayan sayıların daha sık kullanıldığını ifade etmiştir (Newcomb, 1881, s.39-40; M55, Kaşıkçı vd., 2021, s.1198). Ancak Newcomb'un bu "kirli sayfalar" teorisi rastlantı olarak dikkate alınmış ve önemsenmemiştir. 57 yıl sonra Benford'un benzer gözlemi ile nüfus, nehir uzunlukları, elementlerin atomik ağırlıkları, gazete tirajları vb. gibi çok çeşitli farklı alanda yaptığı 20.229 adet veri üzerindeki analizi sonucunda bu teori, doğrulanarak tanınmıştır (Ertikin, 2017, s.86).

Benford (1938)'un analiz sonuçlarına göre; herhangi bir sayısal veri kümesinin ilk rakamının, 1'den 9'a kadar olan rakamlar içinden 1 olma olasılığı  $1/9$  olmamakta; %30,1 olmaktadır. Ve bu olasılık rakamlar büyüdükçe azalmaktadır. Ayrıca benzer şekilde, bir sayının ikinci basamağının 0'dan 9'a kadar rakamlar içinden gelme olasılığı da rakam büyüdükçe azalmaktadır. Buna göre Tablo 3.10'da 0-9 arası rakamların ilk ve ikinci basamaklarda ortaya çıkış frekansları bir diğer deyişle görülme sıklıkları verilmiştir.

**Tablo 3.10:** Benford Kanunu'na Göre Rakamların Görülme Sıklığı.

| Rakamlar                | 0     | 1     | 2     | 3     | 4     | 5    | 6    | 7    | 8    | 9    |
|-------------------------|-------|-------|-------|-------|-------|------|------|------|------|------|
| İlk Basamak Frekansı    | -     | 30.1% | 17.6% | 12.5% | 9.7%  | 7.9% | 6.7% | 5.8% | 5.1% | 4.6% |
| İkinci Basamak Frekansı | 12.0% | 11.4% | 10.8% | 10.4% | 10.0% | 9.7% | 9.3% | 9.0% | 8.8% | 8.5% |

**Kaynak :** [Benford, 1938, s.556]

Benford Kanunu'nun geçerliliği ise bazı koşulların varlığında mümkün olabilmektedir. Bu koşullar aşağıda sıralanmıştır (Abdioğlu, 2007, s.125-126; Ertikin, 2017, s.86-87):

- Veri kümesi büyüklüğü yeterli olmalı: Analizde kullanılan veri kümesi, en az dört basamaklı sayılardan oluşmalıdır. 10.000 ve üzerinde veri içeren çalışmalarda dağılım ortaya çıkmaktadır. Daha az basamaklı veri kümelerinde ise küçük rakamların ağırlığı artmaktadır.
- Veri kümesi, tesadüfi olmayan sayılardan oluşmalı: Veri kümesi, tam anlamıyla tesadüfi sayılardan oluşmamalıdır. Aksi durumda, her basamak için 0'dan 9'a rakamların görülme olasılığı eşit olacaktır.
- Veri kümesi, kodlanmamış sayılardan oluşmalı: Veri kümesindeki değerler, telefon numarası, posta kodu, sosyal güvenlik numaraları, kimlik numaraları vb. gibi atanmış sayılardan oluşmamalıdır. Bu sayılar tekdüze dağılıma sahip olduklarından rakamların görülme sıklıkları eşittir.
- Veri kümesinin, alt ve üst sınırları olmamalı: Veri kümesi, belirli limitler dahilinde kontrol edilmemelidir. Aksi durumda dağılım bozulacak ve sonuçların güvenilirliği etkilenecektir. Dolayısıyla şehirdeki petrol fiyatları gibi bir veri kümesi örneğinde Benford Kanunu geçersiz olacaktır.

- e. Veri kümesi, homojen değerlerden oluşmamalı: Veri kümesinde yer alan değerler, birbirine yakın olmamalıdır. Örneğin; 10 yaş grubundaki çocukların kilo ölçümlerine yönelik bir değer grubunun analizinde sayılar arasında belirgin bir fark olmayacağından Benford Kanunu geçerli olmayacaktır.
- f. Veri kümesindeki değerler aynı birim ile ifade edilmeli: Veri kümesindeki sayıların sıfır hariç belirli bir sayı ile çarpılması dağılımı etkilemez. Örneğin; dolar para birimi ile ifade edilen sayıların euro para birimine çevrilmesi analizi etkilemez. Ancak değerlerin bir kısmının dolar bir kısmının euro olarak analiz edilmesi Benford Kanunu'nu geçersiz kılmaktadır.

Benford Kanunu'nun finansal bilgi manipülasyonunun tespitinde kullanılmasına yönelik ilk öneri, Mark Nigrini tarafından 1992'de tamamladığı doktora çalışması ile getirilmiştir. Bu çalışmada, harcama ve satış kalemleri gibi muhasebe verilerinin Benford Kanunu'nun geçerliliğine uygun olduğu ve beklenen sıklık oranlarından sapmaların ölçülmesi ile muhasebe hilelerinin tespit edilebileceği ortaya konmuştur. Bu yaklaşım ile Benford Kanunu'nun ilk uygulaması yine Nigrini tarafından Brooklyn Gelir İdaresi'nde gerçekleştirilmiş, sonrasında Nigrini'nin geliştirmiş olduğu bilgisayar yazılımı ile yedi işletmede kullanılarak olumlu sonuçlar elde edilmiştir. Bu uygulama sonuçlarının makale olarak yayınlanmasının ardından Benford Kanunu'nun hile tespitinde kullanılması muhasebe ve denetim sektöründe benimsenmiştir (Çalış vd., 2014, s.97).

Benford Kanunu'na dayanan dijital analiz tekniğinde; rakamlar, sayıların belirli yerlerinde beklenen oranda görünüp görünmediklerine göre test edilmekte ve buna göre hileli işlemler tespit edilmektedir. Beklentilerden önemli bir sapma genellikle iki koşul altında ortaya çıkmaktadır. Birinci koşul, bir kişinin gözlemlerinin Benford dağılımına uymayan bir temelde eklenmiş olmasıdır. İkinci koşul ise bir kişinin Benford dağılımına uymayan bir veri setinden gözlemleri silmiş olmasıdır. Vergi dolandırıcıları, zimmetine para geçirenler ve çek kalpazanları bilinçli olarak rastgele sayılar üretmediklerinden dijital analiz yazılımları ile bu uygunsuzluk saptanabilmektedir (Bierstaker vd., 2006, s.526). Ancak bir işleme ilişkin analiz sonucunun Benford Kanunu'na uymaması, bu işlemin kesin olarak hileli olduğunu ortaya koymamakta, söz konusu işlemle ilgili detaylı inceleme başlatılması gerektiği anlamına gelmektedir (Mert vd., 2022, s.73).

Satış ve fiyat geçmişleri, satın alımlar, çek kayıtları, envanter birim maliyetleri, gelir/gider hesapları, havale bilgileri, sigorta poliçe değerleri, varlık/yükümlülük hesapları gibi veri setlerinde dijital analiz yazılımları kullanılarak hile tespiti yapılabilirken; banka hesapları, mükerrer adresler, sözleşmeye fesat karıştırma, kusurlu sevkiyat veya kusurlu teslimat şeklinde yapılan dolandırıcılıklar, Benford Kanunu veri kümesi koşullarına uymadığından ortaya çıkarılamamaktadır (Bierstaker vd., 2006, s.526).

#### **3.6.2.4 Bilgisayar destekli denetim teknikleri : Sürekli denetim**

Bilgisayar destekli denetim teknikleri (CAATs – Computer Assisted Audit Techniques); büyük miktarda verinin manuel olarak incelenmesinin imkânsız olduğu durumlarda, bilgisayar tabanlı teknolojiler kullanılarak bu verilerin analiz edilmesini sağlayan sistemlerdir (Murdock, 2016, s.24). Bir başka deyişle CAATs; denetim sürecinin etkinliğinin ve verimliliğinin artırılmasına yönelik manuel süreçlerin otomatikleştirilmesi, denetim alanının genişletilmesi ya da yeni denetim prosedürlerinin geliştirilmesi amacıyla kullanılan bilgisayar yazılımları ve uygulamalarıdır (Champlain, 2003, s.278). Bu bilgisayar yazılımları; özetleme, filtreleme ve katmanlaştırma gibi yöntemler ile hile belirteçlerinin tespit edilmesini sağlayan elektronik araç ve yöntemleri içeren paket programlardır (Ertikin, 2017, s.78).

Sürekli denetim ise fiziksel belge olmadan ve gerçek zamanlı muhasebe sistemleri kullanılarak hazırlanan mali tabloların doğruluğu hakkında makul görüş bildirmek amacı ile elektronik denetim kanıtlarını toplamak üzere uygulanan sistematik bir süreci ifade etmektedir (Rezaee vd., 2001, s.151). Dolayısıyla sürekli denetim sürecinde toplanan elektronik kanıtlar, bilgisayar destekli denetim teknikleri ve analitik denetim prosedürleri kullanılarak elde edilmektedir (Acar vd., 2016, s.1562).

AICPA ile CICA (The Canadian Institute of Chartered Accountants - Kanada Yeminli Mali Müşavirler Enstitüsü)'nin ortaklaşa hazırlamış oldukları “kırmızı kitap (red book)” olarak da adlandırılan raporda (1999) sürekli denetim; bağımsız denetçilerin, işletme yönetiminin sorumlu olduğu konular hakkında, ilgili olaylar gerçekleşir gerçekleşmez (eş zamanlı) veya kısa süre içinde düzenlenen raporlar aracılığıyla yazılı güvence sağlama yöntemi olarak tanımlanmıştır (AICPA, 2015, s.3-4).

Dolayısıyla sürekli denetim ile, işletme içindeki kontrol çerçevesi güçlendirilerek hatalı ve hileli işlemler en kısa sürede ortaya çıkarılmakta ve önlenmektedir. Herhangi bir önemli sorun hakkında, üst yönetim ve denetçiler eşanlı olarak bilgi edinebilmektedirler. Bu yöntem ile, riskli alanlar erken tespit edilmekte ve risk yönetim stratejilerinin etkinliği değerlendirilerek gerekli önlemlerin zamanında alınması sağlanmaktadır (Abdioğlu, 2007, s.130-131).

Sürekli denetim, iki ana bileşene sahiptir: (i) sürekli kontrol değerlendirmesi (continuous control assessment) ve (ii) sürekli risk değerlendirmesi (continuous risk assessment). Sürekli kontrol değerlendirmesi, kontrol zayıflıklarını hızlıca tespit ederek iç denetçilerin yönetimin izleme işlevinin etkinliğini belirlemesini sağlamaktadır. Ayrıca yönetim ile denetim kurullarına kontrollerin etkinliği ve olumsuzlukların düzeltilmesi hakkında garanti vermektedir. Sürekli risk değerlendirmesi ise risk düzeyinin yüksek olduğu sistem ve süreçleri belirleyerek riskleri derecelendirmekte ve sınırlı denetim kaynaklarının daha etkin kullanılmasını sağlamaktadır. Böylece işletmenin potansiyel sorunları hızlıca tespit edilmekte ve düzeltilmektedir (Mert vd., 2022, s.74).

1990'ların başında AT&T, HCA Inc., Siemens, New York Federal Reserve, Unibanco ve IBM'de ilk kez uygulanan sürekli denetim çalışmalarında denetim kanıtları, geleneksel örneklem yönteminin aksine gerçek zamanlı tüm işletme verileri ile gerçekleştirilmektedir. Bu şekilde işletmelerin "gerçek dünyasına" erişilebildiğinden sadece potansiyel riskler değil aynı zamanda gerçekleşmiş risklerin matematiksel boyutu da tespit edilerek sorunlu alanlar çözümlenebilmekte ve gelecek bugünden denetlenebilmektedir (Sevimli, 2010, s.30).

Yaşanan Enron muhasebe skandalı sonucu 2002 yılında yürürlüğe giren Sarbanes Oxley Yasası ile birlikte bilgi teknolojilerindeki gelişim ve elektronik veri miktarındaki artışın etkisiyle, sürekli denetim giderek daha önemli bir hale gelmekte ve bu durum, denetim süreçlerinin daha dinamik ve teknoloji odaklı bir şekle evrilmesini zorunlu kılmaktadır. Buradan hareketle geleneksel denetim sürecinin değişimi, sürekli denetim ile karşılaştırılarak Tablo 3.11 ve Tablo 3.12'de özetlenerek ortaya konulmuştur.

**Tablo 3.11:** Geleneksel ve Sürekli Denetimin Karşılaştırılması- 1.

|                | <b>Sürekli Denetim</b>                 | <b>Geleneksel Denetim</b>                         |
|----------------|----------------------------------------|---------------------------------------------------|
| Denetim Alanı  | Tüm Kayıtlar                           | Örnekleme ile seçilen sınırlı sayıdaki kayıtlar   |
| Denetim Zamanı | Sürekli (Eş zamanlı)                   | Belirli dönemlerde                                |
| Denetim Verisi | Elektronik ortamdaki kayıt ve belgeler | Elektronik ve kâğıt ortamındaki kayıt ve belgeler |
| Denetimi Yapan | CAATs                                  | Denetçi                                           |

**Kaynak :** [Ertikin, 2017, s.85]

**Tablo 3.12:** Geleneksel ve Sürekli Denetimin Karşılaştırılması– 2.

|   | <b>Geleneksel Denetim Aşamaları</b> | <b>Sürekli Denetim Aşamaları</b>              |
|---|-------------------------------------|-----------------------------------------------|
| 1 | Denetim anlaşması                   | Sürekli izleme ve sürekli kontrol mimarisi    |
| 2 | Denetim planı                       | Analitik izlemenin yapılandırılması           |
| 3 | İç kontrol sistemi değerlemesi      | Uyumsuz noktaların gözlemlenmesi              |
| 4 | Maddi doğruluk testleri             | Sürekli olarak model oluşturma ve birleştirme |
| 5 | Denetçi görüşü                      | Alarmlar ve bilgilendirme                     |
| 6 | Raporlama                           | Uyumsuzluğun incelenmesi                      |
| 7 |                                     | Çok katmanlı görüş                            |

**Kaynak :** [Usul, 2013, s.19]

### 3.6.2.5 Veri madenciliği analiz teknikleri

Bilgisayarlaşma ve güçlü veri toplama ve depolama araçlarının gelişimi, hızla büyüyen, geniş çapta erişilebilir olan ve devasa hacimlere ulaşan bir veri yığını yaratmaktadır. Karar almada kullanılan değerli bilgi ise bu veri yığını içinde gömülü bulunmakta ve ortaya çıkarılması gerekmektedir. Ancak büyük miktardaki verinin, bilgi ve enformasyona dönüştürülmesi; insanoğlunun kavrama yeteneğini aşmakta ve manuel becerileri ile maliyetli, zaman alıcı ve hataya açık hale gelmektedir. Bu nedenle veri yığını içinden değerli bilgileri otomatik olarak ortaya çıkarabilecek yardımcı araçlara ve yeni tekniklere ihtiyaç duyulmaktadır. Bu gereklilik veri madenciliğinin doğmasına ve gelişmesine yol açmıştır (Han vd., 2012, s.1-5).

Veri madenciliği, “büyük miktarlardaki verilerden ilginç örüntüler keşfetme sürecidir. Bir bilgi keşif süreci olarak, tipik olarak veri temizleme, veri entegrasyonu, veri seçimi, veri dönüşümü, örüntü keşfi, örüntü değerlendirme ve bilgi sunumu adımlarını içermektedir”

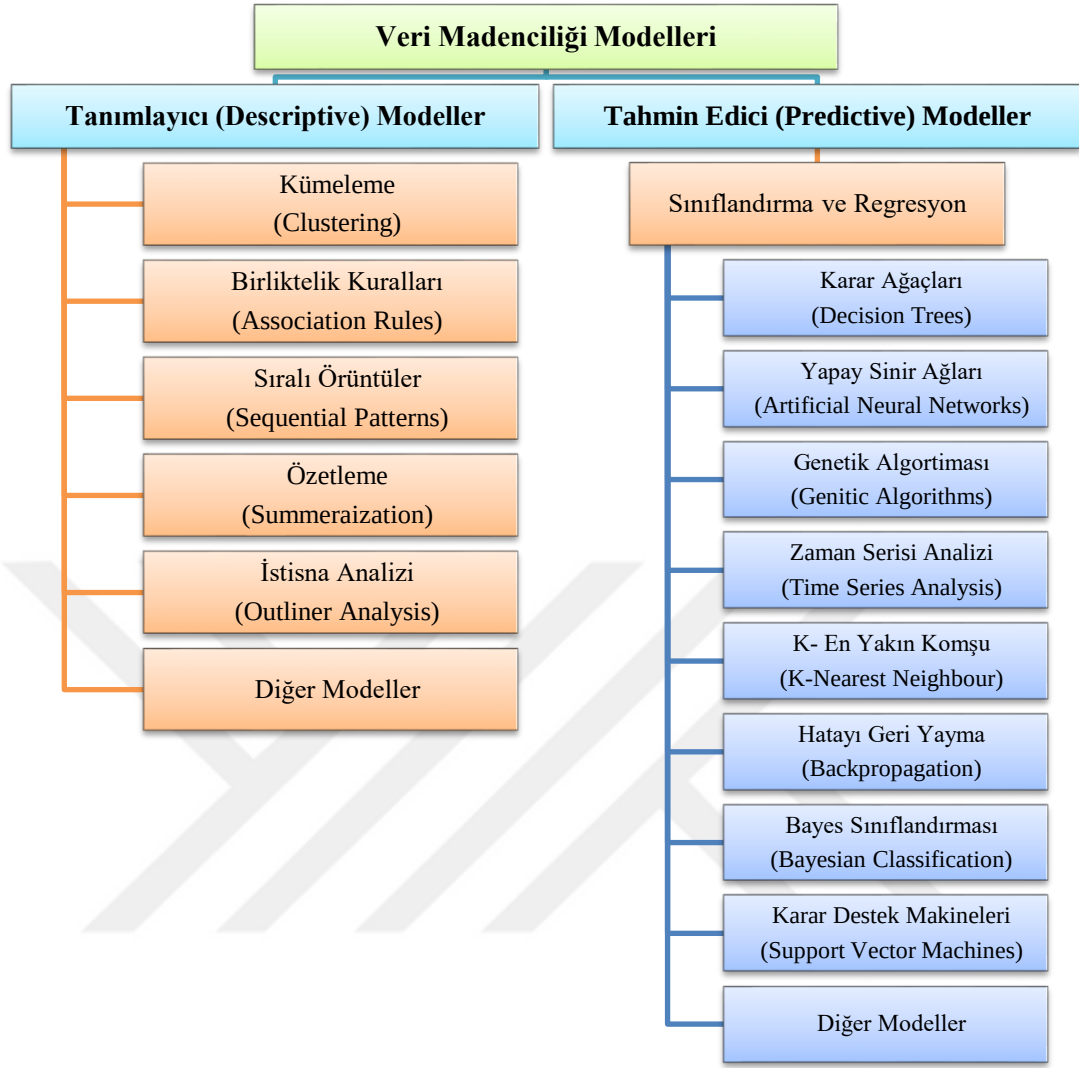
(Han vd., 2012, s.33). Dolayısıyla tek başına bir çözüm sağlamayan, ancak çözüme ulaşmak için gerekli bilgileri sunarak karar verme sürecini destekleyen bir araçtır (Özmen, 2001, s.2)

Veri madenciliği; veri yığınları içindeki örüntüleri keşfetmek için makine öğrenimi (machine learning), istatistik, veri tabanı teknolojisi, yapay zekâ (AI- artificial intelligence), veri görselleştirmesi (data visualization) ve örüntü tanımlama (pattem recognition) vb. gibi birçok teknolojiden faydalanan, çok sayıda disiplini bir araya getiren bir alandır. Tıptan finansa, pazarlamaya, astronomiye, biyolojiye kadar pek çok dalda veri madenciliği uygulanma fırsatı bulunmaktadır (Özekes, 2003, s.66). Finansa risk analizlerinin yapılmasında veya tıpta sağlık taraması ile bulgulara ulaşılmasında kullanıldığı gibi muhasebe hilelerinin tespiti için delil elde etmede de veri madenciliği kullanılabilmektedir (Kiracı, 2005, s.111).

Veri madenciliği, Şekil 3.4'te gösterildiği üzere tanımlayıcı (descriptive) ve tahmin edici (predictive) olmak üzere iki ana model altında kullanılmaktadır. *Tanımlayıcı modellerde*, karar verme sürecine yardımcı olmak için kullanılacak mevcut verilere ait örüntüler belirlenmektedir. *Tahmin edici modellerde* ise sonuçları bilinen verilere dayalı olarak bir model oluşturulmakta ve bu model kullanılarak sonuçları bilinmeyen veri kümelerinin sonuçları tahmin edilmeye çalışılmaktadır (Özekes, 2003, s.67).

Veri madenciliği modelleri işlevlerine göre; (i) sınıflama (classification) ve regresyon (regression), (ii) kümeleme (clustering), (iii) birliktelik kuralları (association rules) ve (iv) sıralı örüntüler (sequential patterns) olmak üzere dört temel gruba ayrılmaktadır. Sınıflama ve regresyon, tahmin edici modeller altında; kümeleme, birliktelik kuralları ve sıralı örüntü, tanımlayıcı modeller altında sınıflandırılmaktadır (Albayrak vd., 2009, s.33).

Şekil 3.4'te de görüldüğü üzere çeşitli amaçlara yönelik farklı veri madenciliği yöntemleri kullanılabilmektedir. Ancak finansal bilgi manipülasyonu tespitine yönelik en sık kullanılan yöntemler karar ağaçları ve yapay sinir ağlarıdır (Onocak, 2022, s.224). Bu nedenle çalışma kapsamında yalnızca bu iki yöntem aşağıda kısaca açıklanmıştır.



**Şekil 3.4:** Veri Madenciliği Modelleri.

[Alagöz vd., 2014, s.8]

### ***Karar ağaçları***

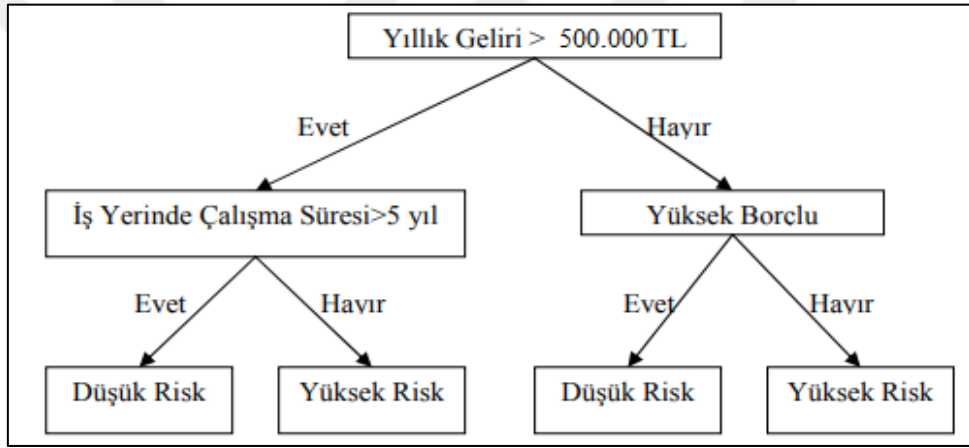
Karar ağaçları, tümevarım yöntemi kullanılarak verileri sınıflandıran ve ağaç yapısı görseline sahip bir akış diyagramıdır. Bu yapı sayesinde, büyük veri kümeleri belirli özelliklere göre küçük parçalara bölünerek gruplandırılabilmekte ve böylece verilerin, daha anlaşılır ve yorumlanabilir hale gelmesi sağlanabilmektedir (Onocak, 2022, s.225).

Karar ağaçları, karar noktalarını temsil eden düğümler ve ilgili düğümleri birbirlerine bağlayan dallardan meydana gelmektedir. Kök düğümden başlayarak dallanan ve her dallanma noktasında çeşitli özelliklerin test edildiği bir model yapısına sahiptir. En alta, test



edilen özelliklerin sonuçlarına göre daha fazla dallanmayan yaprak düğümleri bulunmaktadır (Alagöz vd., 2014, s.9).

Karar ağacının, herhangi bir problemin çözümüne yönelik uygulanabilirliği ve sonuçlarının anlaşılabilirliği kolaydır; bu nedenle yaygın olarak kullanılmaktadır. Ayrıca verilere ilişkin varsayımlarda bulunulmasına gerek olmaması da bir diğer avantajıdır. Diğer yandan verilerdeki küçük değişimlerin, kural setinde veya karar ağacının yapısında büyük değişikliklere yol açması sonuçların stabil olmamasına sebep olmakta, bu durum da yöntemin dezavantajı olarak kendini göstermektedir (Alkan, 2007, s.21). Yöntemin daha iyi anlaşılması için hile tespitine yönelik kanıt toplamda uygulanan basit bir karar ağacı yapısı Şekil 3.5’te gösterilmiştir.



Şekil 3.5: Hile Tespitinde Karar Ağacı Uygulama Örneği.

[Alkan, 2007, s.21]

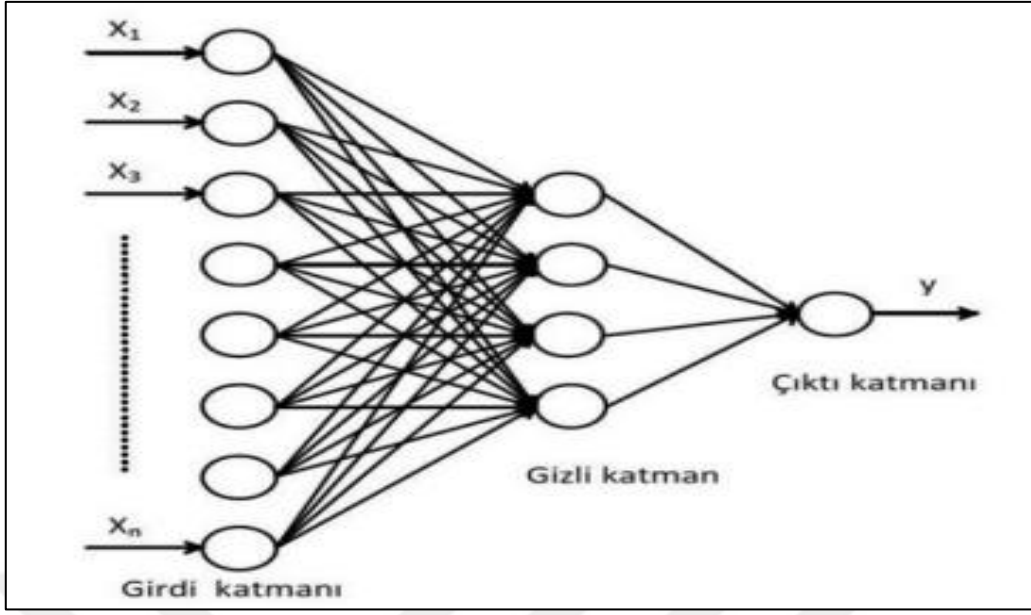
### ***Yapay sinir ağları***

1990’larda bilgisayar teknolojisinin hızlı gelişimine rağmen insanların kolaylıkla gerçekleştirebildiği el yazısı tanıma, görme ve konuşma gibi görevlerin otomatik olarak yapılmasına yönelik hala eksiklikler bulunmaktaydı. Bu eksiklikler, bilim insanlarını geleneksel bilgisayarlardan farklı bilgi işleme sistemleri geliştirmeye yöneltmiştir. İlk adımlardan biri olarak, insan beyninin sinir ağlarının yapısal ve işlevsel özelliklerini matematiksel olarak modellemeye yönelik çalışmalar yapılmıştır. Bu matematiksel modeller “sinir ağları” olarak bilinmektedir (Küçükkocaoğlu vd., 1997, s.10).

Yapay sinir ağı, yeni bilgileri otomatik olarak oluşturma ve keşfetme yeteneğine sahip bilgisayar sistemleri olarak geliştirilmişlerdir (Terzi vd., 2015, s.483). Yapay sinir ağı, belirli bir amaca hizmet etmeye yönelik oluşturulan ve insanlara benzer şekilde örnekler üzerinden öğrenen bir yapay zekâ teknolojisidir. Tekrarlanan girdilerle, kendi ağırlığını ve yapısını değiştirmektedir. Canlıların sinir sisteminin bir benzeri şekilde adaptasyon yeteneğine sahip bulunmaktadır (Ertikin, 2017, s.83). Çok sayıda değişkenin varlığı halinde ve bu değişkenlerin birbirleriyle karşılıklı karmaşık etkileşimlerde bulunduğu ya da belirli bir çözüm kümesinin olmadığı durumlarda, başarılı sonuçlar veren bir teknolojidir (Küçükkocaoğlu vd., 1997, s.10). Hatalı veriler ile çalışıp çözüm üretebilirler ancak elde ettikleri sonuçların nedenlerini açıklayamazlar. Diğer yandan ezbere hareket edebilmeleri mümkün olduğundan optimum sonuca ulaşamayabilirler bu nedenle uygun testler ile sağlamaları yapılmalıdır (Alkan, 2007, s.15).

Yapay sinir ağı, öncelikle bilgisayar programları kullanılarak verilerle eğitilmektedir. Eğitim ile veriler arasındaki ilişkileri öğrendikten, verileri işledikten ve çözümledikten sonra, karar vermesi istenilen konu hakkındaki veriler ağa girilerek yapay sinir ağının karar vermesi istenmektedir (Kiracı, 2005, s.111). Gerçek sonuçlar ile yapay sinir ağının elde ettiği sonuçlar karşılaştırılarak model iyileştirilmektedir. Karşılaştırma sonuçları en az hata düzeyine ulaştığında ise model geliştirme süreci tamamlanmaktadır (Alagöz vd., 2014, s.9).

Yapay sinir ağı; Şekil 3.6'da gösterildiği üzere üç katmanlı bir modelden oluşmaktadır: (i) girdi katmanı, (ii) gizli katman ve (iii) çıktı katmanı. Girdi katmanında, veriler sürece dahil edilmekte; gizli katmanda, veriler işlenmekte ve çıktı katmanında ise veriler bilgiye dönüşmektedir (Onocak, 2022, s.224). İstatistiksel açıdan bakıldığında girdi katmanındaki veriler, bağımsız değişkenleri; çıktı katmanındaki veriler ise bağımlı değişkenleri ifade etmektedir. Gizli katman da bu iki katman arasında yer almakta ve dış ortamla bağlantısı olmayan sinirler aracılığıyla girdi katmanından gelen sinyalleri çıktı katmanına iletmektedir. Bu gizli katmandaki sinir sayısı ağın büyüklüğü ve performansını belirlemektedir. Ne kadar çok gizli sinir (nöron) var ise ağ o kadar karmaşık bir yapıya sahip olmaktadır (Küçükkocaoğlu vd., 1997, s.11).



Şekil 3.6: Yapay Sinir Ağlarının Modellemesi.

[Onocak, 2022, s.224]

Hile denetiminde veri madenciliği analiz tekniklerinin kullanılması durumunda ise şirketlerdeki anormal durumların ve hile belirtilerinin tespit edilmesi amacıyla işlemlere dair veriler çıkarılarak analiz edilmesi sağlanmaktadır (Mert vd., 2022, s.71). Yüksek miktarda verinin analizi, eğilimlerin belirlenmesi ve araştırılması gerekli belgelerin tespit edilmesi konularında hızlı ve kapsamlı inceleme sağlamaktadır. Ayrıca belgeler eksik olduğunda mantıksal ilişkileri anlamaya yardımcı olmakta ve bulguları açık bir şekilde özetlemektedir. Ancak veri madenciliği ile denetim veya inceleme sürecinin tamamının gerçekleştirildiği düşünülmemelidir. Denetçinin gözlem ve deneyiminin yerine geçmeyen analiz sonuçları yalnızca sürecin bir parçası olarak kullanılmaktadır (Kandemir vd., 2012b, s.61).

Ayrıca yapay zekâ teknolojisi kapsamında; yapay sinir ağlarının dışında uzman sistemler, bulanık mantık, robotik teknoloji, genetik algoritma, bilgiye dayalı sistem, doğal dil işleme vb. gibi teknolojiler de hile tespitinde kullanılmaktadır (Özçetin, 2022, s.35).

### 3.6.2.6 Kurumsal yönetim (Corporate governance)

Kurumsal yönetim olarak da adlandırılan “kurumsal yönetim” kavramının, literatürde yaygın olarak kabul edilen tek bir tanımı bulunmamakla birlikte; nerede, hangi amaçla ve kim tarafından kullanıldığına ya da kurumsal yönetime ilişkin ilkelerin yayımlandığı kuruluşlara göre farklı tanımlamaları bulunmaktadır (Alp vd., 2014, s.23).

Kurumsal yönetim ile ilgili modern anlamdaki en eski çalışma, Birleşik Krallık'ta Sir Adrian Cudbury başkanlığındaki Cadbury Komitesi'nin 1992 yılında hazırlamış olduğu Cadbury Raporu'dur. Söz konusu rapora göre kurumsal yönetim, *“şirketlerin yönetildiği ve kontrol edildiği sistem”* olarak tanımlanırken; yönetim kurulunun görevinin, şirketi yönetmek ve ortaklara uygulamaları hakkında rapor sunmak olduğu, işletme ortaklarının görevinin ise uygun yönetim yapısının oluşturulması amacıyla yönetim kurulu üyeleri ile denetim komitesi üyelerini seçmek olduğu ifade edilmektedir. Dolayısıyla bu dar kapsamda kurumsal yönetim tanımı ile halka açık şirketlerde karşılaşılan vekalet sorununun (agency problem) çözümüne yönelik şirket hissedarlarının haklarına odaklanılmaktadır. Bununla birlikte kurumsal yönetim kavramının sadece hissedarların haklarına yönelik değil aynı zamanda diğer paydaşların ve toplumun haklarına yönelik hem aile şirketlerinde hem de kamuda uygulanabilirliğine ilişkin görüşler neticesinde, Cadbury Komitesi 1999 yılında kurumsal yönetim tanımının kapsamını genişleterek güncellemiştir (Alp vd., 2014, s.24).

Kurumsal yönetim kavramı ile ilgili bir diğer önemli çalışma, OECD tarafından 1999 yılında yayınlanan *“Kurumsal Yönetim İlkeleri”*dir. Söz konusu ilkelere göre kurumsal yönetim; *“bir şirketin yönetimi, yönetim kurulu, hissedarları ve diğer paydaşlar arasındaki bir dizi ilişkiyi kapsar. Kurumsal yönetim aynı zamanda şirketin hedeflerinin belirlendiği bir yapıyı ortaya koymakta ve bu hedeflere nasıl ulaşılacağı ve performansın nasıl denetleneceğinin yollarını çizmektedir. İyi kurumsal yönetim, yönetim kurulları ve üst yönetim için şirketin ve hissedarlarının çıkarları doğrultusunda hedeflere yönelme açısından uygun teşvikleri sağlamalı ve etkin denetimi kolaylaştırmalıdır.”* ifadeleri ile açıklanmaktadır (OECD, 2004).

Literatürdeki mevcut kurumsal yönetim tanımları, kavrama farklı açılardan yaklaşmakta ve diğer yönlerini ihmal etmektedir. Bu bağlamda kurumsal yönetim kavramı Alp ve Kılıç (2014) tarafından tüm yönleri ile dikkate alınarak: *“Sürdürülebilir bir şekilde değer yaratma ve uzun vadede şirketin sürekliliğini sağlama amaçları doğrultusunda şirket faaliyetleri yürütülürken; yönetim kurulu, üst yönetim, hissedarlar ve diğer paydaşlarla olan ilişkilerin, bunların rol ve sorumluluklarının şeffaflık, adillik, hesap verebilirlik ve sorumluluk ilkeleri esas alınarak en uygun şekilde tasarlandığı, yönetim ve denetim fonksiyonlarının birbirinden ayrıldığı, hissedarların çıkarları korunurken diğer ilgili paydaşların hak ve menfaatlerine de saygı gösterildiği, iyi şirket yönetimi biçimidir.”* şeklinde geniş kapsamda tanımlanmaktadır (Alp vd., 2014, s.37).

Bu tanımdan hareketle etkili kurumsal yönetim ile hesap verebilirlik ve değer yaratma arasındaki güçlü ilişki dolayısıyla kurumsal yönetim ilkelerine uygun faaliyet gösteren işletmeler, daha nitelikli yönetim ve güçlü kontrol sayesinde daha yüksek mali performans elde etmektedirler (Kandemir vd., 2012b, s.59). Etkin bir kurumsal yönetim uygulaması, üst yönetimin, yönetim kuruluna; yönetim kurulunun ise hissedarlara hesap verdiği, bununla birlikte işletmenin, çalışanlara, ortaklara, müşterilere ve bankalara yönelik eylemlerinin de yönetim-denetim süreci kapsamında değerlendirildiği bir sisteme dayanmaktadır (Alp vd., 2014, s.26). Bu şekilde şirketin değeri artırılırken, yöneticilerin, yönetim kurulu üyelerinin ve yatırımcıların menfaatleri uyumlu hale getirilmekte ve sonuç olarak kurumsal yönetim ile yatırımcıların çıkarlarını korumak ve onlara hizmet etmek amacıyla yönetim kurulu, denetim komitesi, yönetim ve denetçiler aracılığıyla işletmelerde hesap verebilirlik ve sorumluluk mekanizmaları işler hale getirilmektedir. Böylece kurumsal yönetim ile denetimden geçirilerek önemli hata, hile ve usulsüzlüklerden arındırılmış finansal raporlama süreci sağlanarak finansal bilgi manipülasyonları azaltılmakta ve şeffaflaştırılan finansal raporlama süreci sayesinde ortakların ve paydaşların işletme faaliyetlerine ve sonuçlarına duydukları güven artırılmaktadır (Kandemir vd., 2012b, s.59).

### **3.6.2.7 Adli muhasebe (Forensic accounting)**

Adli muhasebe kavramı ilk kez, Maurice E. Peloubet tarafından 1946 yılında yayınlanan "Forensic Accounting: Its Place in Today's Economy (Adli Muhasebe: Günümüz Ekonomisindeki Yeri)" adlı makalesinde kullanılmıştır (Enofe vd., 2013, s.62). Türkçe'ye "adli" olarak çevrilen "forensic" kelimesi "*mahkemede kullanılmaya uygun olan*" anlamına gelmektedir. Bu kelime; bilimsel bilgi ve yöntemlerin, hukuki sorunlar ve cezai soruşturmalar için uygulanmasını ifade eden teknik bir terim olarak kullanılmakta ve adli mühendislik, adli tıp gibi çeşitli alanlarda örnekleri bulunmaktadır. Bu bağlamda adli muhasebe sürecinde; muhasebe kavram ve teknikleri, dolandırıcılık soruşturmaları, davaları ve sigorta talepleri gibi belirli uyuşmazlık türlerinde uygulanarak finansal dolandırıcılık araştırılmakta ve ilgili konularda avukatlara davalarında destek verilmektedir (AICPA, 2014, s.15). Dolayısıyla adli muhasebe; muhasebenin, gerçek veya beklenen anlaşmazlıklar ve davalardan kaynaklanan görevlerini tanımlayan bir uzmanlık alanını ifade etmektedir (Bhasin, 2007, s.1000).

Muhasebe, denetim, hukuk, kriminoloji, grafoloji, psikoloji gibi disiplinleri birleştiren (Çekmen, 2022, s.65) adli muhasebe; soruşturma, muhasebe ve denetim becerilerinin entegrasyonunu gerektiren yasal sorunları çözmek için denetim yöntemleri, teknikleri ve prosedürleri aracılığıyla toplanan muhasebe gerçeklerinin ve kavramlarının uygulanmasıyla ilgilenen bir bilim dalıdır (Enofe vd., 2013, s.62).

Adli muhasebe uygulamalarını ifa eden meslek mensuplarına ise “adli muhasebeci (forensic accountant)” denilmektedir. Adli muhasebecilik mesleği, 1988 yılında ACFE’nin kuruluşu ile örgütlenmiştir (Çankaya vd., 2009, s.95). Bu meslek, adli sorunların çözümü ve hile denetimi alanlarında mesleki bilgi ve tecrübeye sahip kişilere, merkezi Amerika’da bulunan ACFE tarafından verilen “CFE (Certified Fraud Examiner / Suistimal İnceleme Uzmanlığı - SİU)” ünvanı ile ifa edilmektedir (USUID, [https://acfetr.com/index.php?pg=sertifika\\_main](https://acfetr.com/index.php?pg=sertifika_main)).

Adli muhasebecilik uygulamaları; (i) dava destek danışmanlığı, (ii) uzman şahitliği ve (iii) hile denetçiliği (fraud audit) veya araştırmacı muhasebecilik (fraud investigation) faaliyetlerini kapsamaktadır (Rezaee vd., 1992, s.33 Akt. Bozkurt, 2000b, s.57). Dava destek danışmanlığı; adli muhasebecilerin, dava öncesinde ve dava sürecinde avukatlara, ihtiyaç duyulan verilerin ortaya konması ve toplanan verilerin analiz edilmesi şekillerinde sunmuş oldukları hizmetlerdir. Verilerin ortaya konulmasında, avukatların yasal işlemler için ihtiyaç duyduğu bilgilerin doğruluğu ve geçerliliği sağlanmakta; analiz sürecinde ise mali veriler değerlendirilmekte ve avukatların bu bulguları yasal bağlamda yorumlamalarına yardımcı olunmaktadır. Uzman şahitliği; adli muhasebecilerin gerek rapor düzenleyerek gerek doğrudan şahitlik yaparak davalarda bilirkişi olarak hizmet vermeleridir (Bozkurt, 2000, s.57). Hile denetçiliği ise hileyi ortaya çıkarmak için özel bir yaklaşım ve metodoloji kullanarak hile kanıtı arama faaliyetleridir (Singleton vd., 2010, s.12).

Adli muhasebecilik faaliyetlerinin kapsamı neticesinde literatürde adli muhasebecilik ile hile denetçiliği birbiri yerine kullanılıyor olsa da aralarında farklılıklar bulunmaktadır. Hile denetçiliği adli muhasebeciliğin bir parçasıdır. Hile denetiminde amaç, bir hilenin varlığını kanıtlamak ya da çürütmektir, yani hile belirtisi veya şüphesinden önce uygulanan faaliyetlerdir. Ancak adli muhasebeciler, bir iddia, şikâyet veya keşif yoluyla suistimal kanıtının veya şüphesinin ortaya çıkmasından sonra görev almaktadırlar. Diğer yandan adli

muhasebecilik, bir hile ile ilgili tüm taraflarla yapılan görüşmeler gibi finansal olmayan bilgilerin toplanması faaliyetlerini de içermektedir (Singleton vd., 2010, s.12).

Adli muhasebecilik adı altında hata ve hileleri ortaya çıkaracak uzman ihtiyacı; yaşanan işletme skandalları, ticari işlemlerin karmaşılaşması, artan mahkeme başvuruları, teknolojiyle hilelerin tespitinin zorlaşması (Bozkurt, 2000b, s.56), artan etik dışı davranışlar, muhasebe öğretisinin ve hukuk eğitiminde verilen finansal bilgilerin yetersizliği ve bilirkışılık sistemindeki eksiklikler (Usul vd., 2011, s.57-61) sonucu ortaya çıkmıştır. Diğer yandan denetim ve kontrol faaliyetlerinin hileleri tespit etme konusunda yetersiz kalması da sadece hileleri ortaya çıkarmak için araştırma, soruşturma ve denetim yapan, suçlular gibi düşünme, sezgi ve yaratıcılık yeteneklerine sahip kişilerden oluşan adli muhasebecilik mesleğinin gelişimine ön ayak olmuştur (Kandemir vd., 2012b, s.40).

Muhasebe denetimlerinin, hile tespiti ve önlemede yetersiz kalmasının sebebi ise iç ve dış denetimlerin kapsamı ve denetçilerin özelliklerinden kaynaklanmaktadır. Muhasebe hileleri, özel uzmanlık gerektiren bir alan olduğundan sadece hile denetimi konusunda uzmanlaşmış denetçiler tarafından ele alınmalıdır (Yaylalı, 2024, s.111). Bu kapsamda hile denetimi, hileli işlemleri ortaya çıkarmak ve soruşturmak için şüpheli işlemleri, belge inceleme, mülakatlar ve dış veriler yoluyla araştırırken; bağımsız denetim finansal tabloların muhasebe ilkelerine uygunluğunu denetlemektedir. Bağımsız denetçiler, hile tespiti konusunda eğitim almadıkları ve sadece finansal tabloların doğruluğu hakkında makul güvence verdikleri için hilelerin tespiti konusunda yetersiz kalabilmektedirler (Yaylalı, 2024, s.122). Dolayısıyla adli muhasebecilerin yaptığı hile denetimi, iç ve dış muhasebe denetimlerinin yerini almayan, onları tamamlayarak hile tespit ve önlenmesine yönelik etkili bir yaklaşım olarak kullanılmaktadır (Kandemir vd., 2012b, s.45).

#### **4. BLOKZİNCİR TEKNOLOJİSİNİN FİNANSAL BİLGİ MANİPÜLASYONUNU AZALTMADA KULLANILMASI**

Dijitalleşme, muhasebe ve denetim sektörlerinde iş süreçlerini otomatikleştirerek veri yönetimini hızlandırmıştır. Ancak muhasebe bilgi sisteminin güvenliği ve şeffaflığı, giderek daha büyük bir önem kazanmıştır. 2000'li yılların başında yaşanan Enron, WorldCom, Global Crossing, Tyco ve Parmalat gibi büyük finansal skandallar, muhasebe manipülasyonunun mali ve toplumsal etkilerini gözler önüne sermiş ve mevcut denetim sistemlerinin yetersizliğini ortaya koymuştur. 2008 küresel finans krizi ise bu eksiklikleri daha da vurgulamakla kalmamış, finansal piyasalara ve aracılara olan güvenin de kaybolmasına yol açarak, tüm sistem işleyişinin sorgulanmasına ve güvenilir ve şeffaf bir sistem ihtiyacının derinleşmesine neden olmuştur. Böyle bir ortamda, blokzincir teknolojisi alternatif bir sistem çözümü olarak ortaya çıkmıştır. İlk bölümde detaylı bir şekilde anlatıldığı üzere blokzincir, verilerin değiştirilemez ve şeffaf bir şekilde kaydedilmesini sağlayarak, muhasebe ve denetim süreçlerinin güvenilirliğini artırma potansiyeline sahiptir. Bu teknolojinin, gelecekteki finansal skandalları önlemeye yönelik güçlü bir savunma hattı sunarak, küresel mali istikrarı desteklemesi beklenmektedir.

Önceki bölümde, finansal bilgi manipülasyonlarının tespiti ve önlenmesinde kullanılan reaktif ve proaktif yöntemler tanımlanmıştır. Söz konusu yöntemler, manipülasyon tespitinin doğruluğunu önemli ölçüde artırmakta, ancak çok az model tüm suistimal senaryolarında mükemmel tespit performansını sağlayabilmektedir. Diğer yandan hileli işlemler başarılı bir şekilde yakalansa bile, gerçeğe ulaşma ve doğru karar verme çoğu zaman gerçekleşmemektedir (Cai vd., 2016, s.2).

Literatürde finansal bilgi manipülasyonunu tespit ve önlemeye yönelik olarak çok çeşitli teknolojik tabanlı yöntem araştırmacılar tarafından uygulanıyor ve test ediliyor olmasına rağmen yapılan araştırmalar, suistimal tespitinde en yaygın kullanılan yöntemin “ihbar” (Tablo 3.6) olduğunu göstermektedir (KPMG, 2020; ACFE, 2024). Dolayısıyla günümüzde çoğunlukla suistimaller hala reaktif yöntemlerle yani hile gerçekleştikten, zarar meydana geldikten sonra tespit edilebilmektedir. Suistimallerin küresel düzeyde toplam maliyetinin, 5 trilyon \$’dan fazla olduğu yani küresel gelirin %5’inin kaybedildiği (ACFE, 2024, s.9) göz



önünde bulundurulduğunda, kayıp yaşanmadan engellenebilmesi daha da önemli hale gelmektedir.

Blokzincir teknolojisinin avantajları ve özellikleri dikkate alındığında ise muhasebe bilgi sisteminde uygulanması ile mevcut muhasebe bilgi sisteminde var olan manipülasyon riskini tamamen önleyebilme ve finansal bilgilerin gerçekliğini ve güvenilirliğini büyük ölçüde artırabilme potansiyeline sahip olduğu görülmektedir (Zheng, 2021, s.4). Nitekim gerek internetteki (Grigg, 2005; Tyra, 2014; Brown, 2015), gerek muhasebe mesleğindeki (Deloitte, 2016) ve gerekse de akademideki (Dai ve Vasarhelyi, 2017; Kokina vd., 2017) yorumcular bu kapsamda muhasebenin blokzinciri teknolojisinden faydalanabileceğini öne sürmektedir (McCallig vd, 2019, s.2).

İlgili bağlamdan hareketle çalışmanın bu bölümünde, blokzincir teknolojisinin finansal bilgi manipülasyonunu azaltmadaki potansiyeli üzerine teorik bir çerçeve sunulmuştur. Bu çerçevede, öncelikle finansal bilgi manipülasyonlarının yaratıldığı “muhasebe” süreçlerinde, sonrasında ise üretilen finansal bilgi ve mali tabloların GKGMİ’ne ve yasal mevzuata uygunluğunu kontrol eden “denetim” süreçlerinde blokzincir teknolojisinin uygulanabilirliği ortaya konulmuştur. Ardından genel itibarıyla blokzincir teknolojisinin finansal bilgi manipülasyonunu engellemeye yönelik avantajları ve bu teknolojinin kullanımının yarattığı tehdit ve riskler özetlenmektedir. Son olarak da blokzincir teknolojisi tabanlı uygulamaların muhasebe ve denetim sektörüne etkileri işletme, meslek profesyonelleri ve kamu kapsamında değerlendirilmektedir.

#### **4.1 BLOKZİNCİR TABANLI MUHASEBE**

Blokzincir teknolojisi, 2008 yılında Bitcoin blokzinciri ile ortaya çıktığında, kripto para birimlerinin eşten eşe ödeme sistemi aracılığıyla transferini mümkün kılan bir teknolojiyi ifade etmekten; 2014 yılına gelindiğinde, akıllı sözleşmelere dayalı Ethereum blokzincirinin geliştirilmesiyle süreçlerin otomatikleştirilerek geleneksel araçların işlevsizleştirildiği bir küresel bilgi işlem sistemi yaratılmasına yönelik devrim niteliğinde bir teknoloji olarak dikkat çekmeye başlamıştır. Bu gelişme ile birlikte blokzincir teknolojisinin, sahip olduğu dağıtık defter yapısı ve işlemlerin otomatikleştirilmesini sağlayan akıllı kodları dolayısıyla muhasebe bilgi sisteminde de kullanılabilme potansiyeli açığa çıkmıştır.

Bu kapsamda; blokzincir teknolojisinin muhasebe sektörünü dönüştürme potansiyeli, ilk kez Lazanis tarafından 2015 yılında Brainstorm internet sitesinde yayınlanan “How Technology Behind Bitcoin Could Transform Accounting As We Know It (Bitcoin'in Arkasındaki Teknoloji Bildiğimiz Muhasebeyi Nasıl Dönüştürebilir?)” adlı makalesinde dile getirilmiştir. CPA olan Lazanis (2015), işletmelerin defter kayıtlarından finansal tablolarına kadar tüm muhasebe süreçlerinin blokzincir teknolojisi üzerinden gerçekleştirilerek, finansal tablo yanlışlıklarının engellenebileceğini ve denetçinin tekrar işlemleri doğrulamasına ihtiyaç kalmayacağını ifade etmiştir. Bu durumun da denetçinin rolünü ve muhasebe mesleğini dönüştüreceğini öne sürmüştür.

Diğer yandan Bellucci, Bianchi ve Manetti (2022)'nin blokzincir teknolojisi ile ilgili muhasebe uygulamaları ve araştırmalarına yönelik yapmış oldukları sistematik literatür tarama çalışması sonuçlarına göre ise 2016 yılı, muhasebe için blokzincir çağının başlangıcı olmuştur (Bellucci vd., 2022, s.128). Bu tarih itibarıyla gerek akademisyenler gerek meslek profesyonelleri ve gerekse de muhasebe ve denetim sektörü öncüleri blokzincir teknolojisinin muhasebe ve denetim süreçlerinde uygulanabilirliğine ilişkin çeşitli teorik çalışmalarda ve girişimlerde bulunmaya başlamışlardır.

Yeminli Muhasebeciler Birliği (ACCA), Yeminli Yönetim Muhasebecileri Enstitüsü (CIMA), Yeminli Kamu Maliyesi ve Muhasebesi Enstitüsü (CIPFA) ve Uluslararası Muhasebeciler Federasyonu (IFAC) gibi muhasebe kuruluşlarının tümü web sitelerinde blokzinciri teknolojisiyle ilgili raporlar yayınlamaktadırlar (Han vd., 2023, s.4). Ayrıca Deloitte, KPMG, PwC ve EY olmak üzere dört büyük denetim firması da blokzincir hakkında raporlar düzenlemekte ve bu raporlarda (Deloitte, 2016; KPMG, 2016, 2018; PwC, 2016, 2017; EY, 2017); muhasebecilerin, denetçilerin, düzenleyicilerin ve standart belirleyicilerin, özellikle işlemlerin başlatılması, işlenmesi, kaydedilmesi, mutabakatı, denetlenmesi ve raporlanması da dahil olmak üzere muhasebe ve denetim süreçleri açısından blokzincir teknolojisinden önemli ölçüde etkilenecekleri belirtilmektedir (Fuller, 2016; ACCA, 2017; AICPA, 2017; Coyne vd., 2017 Akt. Schmitz vd., 2019, s.331).

Teorik çalışmaların yanı sıra muhasebede blokzincir teknolojisinin uygulanabilirliğine ilişkin dört büyük denetim firması araştırma geliştirme faaliyetlerinde de bulunmaktadır. Bu kapsamda; Deloitte, 2014 yılında Kanada-Toronto ofisinde yalnızca blokzincir uygulamaları üzerine çalışan ve müşterilerine blokzincir danışmanlık hizmeti sunan Deloitte Rubix ekibini

kurmuştur. Bu ekip Mayıs 2016'da İrlanda-Dublin'de ilk blokzincir laboratuvarını açmış ve Ethereum uyumlu Rubix Core blokzincirini geliştirmiştir. Rubix Core ile müşterilerin kendi sektörleri ve iş ihtiyaçları için özelleştirilmiş kendi blokzinciri prototiplerini oluşturmalarına yardımcı olunması ve akıllı sözleşme Dapp'lerinin oluşturulmasında kolaylaştırma sağlanması hedeflenmektedir (Prisco, 2016).

EY, Nisan 2017'de EY Ops Chain adını verdiği, işletmelerin dijital token'lar ve akıllı sözleşmeler kullanarak operasyonlarını bir blokzincirinde temsil etmelerine olanak sağlayan blokzincir platformunu geliştirmiştir. İşletmeler, EY Ops Chain'i kullanarak iş ortaklarından oluşan ağlar kurabilmekte, yönetebilmekte ve ardından tedarik, envanter, lojistik, faturalama ve hesap yönetimi dahil olmak üzere tüm ekosistemde paylaşılan süreçleri çalıştırabilmektedir (Smigelski, 2019) Ayrıca yine 2017'de denetçilerin işlemleri toplu olarak izlemesine, işlem geçmişine bakmasına, ticari işlemlerde vergi kurallarının uygulanmasına olanak tanıyan blokzincir çözümü Blockchain Analyzer platformunu geliştirmiştir (Blockchain Türkiye, 2020).

PwC, Mayıs 2016'da bankacılık hizmetleri, sermaye piyasaları, yatırım ve servet yönetimi, sermaye piyasaları, sigorta ve işlem ve ödeme hizmetlerini kapsayan FinTech sektöründeki en son gelişmeleri kapsayan tescilli blokzincir içeriği sunan blokzincir çözümü DeNovo platformunu hayata geçirmiştir. Ancak Haziran 2018'de bu platformu kapatmıştır (Ryan, 2018). Bununla birlikte 2016 yılında güvenilir ve gerçek zamanlı denetimin uygulanabilmesi amacıyla yenilikçi teknolojik altyapılara sahip Aura, Halo ve Connect araçlarını hayata geçirmiştir (PwC, 2016). Daha sonrasında da kripto para birimi denetim yazılımını piyasaya sürmüş ve denetim için Halo aracını güncelleştir (Han vd., 2023, s.4). Mart 2017'de, İsviçre'de blokzinciri araştırmaları ve kamu politikaları alanında faaliyet göstermek üzere kurulan ve kâr amacı gütmeyen bir kuruluş olan Crypto Valley Association'ı desteklediğini duyurmuş; Haziran 2017'de, Birleşmiş Milletler tarafından düzenlenen ve hem kamu hem de özel sektör temsilcilerinin bir araya gelerek blokzinciri girişimlerinin yasal kimliği olmayan bir milyardan fazla insanın sorununu nasıl çözmeye çalışabileceğini inceledikleri ID2020 etkinliğine sponsor olmuştur (Kokina vd., 2017, s.97). Ayrıca 2020 yılında akıllı sözleşme denetimlerini gerçekleştirmek üzere İsviçre firması ChainSecurity ile ortaklık kurmuştur (Blockchain Türkiye, 2020).

Son olarak KPMG ise Şubat 2017'de Microsoft ile ortaklaşa “*blokzincir teknolojisini iş tekliflerine ve süreçlerine uygulayan kullanım örnekleri oluşturmak ve göstermek*” üzere Frankfurt ve Singapur'da blokzincir düğümleri oluşturmuştur. Bu işlem sürecinin odak noktası, finansal hizmetler endüstrisinin yanı sıra sağlık hizmetleri ve kamu sektöründeki blokzinciri uygulama zorluklarını ele almak için prototip modeller oluşturmaktır (Kokina vd., 2017, s.97). Ayrıca KPMG daha sonrasında, blokzinciri tabanlı hizmetler üretmek için Guardtime, R3 ve Tomia ile birlikte de çalışmalara başlamıştır (Han vd., 2023, s.4).

Blokzincir teknolojisi; sahip olduğu veri bütünlüğünü koruma, gerekli bilgilerin anında paylaşılması ve süreçlerin programlanabilir ve otomatik kontrolleri gibi işlevleri ile yeni bir muhasebe ekosisteminin geliştirilmesini sağlayabilecek bir potansiyeli taşımaktadır (Dai vd., 2017, s.5-6). Blokzincir teknolojisine dayalı bir muhasebe sürecinde; blokzincirin merkeziyetsiz ve şeffaf yapısının, muhasebe kayıtlarının doğruluğunu ve güvenilirliğini büyük ölçüde artırabilmesi olasıdır. Dağıtılmış defter teknolojisi sayesinde her işlem, ağdaki birçok düğümde kaydedildiğinden blokzincir teknolojisi, muhasebe sistemini, tahrifat ve dolandırıcılığa karşı son derece dayanıklı hale getirebilmektedir. Blokzincirin muhasebe uygulamalarında bir diğer önemli avantajı ise maliyet düşüşü ve verimlilik artışı sağlayabilmesidir. Bu teknolojinin, muhasebe işlemlerini otomatikleştirerek ve manuel müdahale gereksinimini azaltarak süreçleri hızlandırabilme ve hata oranlarını düşürebilme imkânı sağlaması mümkündür. Söz konusu verimlilik artışı ile de hem işletmelerin hem de müşterilerin maliyetlerini azaltmalarına yardımcı olması ve sonunda daha sorunsuz bir finansal sistemin oluşmasına katkı sağlaması beklenmektedir (Chowdhury vd., 2023, s.864).

Blokzincir teknolojisi, finansal ve finansal olmayan verilerin şeffaflığını ve erişilebilirliğini artırarak kayıt tutma, raporlama, güvence sağlama ve yönetim süreçlerinde köklü bir dönüşüme yol açacaktır. Bu yenilikçi teknoloji, muhasebe sistemi ve süreçleri üzerinde önemli değişiklikler meydana getirirse de finansal bilgi kullanıcıları muhasebe, raporlama ve güvence hizmetlerine ihtiyaç duymaya devam edeceklerdir (CPA Canada, 2016, s.16). Dolayısıyla ilgili bağlamda çalışmanın bu bölümünde; blokzincir teknolojisinin, muhasebe bilgi sisteminde yaratabileceği dönüşüm hem genel sistem açısından hem de muhasebenin kaydetme, özetleme, analiz ve yorum fonksiyonları itibarıyla ele alınarak bölüm alt başlıklarında detaylı bir şekilde açıklanmaktadır.

#### 4.1.1 Küresel Kayıt Defteri (World Wide Ledger - WWL)

Blokszincir teknolojisinin muhasebe sürecindeki birincil uygulama alanı defterdir. Tek bir defter, ilgili taraflar arasında gerçek zamanlı olarak paylaşılan ekonomik işlemleri kaydetmektedir. Ayrıca muhasebe sisteminin sahibi ihtiyaç duysa bile muhasebe verilerinin düzenlenmesi ve değiştirilmesi mümkün değildir (Afifa vd., 2023, s.6).

Geleneksel muhasebe süreci mali işlemlerin belgelerden çıkarılarak kaydedilmesi fonksiyonu ile başlamaktadır ve kayıt işlemi, benzer nitelikteki işlemlerdeki artış ve azalışların takip edildiği sınıflandırmalar olan hesaplar itibarıyla yevmiye ve defter-i kebir olmak üzere yasal defterlere yapılmaktadır. Bu defterler noter onaylı ve tek örnek olarak muhasebe birimince tutulmakta ve saklanmaktadır. Dolayısıyla defterlerin kontrolü işletmeye ait olmaktadır. Ayrıca bir işlemin iki tarafı bulunduğundan yola çıkılarak, herhangi bir ihtilaf durumuna karşı ise iki taraf da kendileri açısından işlemin kaydını tutmakta ve böylece uzlaşma sağlanabilmektedir.

Blokszincir tabanlı muhasebe sisteminde ise geleneksel sistemden farklı olarak veriler tarafların tek defterlerine kaydedilmemekte, onun yerine ortak bir sicil görevi gören bloklara kaydedilmektedir ve bu bloklar birbirlerine zincirlenerek kalıcı muhasebe kayıtlarından oluşan bir sistem oluşturmaktadır. Geleneksel sistemdeki defterlerin noter onayına benzer bir şekilde bloklar kriptografik olarak mühürlenmektedir. Ancak farklı olarak defterlerin kontrolü işletmelere ait değildir. Blokszincirin merkeziyetsiz yapısı dolayısıyla herkesin erişimine açıktır. Bu merkeziyetsizlik ve değiştirilemezlik özellikleri nedeniyle blokszincirde faaliyetleri gizlemek için, verileri tahrif etmek veya yok etmek neredeyse imkânsız olmaktadır (Deloitte, 2016, s.3)

Söz konusu özellikleri sebebiyle muhasebe ile bağlantılı olarak blokszincir için “dünya çapında defter” veya “küresel kayıt defteri” anlamına gelen “World Wide Ledger – WWL” ifadesi literatürde yaygın olarak kabul görmektedir. Bu ifadeyi ilk kez Tapscott’lar (2016) kullanmış olup WWL kavramını, *“uluslararası işletmelerin bütün işlemlerinin şeffaf bir şekilde yayınlandığı ve bu bilgileri; düzenleyiciler, yöneticiler ve diğer önemli paydaşlar için erişilebilir, doğrulanabilir ve denetlenebilir hale getiren bir blokszincir tabanlı muhasebe sisteminin nihai uygulaması”* olarak tanımlamışlardır (Potekhina vd., 2017, s.13).

Diğer yandan geleneksel muhasebe sistemlerinde finansal muhasebe bilgilerinin, merkezi sunucularda depolanması ya da güvenli olmayan ağlar üzerinden iletilmesi, bu bilgileri bilgisayar korsanlığına, veri ihlallerine ya da hırsızlığa maruz bırakarak bir şirketin ticari sırlarına ve müşteri gizliliğine yönelik potansiyel tehditler de oluşturmaktadır (Jiang, 2024, s.2). Blokzincir teknolojisi ise veri kaybı riskini en aza indirerek bilgisayar teknolojisinin genel kontrollerine olan ihtiyacı ortadan kaldırmakta ve bu nedenle bir platform terk edilmediği veya kullanılmadığı sürece veri yedeklemeleri, düğümler arasında toplu işlem ve felaket kurtarma gibi geleneksel kontrollere gerek olmamaktadır. Blokzincir defteri ağdaki birden fazla düğüm arasında paylaşıldığından yedeklemelere güvenmek daha az önemlidir, çünkü defterin en son sürümleri ağdaki etkilenmemiş diğer düğümlerden kurtarılabilmektedir (COSO, 2020, s.16).

Dolayısıyla merkezi olmayan dağıtık defter teknolojisine dayanan blokzinciri; bilgi şeffaflığı, kurcalamaya karşı dayanıklı veri ve yüksek güvenlik gibi özellikler sunmakta ve finansal muhasebe bilgi paylaşımının geleneksel yöntemlerinde mevcut olan zorlukları etkili bir şekilde azaltma potansiyeline sahip bulunmaktadır (Jiang, 2024, s.3).

#### **4.1.2 Üç Taraflı Kayıt Sistemi (Triple-Entry Accounting – TEA)**

Muhasebenin ilk olarak ne zaman, nerede, nasıl ortaya çıktığı bilinmemekle birlikte tarihçiler, hesaplaşma ihtiyacının yazı ve rakamların doğuşuna yol açtığını ve bu nedenle muhasebenin, yazının icadından önceye uzanan bir geçmişe sahip olduğunu ileri sürmektedirler (Can, 2007, s.95). Muhasebeye ilişkin en eski belgeler yazıyı icat eden Sümer uygarlığına uzanmakta dolayısıyla muhasebenin yaklaşık 5000 yıllık bir gelişimi söz konusu olmaktadır. Muhasebe, ilk başlarda belirli bir metodolojiden uzak salt bir kayıt tutma düzeni olarak kullanılmakta ve her uygarlığın kayıt tutma sistemi birbirinden farklılıklar göstermektedir. Bu sistem literatürde “Tek Taraflı Kayıt Sistemi (Single-Entry Accounting – SEA)” olarak adlandırılmaktadır.

Tek taraflı kayıt sistemi veya tek girişli muhasebe, “herkesin” muhasebe yapma yöntemidir. Bu yöntemde, varlıkların sıralandığı bir liste oluşturulmakta ve her girişte tarih, tutar ve olayla ilgili bir açıklama kaydedilmektedir. Ancak çok basit olan bu yöntem, herhangi birinin bu listeye ilaveyi veya bu listeden çıkarmayı kolaylıkla yapabilme potansiyeli dolayısıyla kayıtların hile veya hata içermediğine ilişkin güvenilirlikten uzaktır. Dahası

yanlış bir kaydın fark edilmesi halinde, bunun hatadan mı yoksa sahtekarlıktan mı kaynaklandığının tespiti ise mümkün değildir (Grigg, 2005, s.2).

12. yüzyıl sonları itibarıyla modern bankacılığın ortaya çıkmasıyla hem ticaret için sermaye sağlanmış hem de nakit hareketi olmaksızın hesaplar arası fon transferi mümkün olmuştur. Bu banka kredisi ve banka havalesi birleşimi sistem, ticaretin gelişmesine katkı sağlamıştır. Ancak aynı zamanda da artan finansal risklerin takibi için ayrıntılı kayıt tutma yöntemi ve daha da önemlisi borçlu ve alacaklı olunan tutarların bilinmesinin yanı sıra bu tutarların doğru ve doğrulanabilir olmasını sağlayan bir sistem ihtiyacını ortaya çıkarmıştır. Tek taraflı kayıt sistemi ile bu güvence veren muhasebe sistemi sağlanamadığından muhasebenin geliştirilmesine yönelik çalışmalar yapılmaya başlanmış ve modern muhasebenin temelleri atılmıştır (Sangster, 2016, s.301).

Modern muhasebe sistemi “Çift Taraflı Kayıt Sistemi (Double-Entry Accounting - DEA)”nin kaynağı, tam olarak bilinmemesine rağmen literatürde yaygın olarak 15. yüzyıl İtalya’sına dayandırılmaktadır. Bunun nedeni İtalyan rahip ve matematikçi Fra Luca Bartolomeo de Pacioli (Luca Pacioli)’nin 1494 yılında yazdığı “Summa de Arithmetica, Geometria, Proportioni et Proportionalità (kısaca Summa)(Aritmetik, Geometri, Oranlar ve Orantılar Üzerine Genel Çalışma)” isimli kitabının, “defter tutma ve ona ait evrak üzerine bir etüt” başlıklı bölümünde çift taraflı kayıt yönteminin esaslarını anlatması ve bu kitabın çift taraflı kayıt sistemi hakkında basılı ilk kitap olma özelliğini taşımasıdır. Bu nedenle Pacioli “muhasebenin babası” lakabıyla anılmaktadır (Sangster, 2021, s.126)

Çift taraflı kayıt sistemi veya çift girişli muhasebe, “işletmelerin” muhasebe yapma yöntemidir. Çift kayıt kavramı, bir işlemin tarafları ve/veya işlemde yer alan kalemlere ait hesaplar tutulurken, bir hesaba yapılan her giriş (borç - debit) için, başka bir hesaba eşit ve zıt bir "karşı giriş"(alacak - credit) yapılmasını ve karşı giriş yapılan hesabın yerinin belirtilmesini ifade etmektedir. Karşı girişin yeri ile kastedilen ise işleme ilişkin detayların başka nerede kaydedildiğinin gösterilmesidir. Bu kayıt sistemi sayesinde her iki girişin doğruluğuna ilişkin iç ve dış denetim kolaylaşmaktadır (Sangster, 2016, s.300-301). Tek taraflı kayıt sisteminde hilekarın listeye istediği bir tutarı yazması halinde nereden geldiği tespit edilememektedir. Oysaki çift taraflı kayıt sisteminde, deftere yapılan bir girişin mutlaka geldiği bir yer olması gerektiğinden, yapılan hile iz bırakmakta ve karşı taraf defteri ile karşılaştırılarak hile ortaya çıkarılmaktadır (Grigg, 2005, s.2). Böylece çift taraflı kayıt

sistemi ile yöneticilerin kendi defterlerine güvenip güvenemeyeceklerini bilme sorunu çözümlenmektedir (Tyra, 2014)

İşletmeler, doğru finansal raporların oluşturulmasını kolaylaştırdığı ve hataları ve hileli faaliyetleri azalttığı için 600 yıldan fazla bir süredir bu sistemden önemli ölçüde faydalanmaktadırlar. Ancak çift taraflı sistemde, tek bir işlem iki farklı kuruluştaki iki farklı varlık tarafından yönetilebileceğinden hata ve hilelere de açıktır (Oyovwe, 2023, s.4). Dolayısıyla yöneticiler çift taraflı sistemi bağımsız ve dahili olarak kontrol ettiklerinden, dışarıdakiler (örneğin hissedarlar ve hükümetler) için doğal güven ve şeffaflık sorunları yaratmaktadır. Finansal bilgilerin bütünlüğünü sağlamak için bağımsız dış denetçilerin şirketin finansal bilgilerini doğrulaması gerekmektedir. Mevcut muhasebe ve denetim uygulamaları maliyetli, zahmetli ve zaman alıcı olmasına rağmen dolandırıcılığa karşı korumada yetersiz kalmaktadırlar. Bu anlamda muhasebe bilgilerinin şeffaflığının artırılması ile içerdekiler ve dışardakiler arasındaki güven sorununun çözümüne yönelik yeni kayıt yöntemleri arayışları devam etmektedir (Cai, 2019, s.3),

Diğer yandan teknolojinin gelişimine paralel olarak ticaret biçimleri değişmekte ve muhasebede de buna bağlı olarak dijital dönüşüm gerçekleşmektedir. Günümüzde çoğunlukla kayıt işlemlerinin yapılmasının ve finansal tabloların düzenlenmesinin bilgisayar yazılımları kullanılarak gerçekleştirilmesi her ne kadar muhasebenin dijitalleşmesi anlamında kullanılıyor olsa da potansiyeli dikkate alındığında sadece kullanılan araçların değişmesi muhasebe sisteminin dijitalleşmesi anlamına gelmemektedir. Sistemin tamamıyla dijitalleşmesinde henüz uygulama aşamasına geçmeyen Endüstri 4.0, Yapay Zekâ, Nesnelerin İnterneti gibi birçok teknolojik gelişmenin etkili olacağı araştırmacılar tarafından literatürde çokça dile getirilmektedir (Doğan vd., 2019, s.1663-1664). Bu teknolojilerden biri de blokzincir teknolojisidir.

Bu bağlamda muhasebe kayıt sisteminde bir sonraki adımın blokzincir teknolojisine dayandırılarak geliştirilebilmesi mümkündür (Deloitte, 2016, s3). Blokzincir teknolojisinin, kökeni Rönesans'a kadar uzanan çift taraflı kayıt sistemini "Üç Taraflı Kayıt Sistemine (Triple-Entry Accounting – TEA)" dönüştürerek dış paydaşların şeffaf ve gerçek zamanlı bilgi sağlama ihtiyaçlarını karşılama ve güven sorununu çözme potansiyeline sahip olduğu (Oyovwe, 2023, s.4) literatürde birçok araştırmacı tarafından ifade edilmektedir. Kavramsal açıdan baktığımızda; üç taraflı kayıt sistemi, blokzincir teknolojisinin ortaya çıkmasından



çok daha önce ortaya atılmış bir kavramdır ancak uygulanabilirliğinin blokzincir teknolojisi sayesinde mümkün olabileceği öne sürülmektedir (Tyra, 2014). Bu kapsamda söz konusu kavramın gelişimine katkı sağlayan önemli çalışmalar ve sağladıkları katkı Tablo 4.1’de özetlenmiştir:

**Tablo 4.1:** Üç Taraflı Kayıt Sisteminin Gelişimine Katkı Sağlayan Önemli Çalışmalar.

|    | Yıl  | Yazar/Kurum                                  | Sağlanan Katkı                                                                                                                                                                                 |
|----|------|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 1982 | Yuri Ijiri                                   | Momentum muhasebesi adıyla üç girişli defter tutma sisteminden ilk kez bahsedildi.                                                                                                             |
| 2  | 1997 | Todd Boyle                                   | Üçlü Giriş Muhasebesini (TEA) geliştirmek için GL Dialectone'u kurdu.                                                                                                                          |
| 3  | 2005 | Ian Grigg                                    | Kriptografik olarak imzalanmış belgeye dayalı kayıt yapılan üç girişli muhasebe sistemi ve işleyişi tanımlandı.                                                                                |
| 4  | 2014 | Jason Tyra                                   | Grigg'in üçlü kayıt defteri önerisine dayalı bir blokzincir tabanlı muhasebe ve denetim sürecinin işletmelere sağlayabileceği avantajlardan ilk kez bahsedildi.                                |
| 5  | 2015 | Balanc3                                      | Üç girişli defter tutma hizmeti sunan ilk blokzincir şirketi kuruldu.                                                                                                                          |
| 6  | 2016 | Deloitte                                     | Blokzincir teknolojisinin muhasebe sistemi için bir sonraki adım olabileceğini belirterek, Grigg ve Tyra'nın makalelerine atıfta bulundu.                                                      |
| 7  | 2016 | CPA Canada                                   | Finansal bilgilerin kaydedilmesi ve raporlanması için yeni bir yol olarak üç girişli muhasebe sisteminin kullanılabileceğine ilişkin öneride bulundu.                                          |
| 8  | 2017 | Jun Dai & Miklos A. Vasarhelyi               | ERP ve blokzincir teknolojisini bir araya getiren üçlü giriş muhasebesine dayanan blokzincir muhasebe ekosistemi çerçevesini ortaya koydular.                                                  |
| 9  | 2017 | Wang & Kogan                                 | Blokzincir teknolojisi tabanlı bir muhasebe bilgi sistemi tasarımı sunarak, bu tasarıma yönelik prototip geliştirdiler.                                                                        |
| 10 | 2017 | Request Network & bBiller                    | Beyaz kağıtlarına göre Grigg'in üçlü giriş çerçevesine dayalı olarak blokzincir ile üçlü giriş muhasebesi geliştirilmesine yönelik çalışmalar başlattı.                                        |
| 11 | 2018 | Ledgerium                                    | Akıllı sözleşmeler ve üç girişli muhasebeye dayanan, bulut tabanlı blokzincir platformu Luca+ projesi başlatıldı.                                                                              |
| 12 | 2018 | MIT Media Lab                                | İzinli blokzincir tabanlı, sıfır bilgi kanıtı ile defter katılımcılarının gizliliğini koruyan ve hızlı, kanıtlanabilir şekilde doğru denetim imkânı sağlayan ilk sistem zkLedger geliştirildi. |
| 13 | 2019 | Cynthia Weiyi Cai                            | Blokzincir teknolojisinin ortaya çıkardığı üç girişli muhasebe sisteminin gelişimine ve örnek uygulamalarına ilişkin çerçeveyi ortaya koydu.                                                   |
| 14 | 2020 | Hans Weigand, Ivars Blums & Joost de Kruijff | Blokzincir teknolojisi tabanlı ve Finansal Raporlama Standartlarına uyumlu bir paylaşılan defter çözümü önerisinde bulundular.                                                                 |
| 15 | 2024 | Pacio Core                                   | Küresel üçlü giriş uygulamalarını kolaylaştıracak Pacio blokzinciri ağı kuruldu.                                                                                                               |

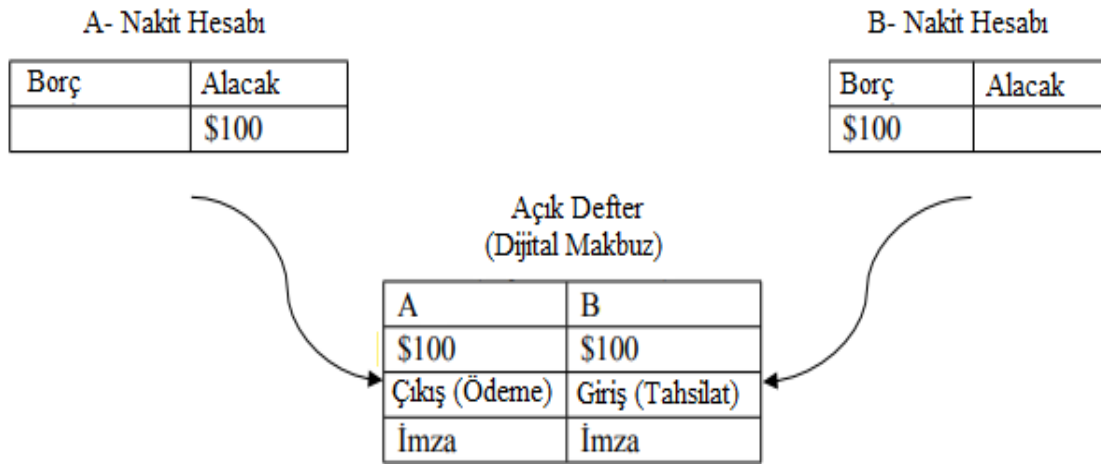
“Üç girişli defter tutma” kavramı ilk kez, Yuji Ijiri tarafından 1982 yılında yayınladığı “Triple-Entry Bookkeeping and Momentum Income (Üç Girişli Defter Tutma ve Momentum Geliri)” adlı makalesi ile ortaya atılmıştır. Ijiri (1986); çift taraflı defter tutmanın mutlak bir sistem olmadığını, çift taraflı sisteme “kuvvet (momentum)” kavramını dahil ederek sistemi genişletmenin mümkün olduğunu ileri sürmüştür. Denklem üçüncü bir girişi (trebit) olan kuvvet, “servetin değişim hızı”nı veya “gelirin kazanılma hızı”nı ifade etmekte ve dönem başına parasal birimler (kuvvetin anlık değişim oranı) ile ölçülmektedir. Kuvvet, gelirin ölçümü için belirtilmesi gereken iki nokta yerine herhangi bir noktadaki kazanılan geliri göstermektedir (Ijiri, 1986, s.745-748). Temel fikir, bir firmanın gelir kapasitesini farklılıklar yerine seviyeler açısından açıklamaktır. Ijiri, zamanın herhangi bir noktasında net servet yerine büyüme seviyesini hesaba katmaya çalışmaktadır. Araba sürmeye benzeterek, sadece o ana kadar kat edilen mesafeyi ölçmek yerine arabanın kat ettiği hızı ölçmek istemektedir (Melse, 2008, s.335). Ijiri’nin üç girişli muhasebe tanımı, iç yönetimin karar almasını kolaylaştırmaya yönelik bir sistem sunmaktadır. Ancak kullanım örneğinin olmaması ve uygulamasının zor olması nedeniyle eleştirilmiştir (Cai, 2019, s.9)

Üç girişe dayanan sistem önerisi, 2005 yılında Grigg tarafından “Triple Entry Accounting (Üç Girişli Muhasebe)” isimli makalesi ile farklı bir yaklaşıma dayanarak ikinci kez ortaya atılmıştır. Grigg’in üç girişli muhasebesinde amaç işletmelerin mali tablolarının güvenilirliğini artırmak olup, tarafsız bir aracından işlem işleme yetkisi alınması ve her bir tarafın (işleme dahil olan iki taraf ve aracı) işlem için bir kayıt oluşturarak toplamda üç giriş yapılması şeklinde işleyen bir sistemi ifade etmektedir. Bu sistemde “işlem olarak belge (the receipt is the transaction)” ilkesi benimsenmekte, borçlu ve alacaklı taraflarca kriptografik olarak imzalanmış (dijital imzalı) belge esas alınarak kayıtlar tutulmaktadır. Böylece hem borçlu ve alacaklı tarafların niyeti hem de aracının bu niyetlere karşılık gerçekleştirdiği eylem doğrulanabilmektedir (Grigg 2005, s.4-6). Dolayısıyla bu mekanizmada, her bir işlemi doğrulamak için bağımsız ve güvenilir bir aracıya yani üçüncü tarafa gereksinim duyulmaktadır. Diğer yandan aracı tarafından saklanan kayıtların siber saldırılar nedeniyle kaybolma veya yetkisiz değişiklik riskine maruz kalması söz konusudur (Dai vd., 2017, s.). Ayrıca üçüncü defter kayıtlarını kontrol edip üçüncü taraf olarak hareket edecek güvenilir tarafın kim olacağına ilişkin belirsizlik de mevcuttur (Cai, 2019, s.10). Blokzincir teknolojisi ise bu noktada, Grigg’in üç taraflı sistemine ilişkin riskleri azaltma ve mekanizmayı iyileştirme konusundaki önemli potansiyeli ile devreye girmektedir. Grigg’in muhasebe

kayıt sisteminde blokzincir teknolojisinin kullanılmasıyla güvenilir merkezi bir üçüncü taraf ihtiyacı ortadan kalkmakta onun yerine merkezi olmayan, güvenli, değişmez ve otomatik bir üçüncü kayıt tarafı yaratılabilmektedir.

Özetle üç taraflı kayıt veya üçlü giriş muhasebesi; dış paydaşların muhasebe verilerine güven sorununu çözerek, “bilgi kullanıcılarının” muhasebe yapma yöntemi olarak, dış tarafları ilgilendiren tüm muhasebe girişlerinin üçüncü bir giriş tarafından kriptografik olarak mühürlendiği geleneksel çift giriş sistemine bir geliştirmedir (Tyra, 2014).

Dolayısıyla blokzincir; bir muhasebe platformu, yevmiye kayıt aracı ya da muhasebe yazılımı yerine geçecek bir araç değildir. Bununla birlikte geleneksel çift girişli muhasebe sistemi üzerine inşa edilmiş, işlemin iki tarafının aynı blokta onaylandığı üçüncü tarafı temsil etmektedir. Geleneksel sistemde işlem tarafları kendi kayıtlarını ayrı ayrı tuttuklarından herhangi bir ihtilaf durumunda hesap mutabakatı ve denetim yapılması ihtiyacı bulunmaktadır. Blokzincirde ise işlem öncelikle iki tarafça onaylanmakta, ardından paylaşılan deftere kaydedilmektedir. Böylece herkes, her zaman, gerçek zamanlı olarak, aynı ve doğru bilgiye sahip olacağından zamandan tasarruf edilmekte, mutabakat ihtiyacı ve hatalar ortadan kalkmaktadır (Nordgren vd., 2019, s.50)



**Şekil 4.1:** Üç Taraflı Kayıt Yönteminin Basit Örneği.

[Cai, 2019, s.32]

Blokzincir tabanlı üç taraflı kayıt sürecini, A ve B arasındaki bir nakit işlemi üzerinden örneklendirecek olursak (Şekil 4.1); satıcı (B) aldığı nakit için bir borç kaydı yaparken, alıcı

(A) ise harcadığı nakit için bir alacak kaydı yapmaktadır. Ancak bu kayıtlar ayrı defterlerde değil, aynı dağıtılmış, kamuya açık defterdeki hesaplar arasında bir işlem olarak gerçekleşmekte ve böylece birbirine bağlı bir muhasebe kayıtları kümesi oluşturmaktadır. Blokzinciri herhangi bir veri değişikliğine karşı değişmez olduğundan, yazılı muhasebe kayıtlarını tahrif etmek veya silmek imkânsız olmaktadır (Tyra, 2014; Potekhina, 2017, s.13)

"Üç taraflı kayıt sistemi" kavramının, blokzincir teknolojisine dayalı olarak kullanılabileceğine ilişkin öneriler (Tyra, 2014; CPA Canada, 2016; Deloitte, 2016) birçok kez dile getirilmekle birlikte bu kavramı, blokzincir ortamında muhasebe kayıtlarını belgelendirmede ilk uygulayan Dai ve Vasarhelyi (2017) olmuştur (Kozlowski, 2018, s.301). Dai & Vasarhelyi (2017), "Toward Blockchain-Based Accounting and Assurance (Blokzincir Tabanlı Muhasebe ve Güvenceye Doğru)" isimli çalışmalarında Grigg'in üç taraflı muhasebe sistemine dayanan ve ERP (Enterprise Resource Planning – Kurumsal Kaynak Planlama) ile blokzincir teknolojisini bir araya getiren bir muhasebe ekosistemi çerçevesi tanımlamışlardır.

İlgili makalede yazarlar, mevcut çift girişli sistem içerisine gömülen üçüncü bir blokzinciri katmanı ile mevcut muhasebe sisteminin genişletilmesini önermektedirler. Bu sistemde her işlem, hem geleneksel çift girişli sisteme göre kaydedilecek hem de bu üçüncü taraf olan blokzinciri defterinde saklanan bir kayıt oluşturulacaktır. Bu üçüncü defterdeki girişler, veri akışlarını yansıtmak üzere borç/alacak hesapları arasında "jeton (token) transferleri" şeklinde kaydedilecektir. Blokzinciri hesapları, muhasebe kayıtlarını üç seviyede toplayan hiyerarşik bir yapıda oluşturulacaktır: en altta bireysel hesaplar; ortada toplam varlıklar, borçlar ve özsermaye ve en üstte bir bütün olarak şirket. Bu yapı, akıllı sözleşmeler kullanılarak bilanço denklemini otomatik olarak doğrulayabilecek ve farklı taraflar için farklı görünümünün verilmesini sağlayabilecektir. Bu şekilde her bir blokzinciri hesabı, bir ERP sisteminde karşılık gelen çift girişli hesaba bağlanarak birbirine kenetlenen bir kayıt sistemi oluşturacaktır. Ayrıca bu jetonlar (token), ticari taraflar arasındaki yükümlülüklerin veya varlıkların sahipliğini kanıtlamak için sertifika olarak da kullanılabilecektir (Dai vd., 2017, s.11-12).

Dai ve Vasarhelyi (2017), geleneksel "merkezi" ERP veri tabanları yerine "merkezi olmayan" bir blokzinciri veri tabanı üzerine inşa edilmiş üçüncü bir defter önermektedirler.

Bu çerçeve, mevcut ERP sistemini değiştirmeyi değil; mevcut sisteme, blokzincir tabanlı bir yapı eklemeyi hedeflemektedir (Cai, 2019, s.16).

Dai ve Vasarhelyi'nin ardından blokzincir teknolojisine dayanan üç taraflı muhasebe sistemine yönelik gerek akademide gerekse de sektörde birçok çalışma (Tablo 4.1) gerçekleştirilmiş ancak henüz yaygın olarak kabul edilmiş bir sistem yaklaşımı mevcut değildir. Diğer yandan blokzincir tabanlı muhasebe sisteminin potansiyeli dikkate alınarak üç girişli muhasebe sistemini uygulamak amacıyla start-up projeleri başlatılmıştır. Request Network, bBiller, Balanc3, Luca+, zkLedger ve Pacio bu amaçla geliştirilmekte olan muhasebe yazılım programlarına örneklerdir (Cai, 2019, s.17).

Sonuç olarak, blokzincir tabanlı üç girişli muhasebe bilgi sistemindeki otomatik bilgi doğrulama, işleme, depolama ve raporlama işlevleri bir arada kendi kendine yeterli bir muhasebe ekosistemi oluşturma potansiyeline sahip bulunmaktadır (Dai vd., 2017, s.13).

#### **4.1.3 Günlük İşlemlerin Değiştirilemez ve Otomatik Kaydı**

Geleneksel muhasebe kayıt sisteminde işlemler defterlere kronolojik olarak kaydedilmektedir. Blokzincir tabanlı muhasebe sisteminde de benzer şekilde muhasebe işlemleri bloklar içine zaman damgası ile kaydedilmekte ve kendinden önceki ve sonraki işlem kayıtlarına blok hash değeri ile bağlanmaktadır. Farklı olarak ise geleneksel muhasebe sisteminde defter kayıtları üzerinde tahrifat yapılabilmesi mümkün iken; dağıtık defter teknolojisi olan blokzincirde, kriptografi, mutabakat algoritmaları ve zincir yapısı ile veri güvenliği sağlandığından ağa kaydedilen verilerin sahte veya hatalı olması, değiştirilmesi ya da silinmesi mümkün olamamaktadır. Bu özellikleri dolayısıyla blokzincir teknolojisine dayalı bir muhasebe bilgi sisteminde deftere kaydedilen işlemler güvenilir, kalıcı ve değişmez niteliklere sahip olmaktadır.

Diğer yandan bu değiştirilemezlik özelliği, avantajlarına rağmen; muhasebede herhangi bir hatalı kayıt durumunda çokça başvurulmuş “ters kayıt” tekniğinin uygulanamayarak blokzincir kayıtlarının geri döndürülebilmesi konusunda eleştirilmekte ve teknolojinin kullanımının yaygınlaşması önünde bir engel olarak görülmektedir (Selg, 2023, s.40)

Blokzincir teknolojisinin muhasebe kayıt sürecine sağladığı bir diğer katkı ise tekrar eden muhasebe işlemlerinin otomatik olarak kaydedilebilmesini sağlamasına yöneliktir. Belirli

koşullar oluştuğunda tetiklenerek işlemlerin otomatik olarak gerçekleştirilebilmesini sağlayan akıllı sözleşmeler aracılığıyla, müşteriler ve tedarikçiler arasındaki anlaşmaların, personel bordro işlemlerinin veya banka mevduat mutabakatlarının otomasyonu sağlanabilmektedir (Giang vd., 2023, s.4).

Akıllı sözleşmeye dayalı bir alım-satım işleminin kayıt sürecini örneklendirecek olursak; işlemin onaylanması halinde geleneksel sistemdeki satıcının alıcıya faturayı göndermesi yerine, fatura doğrudan alıcı ile gerçek zamanlı olarak blokzincir defterinde paylaşılmakta ve ödeme, alıcı firmanın banka hesabından otomatik olarak ödenmektedir. Bu sayede hatalardan veya eksik faturalardan kaynaklanan anlaşmazlıklar azaltılarak, faturalandırma ve ödeme sürecinin doğruluğu ve verimliliği artırılabilir (Gül, 2019, s.191).

Ayrıca blokzincir tabanlı muhasebe sisteminde, muhasebe kurallarının akıllı sözleşmelere kodlanması ile muhasebe ilke ve standartlarına uygun işlemlerin otonom olarak kaydedilmesi de mümkün olabilmektedir. Örneğin, "satışlar, malların sevkiyatından sonra kaydedilmelidir" kuralının kodlanması halinde; akıllı sözleşme yazılımı, blokzincir defterine bir satış kaydı eklemeyi önce sevkiyat tarihini kontrol edip mallar sevk edilene kadar işlem güncellemesini yapmama şeklinde süreci yürütebilmektedir. Böylece muhasebe faaliyetlerine ilişkin kayıtların etkin bir şekilde kontrol edilmesi ve kayıt, sınıflandırma ve işlem yapmama gibi süreçlere otomatik güvence yaratılması sağlanabilmektedir (Dai vd., 2017, s.15).

Diğer yandan defter tutma sürecinin otomatikleştirilmesi için akıllı sözleşmeler, fiziksel nesnelerin gerçek koşullarını ve faaliyetlerini yakalayabilen IoT teknolojileriyle de birleştirilebilirler. Örneğin, bir envanter kaleminin IoT aracılığıyla iletilen coğrafi bilgilerine dayanarak şirketten ayrıldığı biliniyorsa, akıllı sözleşmeler blokzincir defterine bir satış kaydı göndermek için yürütülebilir. Ayrıca gelecekteki cihazlar sensörlerle, akıllı çiplerle donatılacağından ve ağlara erişebileceğinden herhangi bir envanter hasarını, teslim edilmemeyi veya gecikmeyi kendi kendilerine rapor edebilirler. Bu raporlar da ilgili muhasebe ölçümlerini zamanında ayarlamak için akıllı sözleşmeleri tetikleyebilir (Dai vd., 2017, s.16).

Bu kapsamda blokzincir teknolojisine dayalı muhasebe sisteminde gerçekleştirilebilmesi muhtemel otomatik işlemler, aşağıda maddeler halinde örneklendirilmiştir (CPA Canada, 2016, s.18):

- a. Dijital para birimleri şeklindeki nakit, üçüncü taraf kayıtlarıyla mutabakata gerek kalmadan doğrudan takas edilebilir. Söz konusu işlemlerin anlık olarak takas edilmesi, üçüncü taraflar aracılığıyla işlemlerin takas edilmesi için gereken sürenin ortadan kalkmasını sağlayacaktır.
- b. Alacak ve borç hesap bakiyelerindeki fonlar, belirli koşulların karşılanmasına (örneğin, teslimat makbuzlarına ve kararlaştırılan ödeme planlarına dayalı olarak) dayalı programlanan akıllı sözleşmeler aracılığıyla otomatik olarak yönlendirilebilir.
- c. Envanterler, alıcının envanter yönetim sisteminden gelen bir "satın alma mesajına" yanıt veren "varlık transferi" akıllı sözleşmelerine dayalı olarak güncellenebilir.
- d. Fikri mülkiyet haklarını yansıtan maddi olmayan varlıklar, fonları otomatik olarak yönlendirmek üzere programlanabilen "akıllı telif sözleşmeleri" olarak yansıtılabilir. Maddi olmayan varlıkların mülkiyet sahipliği konusundaki anlaşmazlıkları, blokzincirin zaman damgası özelliği sayesinde ortadan kaldırılabilir.
- e. Varlıklar bir blokzincirine kaydedilebilir ve mülkiyet, dijital para birimlerinin transferine benzer bir şekilde kolayca aktarılabilir. Onarım ve bakım işlemlerini kaydetmek için ek blokzincir defterleri oluşturulabilir. Böylece varlıklarının tüm bakım geçmişi kolayca erişilebilir ve aktarılabilir olacaktır. Bu durum sigorta maddelerinde referans olarak gösterilebilir.
- f. Kurumsal krediler "akıllı kredi sözleşmeleri" olarak tamamen dijitalleştirilebilir ve bir blokzincirine yerleştirilebilir. Blokzincir akıllı sözleşmeleri olarak temsil edildikten sonra, bu borç yükümlülükleri kolayca devredilebilir ve geçmişleri otomatik olarak vadeye kadar izlenebilir.

Sonuç olarak blokzincir tabanlı muhasebe sistemi ile sağlanan bu güvenilir, değiştirilemez, eş zamanlı ve otomatik kayıt süreci; fatura edilen tutara karşılık gelmeyen transferler, fatura numaralarındaki hatalar vb. gibi işlemlerin periyodik olarak düzeltilmesi görevlerini (Giang vd., 2023, s.9), işletme ile tedarikçiler ve müşteriler arasındaki bakiye mutabakat işlemlerini

(Özdoğan vd., 2018, s.168) ortadan kaldırmaktadır. Dolayısıyla rutin ve tekrarlayan muhasebe görevlerini otomatikleştirerek hataların sınırlandırılmasına, idari maliyetlerin azaltılmasına ve finansal süreçlerde verimliliğin, doğruluğun ve şeffaflığın artırılmasına katkı sağlamaktadır (Giang vd., 2023, s.4).

#### **4.1.4 Gerçek Zamanlı ve Otomatik Finansal Tablo Sunumu**

Blokszincir teknolojisi akıllı sözleşmeler ile birlikte şeffaf, güvenilir, doğrulanabilir ve değiştirilemez bir muhasebe ekosistemi yaratmaktadır. Bu sisteme, IoT gibi gelişmekte olan teknolojiler entegre edilerek faaliyetlerin gerçek zamanlı izlenmesi sağlanmakta ve böylece iş performansının gerçek zamanlı ve otomatik olarak kaydedilmesi ve ölçülmesi mümkün olabilmektedir. Dolayısıyla bu mekanizma ile elde edilen muhasebe bilgilerinden üretilen raporlar da bilgi kullanıcılarına (yöneticiler, denetçiler, paydaşlar, alacaklılar, devlet kurumları vb. gibi) rollerine ve taleplerine göre çeşitli düzeylerde gerçek zamanlı olarak sunulabilmektedir (Dai vd., 2017, s.6).

Diğer yandan geleneksel finansal raporlamada; işletmeler, mali tabloları üç ay gecikmeli olarak yayınlamaktadırlar. Ancak gerçek zamanlı blokszincir muhasebe sisteminin kullanılması halinde bu zaman gecikmesi tamamen ortadan kalkmaktadır (Potekhina vd., 2017, s.17). Bu durumda işletmenin tüm muhasebe bilgileri, herhangi bir hissedar, müşteri, borç veren, ticari alacaklı ya da diğer ilgililer tarafından anında görülebilmekte ve herkes istediği zaman firmanın işlemlerini bir gelir tablosu ve bilanço şeklinde toplayabilmektedir. Böylece ilgililerin, firma ve denetçileri tarafından hazırlanan üç aylık mali tablolara güvenme mecburiyeti artık kalmamaktadır (Yermack, 2017, s.24). Ayrıca GKGMİ ve UFRS düzenleyici çerçevelerine göre hazırlanan finansal tabloların karmaşasını azaltmak için uygulanan maliyetli ve zaman alıcı yeniden formülasyon süreci de şeffaf bir blokszinciri defteri sayesinde saniyeler içinde gerçekleştirilebilir hale gelebilmektedir (Potekhina vd., 2017, s.35).

Ancak blokszincir tabanlı finansal bilgilerin, tüm muhasebe bilgi kullanıcıları tarafından eş zamanlı olarak görülebilmesi avantajlı olsa da her bilgi kullanıcısının tüm muhasebe verilerine erişebiliyor oluşu eleştirilmektedir. Bu eleştiriye göre; her bilgi tüketicisinin, muhasebe verilerine yönelik farklı ihtiyaçları ve hedefleri bulunmaktadır. Örneğin; CFO ve denetçilerin tüm muhasebe verilerine tam erişim ihtiyacı, hesap ödeme memurlarının



yalnızca ödenecek hesap girişlerini gözden geçirme ihtiyaçları ve yatırımcıların ise toplu özetlenmiş verilere ihtiyaçları bulunmaktadır. Bu nedenle her bilgi kullanıcı grubuna rollerine ve gereksinimlerine göre özel erişim yetkilerinin tanımlanması (Dai vd., 2017, s.13) ve buna bağlı olarak da düzenleyicilerin ve diğerlerinin kimin, hangi bilgiye, ne zaman eriştiğini belirleyebilmeleri için erişim anahtarları etrafında uygun kontrollerin yapılması ve prosedürlerin oluşturulması gerekmektedir (CPA Canada, 2016, s.17).

Bununla birlikte blokzincir teknolojisi, dağıtık defter yapısı ve akıllı sözleşmeler ile muhasebe verilerini gerçek zamanlı olarak özetlemekte ve işletme genelinde yönetici ve yönetim kurulu raporlamaları için mali tabloların konsolidasyonunu otomatikleştirebilmektedir. Ek olarak akıllı sözleşmeler, iç ve dış raporlamayı etkileyen operasyonel ve idari işlemlere entegre edilerek performans hedeflerini ve bütçeleri, gerçek sonuçlarla takip etmeyi sağlayabilmektedir. Böylece blokzincir tabanlı yeni performans yönetimi araçları ile performans sözleşmeleri, verimlilik değerlendirmeleri ve performans primlerinin daha etkili ve otomatik bir şekilde yönetilmesi mümkün hale gelebilmektedir. Ayrıca blokzincir teknolojisi ile sürdürülebilirlik raporlaması gibi finansal olmayan raporlamalar da otomatikleştirilerek; paydaşların, blokzincire dayalı üretim tedarik zincirine erişim sağlamasına ve üretim sürecini, hammaddeden mamul ürüne kadar şeffaf bir şekilde izlemesine olanak tanıyabilmektedir (CPA Canada, 2016, s.17).

Dolayısıyla geleneksel finansal raporlama yöntemleriyle karşılaştırıldığında, blokzincir teknolojisine dayalı muhasebe bilgi sistemi yüksek şeffaflık, izlenebilirlik, zamanlılık, kurcalamaya karşı dayanıklılık ve finansal tablo üretiminde otomasyon gibi avantajlara sahiptir. Bu avantajlar hem finansal muhasebe maliyetlerini büyük ölçüde azaltabilmekte hem de bilginin güncelliğini, güvenilirliğini ve karşılaştırılabilirliğini daha da geliştirebilmektedir (Yu vd., 2018, s.44). Özetle blokzincir teknolojisi; finansal raporlamanın odağını, iş merkezli bir modelden değişim merkezli bir modele dönüştürmekte ve finansal raporlamanın kalitesini ve güvenilirliğini artırmaktadır (Atik vd., 2021, s.504).

#### 4.1.5 Dinamik Analiz ve Etkin Karar Alma Süreci

İşletmenin finansal durumunun ve faaliyet sonuçlarının analiz edilebilmesi için geniş içeriklere sahip büyük miktarlardaki muhasebe verilerinin özetlenerek finansal raporlara dönüştürülmesi gerekmektedir. Bu finansal raporların, geleneksel sistemler ile kanun ve yönetmeliklere uygun olarak hazırlanması gerek muhasebe verilerinin kalitesi gerekse de muhasebe personelinin ağır iş yükü nedeniyle uzun süreler almakta ve raporlar güncel olarak analiz için ihtiyaç duyulan zamanda düzenlenememektedir. Blokzincir teknolojisi ise finansal raporlamanın eşzamanlı ve otomatik olarak talebe göre oluşturulmasını sağlamaktadır. Böylece finansal raporlamanın post analizini, süreç öncesi ve süreç içi dinamik analize dönüştürmektedir. Finansal durumu dinamik ve gerçek anlamda önceden yansıtabilmekte ve finansal durum ile operasyon faaliyetlerinin önceden tahmin edilebilir olmasını sağlayabilmektedir (Zheng, 2021, s.3).

Blokzincir teknolojisinin hash fonksiyonlarıyla birbirine bağlı zincir yapısı sayesinde işletmeye ait tüm veri tabanına erişilebilmekte ve hem son birkaç dakika içinde işletmede gerçekleşen değişimler hem de kuruluşundan itibaren işletmenin tarihsel bir resmi elde edilebilmektedir (Tapscott vd.,2017, s.12). Yani kullanılan muhasebe ilkelerinin ve değerlendirme modellerinin kökenleri hakkındaki bilgiler de gözden geçirilebilmektedir (Abu Afifa vd., 2023, s.9) Bu şekilde muhasebe politikalarının ve varsayımlarının akıllı sistemlerle izlenebilmesi, muhasebe seçimlerinin ve yargılarının şeffaf olmasını sağlamakta ve buna bağlı olarak da muhasebe bilgilerinin karşılaştırılabilirliğini artırmaktadır (Yu vd., 2018, s.43)

Halka açık işletmelerin finansal tabloları, denetlendikten sonra yatırımcılar için bir dereceye kadar güvenilirlik kazanmaktadır. Ancak yatırımcılar bu tabloları sadece biçimsel olarak değerlendirebilmekte ve işletmenin gerçek muhasebe süreçlerini tam olarak gözlemleyememektedirler. Bu nedenle sadece finansal tablolara dayanarak işletmenin mali durumu, faaliyet performansı ve nakit akışı hakkında tam, doğru ve zamanında bir değerlendirme yapmaları mümkün olmamaktadır (Yu vd., 2018, s.41). Blokzincir teknolojisine dayalı bir muhasebe sistemi ile bilgi kullanıcıları firmanın ham verilerine erişebildiklerinden, amortisman veya envanter gibi kendi nakit dışı ayarlamalarını yapmak üzere kendi muhasebe yargılarını uygulayarak, blokzincirde kayıtlı verilerden istedikleri zaman kendi mali tablolarını oluşturabilmekte ve amortisman işlemleri, varlıkların piyasa

değerine göre belirlenmesi ve gayri nakdi tahakkukların kazançlara yansıtılması gibi konularda kendi kararlarını verebilmektedirler (Yermack, 2017, s.25). Ayrıca işletme yönetimi ve yönetim kurulu tarafından alınan tüm kararların ve eylemlerin zaman damgalı bir kaydının tamamen izlenebilmesi de mümkün olabilmektedir (CPA Canada, 2016, s.38). Ek olarak blokzincir çözümleri sadece işletme ortakları ve yatırımcılara bilgi sağlayarak değil, aynı zamanda tüketicilere de bilgi aktararak karar verme sürecini etkinleştirmektedir. Tüketicilerin mal ve hizmetlerin menşesine ilişkin elde ettikleri doğru, tam ve zamanında bilgiler, onların daha bilinçli kararlar vermesini de sağlayabilecektir (CA ANZ, 2017, s.33).

Bununla birlikte müşterinin ve ticaret ortaklarının faaliyet gösterdiği yönetim kuralları ve karar alma politikaları, akıllı sözleşmeler ile otomatikleştirilebilmekte ve karar verme gücü blokzincirdeki birden fazla katılımcıya dağıtılabilir (Kozlowski, 2018, s.301). Hatta akıllı sözleşmelere, büyük veri ve tahmine dayalı analiz entegre edilerek muhasebe sürecine zekâ katılabilmesi de mümkün olmaktadır. Örneğin, bir temerrüt veya kredi notu tahmin modeline dayalı kodlanmış bir akıllı sözleşme ile, borçluların temerrüt riskleri mali durumlarına ve satın alma davranışlarına göre izlenerek kötü borç tahminlerinde ayarlama yapılabilmektedir (Dai vd., 2017, s.13).

Diğer yandan akıllı sözleşmelerin yapay zekâ ile bütünleştirilmesi halinde analiz ve karar verme süreçlerinde insan muhakemesini taklit etmek üzere yapay zekâ kullanılarak, gerçek zamanlı ticari işlem verilerinin ve bir blokzincirdeki diğer bilgilerin analiz edilmesi de mümkün olabilecektir (COSO, 2020, s.4). Böylece blokzincir verilerini analiz etmek ve belirli kalıplar ve eğilimleri ortaya çıkarmak için yapay zekâ tekniklerinden yararlanılarak, daha akıllı muhasebe süreçleri ve karar desteği sağlanabilecektir (Liu vd., 2024, s.6).

Sonuç olarak blokzincir teknolojisi, dağıtık defter teknolojisi ve akıllı sözleşmeleri ile geçmiş ve gerçek zamanlı işlemler için tüm piyasa katılımcılarına şeffaf bilgi sağlayarak asimetrik bilgi sorununun çözümlenmesine ve karar alma sürecinin etkin bir şekilde yürütülmesine katkı sağlamaktadır (CA ANZ, 2017, s.33).

## 4.2 BLOKZİNCİR TABANLI DENETİM

Muhasebe denetimi, belirli bir ekonomik birim veya döneme ilişkin bilgilerin önceden belirlenen kriterlere uygunluğunu incelemek ve bu süreç sonucunda bir rapor hazırlamak amacıyla bağımsız bir denetçi tarafından gerçekleştirilen kanıt toplama ve değerlendirme sürecidir. (Bozkurt, 2015, s.29). Bu süreç dört ana aşamadan oluşmaktadır: (i) müşteri işletmenin incelenmesinin, analitik incelemenin, önemlilik düzeyi ve riskinin ön belirlenmesinin ve denetim programının yapıldığı “planlama”, (ii) iç kontrol sisteminin değerlendirildiği ve maddi doğruluk testlerinin yapıldığı “denetimin yürütülmesi”, (iii) kanıtların değerlendirildiği, denetim görüşünün oluşturulduğu ve denetim raporunun yazıldığı “raporlama” ve son olarak (iv) denetim sonuçlarının izlenmesi. Bununla birlikte geleneksel denetim süreci; (i) önemli yanlışlık riski hakkında denetim kanıtı toplamak için işlemlerin örneklenmesini, (ii) geriye dönük bir denetim yaklaşımını ve (iii) yıllık, anlık bir denetim görüşünü kapsamaktadır (Rozario vd., 2018, s.3). Dolayısıyla tüm bu zorlu, zaman alıcı ve maliyetli sürece rağmen denetçiler, denetim süreci sonucunda elde ettikleri yeterli ve uygun denetim kanıtlarıyla önemli bir yanlışlık olmadığına dair ancak makul bir güvence verebilmektedirler.

Ancak mevcut denetim sürecine rağmen finansal bilgi manipülasyonlarının önüne geçilememesi, bu denetim alanındaki zayıf noktaları açığa çıkarmaktadır. Teknolojik gelişmelerin sağladığı otomasyon da geleneksel denetim modelinin evrim geçirmesine neden olmaktadır. Bununla birlikte bir denetim sürecinin, muhasebe bilgi sisteminden elde edilen kanıtlar üzerinden yürütüldüğü göz önünde bulundurulduğunda muhasebe alanında ortaya çıkan değişiklikler ve gelişmeler de denetim alanını etkilemektedir. Önceki bölümde detaylı olarak ele alındığı üzere; blokzincir teknolojisi tabanlı üç girişli muhasebe bilgi sistemi, bilgilerin otomatik olarak doğrulanması, işlenmesi, depolanması ve raporlanması yoluyla kendi kendine yeterli bir muhasebe ekosistemi oluşturma potansiyeli yaratmaktadır (Dai vd., 2017, s.9). Dolayısıyla benzer şekilde; blokzincir teknolojisine dayalı bir denetim süreci ile de muhasebenin doğrulama, işleme, depolama ve raporlama işlevlerinin doğruluğunun eş zamanlı ve otomatik olarak teyit edilmesi mümkün olabilmektedir. Böylece blokzincir teknolojisine dayalı bir denetim ekosisteminin de oluşturulma potansiyeli bulunmaktadır (Kozlowski, 2018, s.304).

Sonuç olarak blokzincir teknolojisinin denetim süreçlerinde kullanılmasının, klasik denetim anlayışında önemli değişiklikler yaratması beklenmektedir. Söz konusu kapsamda çalışmanın bu bölümünde blokzincir teknolojisinin denetim sürecinde yaratabileceği olası değişiklikler, özellikleri itibarıyla alt başlıklar altında açıklanmıştır.

#### **4.2.1 Gerçek Zamanlı Sürekli Denetim**

Geleneksel denetim uygulamaları, emek yoğun bir süreçtir. Denetim öncesinde, denetçilere yevmiye kayıtları, elektronik tablo dosyaları ve hem elektronik hem de manuel formatta diğer belgeler gönderilmektedir. Asıl denetim süreci başlamadan önce denetçilerin, verilerin hazırlanması ve denetimin planlanması için önemli bir zaman ayırması gerekmektedir. Bu uzun hazırlık süreci, verimlilik ve maliyet etkinliği açısından olumsuz etkiler yaratabilmektedir (Schmitz vd., 2019, s.336).

Diğer yandan bilgisayar destekli denetim teknikleri (CAAT) aracılığıyla manuel süreçler otomatikleştirilerek, denetim alanı genişletilerek ve yeni denetim prosedürleri geliştirilerek denetim sürecinin etkinliği ve verimliliği artırılmaya çalışılmaktadır (Champlain, 2003, s.278). Bu kapsamda gerçekleştirilen sürekli denetimler<sup>52</sup>, fiziksel belge olmadan ve gerçek zamanlı muhasebe sistemleri kullanılarak hazırlanan mali tabloların doğruluğu hakkında makul görüş elde edilmesini sağlamaktadır (Rezaee vd., 2001, s.151). Ancak mevcut bilgisayar destekli denetim teknikleri ile gerçekleştirilen sürekli denetim uygulamaları her ne kadar denetim sürecinin otomasyonuna katkı sağlasa da bu yöntemler ideal gerçek zamanlı denetim anlayışından uzak kalmaktadır. Daha çok belirli bir dönemsellığe bağlı "gerçek zamanlıya yakın" denetim kavramını ifade etmektedir (Ertikin, 2017, s.84). Bu noktada blokzincir teknolojisi, ideal anlamdaki gerçek zamanlı sürekli denetimin uygulanabilmesi için ihtiyaç duyulan teknolojik altyapıyı sağlamaktadır.

Blokzincir tabanlı denetim sürecinde; bir ticari işlem gerçekleştiğinde, dijital paranın bir varlıktan diğerine aktarılmasıyla temsil edilen ticari olay kamuya açıklanmakta ve gerçek zamanlı olarak kaydedilmektedir. Bu şekilde işlemler sürekli olarak blokzincirine eklenmekte ve bu blokzincirine tüm kullanıcılar istedikleri zaman erişim sağlayabilmektedir. Bu nedenle denetçiler, müşterilerinin işlem verilerinin tam bir kopyasına sahip

---

<sup>52</sup> “Sürekli denetim” hakkında detaylı bilgi için bkz. s.157.

olabilmektedirler. İşlem verilerinin gerçek zamanlı olarak elde edilebiliyor olması, denetçilerin, firmanın küresel varlıklarını sürekli olarak izleyebilmelerini mümkün kılmaktadır. Bir denetçi, müşterisinin müşterilerinden veya tedarikçilerinden alacaklı olduğu hesapları teyit etmek isterse denetçinin, yalnızca ilgili satış veya tedarik işlem verilerini blokzincirinden toplaması ve analitik prosedürleri (örneğin, işlem tutarını alacaklı veya borçlu hesaplarla eşleştirme) gerçekleştirmesi yeterli olmaktadır (Wang vd., 2018, s.4).

Özetle; blokzincir teknolojisine dayalı denetim süreci ile gerçek zamanlı sürekli denetim yapılabilmekte, birden fazla veri tabanına veri girme ve mutabakat ihtiyacını ortadan kaldırarak insan hatası riski azaltılabilmektedir (Kokina vd., 2017, s.96). Böylece muhasebe bilgilerinin daha anlaşılır olması, denetim sürecinin daha kolay, kısa ve düşük maliyetli olması sağlanmaktadır (Schmitz vd., 2019, s.336). Dolayısıyla blokzincir teknolojisi, denetim sürecinin etkinliğinin ve verimliliğinin artmasına katkıda bulunmaktadır.

#### **4.2.2 Otomatik Doğrulanabilir Kanıt Üretme**

Mali tablo denetiminin temel unsuru bir işlemin gerçekleştiğinin doğrulanması olup bu doğrulama, aynı zamanda kaydedilen işlemlerin ilgili, güvenilir, nesnel, doğru ve doğrulanabilir kanıtlarla desteklendiğine dair bir değerlendirmeyi de içermektedir (AICPA, 2017, s.9). Doğrulanabilir kanıt üretmek için ise denetçiler, belge incelemesi, mutabakatlar, örnekleme, iç kontrol testleri, analitik inceleme prosedürleri gibi yollarla hem muhasebe sisteminden hem de destekleyici belge, işlem ve çalışma kağıtlarından denetim kanıtı elde etmektedirler. Ancak geniş içeriklere sahip büyük miktardaki finansal veri içerisinde uygun ve yeterli denetim kanıtı oluşturulabilmesi uzun zaman alan ve maliyetli bir süreçtir.

Bu kapsamda blokzincir teknolojisi, zincire kayıtlı işlemlerin değiştirilemez, kurcalamaya dayanıklı ve izlenebilir yapısı sayesinde denetim sürecinde otomatik olarak denetim izi oluşturulmasını sağlamaktadır (COSO, 2020, s.6). Dolayısıyla; bir işlemin zincire kabul edilmesi, mali tablo iddiaları için yeterli ve uygun denetim kanıtının elde edilmesine ve işlemlerin gerçekliğinin otomatik olarak doğrulanmasına olanak tanımaktadır (AICPA, 2017, s.9). Sonuç olarak denetim sürecinin yürütülmesi için gereken maliyet ve zaman önemli ölçüde azaltılabilmektedir (Deloitte, 2016, s.3).

Bununla birlikte bir işlemin blokzincirinde yer almasının, defter ve kayıt amaçları açısından her zaman doğrulayıcı olmayacağına ilişkin eleştiriler de bulunmaktadır (COSO, 2020, s.6).

Bu bakış açısına göre zincire kaydedilen veriler gerçektir, ancak; (i) yetkisiz veya yasadışı bir işlem, (ii) ilişkili taraflar arasında imzalanan anlaşmalardan, (iii) zincir dışı yan anlaşmalardan veya (iv) finansal tablolarda yanlış sınıflandırmadan kaynaklanabilir (AICPA, 2017, s.10). Bu nedenle blokzincir teknolojisine dayalı bir kanıt toplama sürecinde, verilerin kendisinin kontrol edilmesinden ziyade, verilerin nasıl oluşturulduğunun ayrıntılı bir şekilde anlaşılması daha önemli hale gelmektedir (ACCA, 2017, s.32).

#### **4.2.3 Tüm İşlemlerin Denetimi**

Geleneksel denetim sürecinde, tüm işlemlerin incelenmesine ilişkin zaman ve maliyet kaynaklı insani sınırlamalar nedeniyle (ACCA, 2017, s.25) tüm işlemler arasından örnekleme yöntemiyle seçilen sınırlı sayıdaki kayıtlar ile denetim kanıtı toplanmakta ve bu örnekler üzerinden verilerin doğruluğu hakkında makul güvence elde edilmektedir. Buna karşılık blokzincir teknolojisinin dağıtık ve hash fonksiyonları ile birbirine bağlanan zincir yapısı sayesinde denetçiler, gözlem altındaki mevcut tüm işlem grubunu test edebilmekte; dolayısıyla örnekleme dayalı maddi testler işlevsizleşmektedir. Bu geniş kapsam, elde edilen güvence düzeyinin büyük ölçüde artmasını sağlamaktadır (Saifi, 2020, s.3).

Denetçi açısından değerlendirdiğimizde ise denetçinin artık örnekleme tekniklerini anlaması veya münferit işlemleri sorgulaması gerekmemektedir. Bunun yerine denetim sürecinde teknolojiyi sorgulama becerisi ve sistemde ya da verilerin kullanımında potansiyel sorunların nerede ve nasıl aranacağını bilme gerekliliği ön plana çıkmaktadır (ACCA, 2017, s.32).

#### **4.2.4 Denetim Risklerinin Azalması**

Denetim riski, *“finansal tabloların önemli bir yanlışlık içermesine rağmen, denetçinin duruma uygun olmayan bir denetim görüşü vermesi riskidir”* ve *“önemli yanlışlık”* riski ile *“tespit edememe”* riskini içeren bir kavramdır. Bu risklerin değerlendirilmesi, denetim sürecinde elde edilen yeterli ve uygun kanıtlara ve uygulanan denetim prosedürlerine dayanmaktadır. Önemli yanlışlık riskleri, iki ana düzeyde ortaya çıkmaktadır. İlk düzey, finansal tabloların genelinde bulunan risklerdir; bu düzeyde, finansal tabloların bir bütün olarak doğru ve güvenilir olup olmadığı ve yönetim beyanını etkileyen çok sayıda yanlışlık riski bulunup bulunmadığı değerlendirilmektedir. İkinci düzey ise işlem sınıfları, hesap

bakiyeleri ve açıklamalara yönelik yönetim beyanlarıyla ilgilidir. Bu düzeyde ise belirli işlemlerin, hesapların ve açıklamaların doğru bir şekilde raporlanıp raporlanmadığına dair riskler incelenir. Yönetim beyanlarına ilişkin riskler de yapısal (doğal) risk ve kontrol riski olarak ikiye ayrılmaktadır. Doğal risk, işletme ve çevresiyle ilgili faktörlerden kaynaklanan riskler iken; kontrol riski, iç kontrol sisteminden kaynaklanan risklerdir. Tespit edememe riski ise denetçinin, denetim riskini kabul edilebilir bir seviyeye indirmek için belirlediği prosedürlerin kapsamı, niteliği ve zamanlaması ile ilgili olan ve mevcut yanlışlığın tespit edilememesi riskidir (BDS 200, s.21-22). Blokzincir teknolojisine dayalı bir denetim süreci ise tanımlanan bu denetim risklerinin ortaya çıkma ihtimalini azaltma potansiyeline sahiptir.

Blokzincir teknolojisinde, bloklara kaydedilen işlemler ağın çoğunluk kararı sonucunda zincire eklenebilmekte ve dağıtık defter yapısı sayesinde herkesin erişimine açık bulunmaktadır. Bu özellikleri; denetim sürecinin, birden fazla, birbirinden bağımsız ve mutabakat gerektiren dahili ve harici kayıt veri tabanlarını ortadan kaldırarak zamanlama uyumsuzluklarını ve eksik veya hatalı kayıtlardan kaynaklanan işlem riskini azaltmaktadır (Saifi, 2020, s.3).

Ayrıca blokzincir teknolojisi ile işletmenin tüm verilerine erişerek gerçek zamanlı ve sürekli denetim yapılabildiğinden; denetçiler, işletmeyi daha iyi tanıyabilmekte ve denetim sürecini daha etkin bir şekilde yürütebilmektedirler. Böylece tespit edememe (bulgu) riski düzeyi düşürülebilmektedir (Kılınç, 2020, s.998).

Diğer yandan kurcalamaya karşı dayanıklılık, izlenebilirlik ve akıllı sözleşmeler aracılığıyla muhasebe ve raporlamada otomasyonun sağlanması kontrol riskinin azaltılmasına olanak tanımaktadır. Ancak finansal verilerde manipülasyonun zorlaşmasına rağmen firmaların verileri taklit ederek hile yapma riski hâlâ mevcuttur, bu nedenle yapısal riskte artış söz konusudur. Bu koşullar altında denetçilerin ana odağı, önemli yanlışlıkları önlemekten ziyade, denetlenen işletmenin faaliyetlerinin uygunluğu ve gerçekliğini analiz etmeye kayacaktır (Yu vd., 2018, s.44).

Ek olarak blokzincirin merkezi olmayan ve dağıtık yapısı, denetimin izleme, bilgi ve garanti verme gibi üç geleneksel rolünü üstlenme potansiyeline sahiptir. Bu nedenle blokzincir teknolojisi, sürekli güvence rolü aracılığıyla denetçilerin desteğiyle asimetrik bilgi riskini ve



ahlaki tehlikeyi azaltarak, asil ve vekil arasında gereken şeffaflığı sağlayacaktır (Chedrawi vd., 2018, s.12)

#### **4.2.5 Tasdik Hizmetlerinin Kolaylaşması ve Otomatik Vergi Denetimi**

Blokszincir teknolojisinin sağladığı doğru, gerçek zamanlı ve değiştirilemez kayıt özelliği, vergilendirme sürecini gerek muhasebe gerek mükellefler gerekse de devlet açısından önemli ölçüde dönüştürme potansiyeli taşımaktadır (Gül, 2019, s.193). Blokszincir teknolojisi, vergilendirme süreçlerini otomatikleştirerek tarhiyat, tebligat ve tahsilat işlemlerinin daha şeffaf ve hızlı yapılabilmesini sağlayacaktır. Örneğin; akıllı sözleşmeler aracılığıyla vergi beyannameleri otomatik olarak oluşturulabilecek, bu sayede mükelleflerin eksik veya hatalı bilgi girişi engellenerek hata oranı azaltılabilecektir. Ayrıca blokszincir üzerinden tebligat ile mükellefe veya vergi sorumlusuna tebliğ eş zamanlı olarak iletilebilecektir. Blokszincir sistemi, tahsilat işlemlerini de dijital finans sistemleriyle entegre ederek, örneğin kripto paralarla anında ödeme alınması sağlanarak, vergi kesintilerinin doğrudan hazineye aktarılmasını mümkün hale getirebilecektir (Carda, 2021, s.64-66).

Diğer yandan bildirimde bulunma, defter tutma, belge düzenleme, beyanname verme, saklama ve ibraz gibi mükellef ödevleri de blokszincir teknolojisi ile köklü değişikliklere uğrayacaktır. Örneğin bir mükellef işyerini kapatmak istediğinde, akıllı sözleşmeler aracılığıyla bu bildirim anında vergi idaresine iletilebilecek ve böylece işyeri kapanışının resmi kayıtlara geçmesi sağlanabilecektir. Blokszincirde mükellefin yaptığı her bir işlemin değiştirilemez ve eş zamanlı olarak dağıtık deftere kaydedilmesi, tüm kayıtların blokszincir üzerinden izlenebilir olması sayesinde, defter tutma ve belge düzenleme görevleri kısmen ortadan kalkmakla birlikte vergi idaresinin her türlü işlemde anında haberdar olması sağlanabilecektir. Bu hususta Çin'in Gachain sistemi, vergi kaçakçılığını engellemek için blokszincir tabanlı elektronik fatura sistemini başarıyla kullanmaktadır. Beyanname verme ödevi ise vergi beyannamelerinin otomatik olarak doldurularak vergi idaresine sunulması şeklinde gerçekleştirilebilecektir. Böylece vergi mükellefleri sadece onay vererek beyannameyi tamamlayabilecek ve vergi idaresi de sistem üzerinden verilerin doğruluğunu anında kontrol ederek uyumsuzlukları hızlı bir şekilde tespit edebilecektir. Bu amaçla blokszincir teknolojisinin kullanımına ilişkin Belçika ve Hollanda ülkelerinin uygulamaları mevcuttur. Son olarak saklama ve ibraz ödevi açısından değerlendirdiğimizde; mükelleflerin defter beratlarını ve mali mühürleri ibraz etme zorunluluğu ortadan kalkacak ve vergi

otoritelerinin blokzincir üzerinden mükelleflerin tüm defter ve belgelerine eş zamanlı bir şekilde erişebilmesi mümkün olacaktır (Carda, 2021, s.66-75).

Literatürde blokzincir teknolojisinin vergilendirme işlemlerinde kullanılmasına yönelik olarak, özellikle tevkifat yoluyla kaynakta ödenen vergi, Katma Değer Vergisi ve transfer fiyatlandırması yoluyla örtülü kazanç işlemlerinde sağlayacağı katkılar üzerinde durulmaktadır. Akıllı sözleşmelerle desteklenen blokzincir teknolojisine dayalı bir muhasebe sisteminde, personel bordrolarının düzenlenmesi ve tevkif edilen vergilerin ödenmesi işlemlerinin güvenilir ve doğru bir şekilde otomatik olarak yapılabilmesi sağlanabilecektir. Böylece işverenlerin, çalışan maaşlarından vergi ve sosyal güvenlik ödemelerinin hesaplanarak ilgili kurumlara aktarılmasına ilişkin aracılık sorumluluğu ortadan kalkacaktır. Bu kapsamda işverenin, personelin brüt maaşını sisteme girmesiyle vergi ve sosyal güvenlik hesaplamaları otomatik olarak yapılacak; ardından net maaş çalışanın hesabına, sosyal güvenlik kesintileri Sosyal Güvenlik Kurumu'na ve vergi de doğrudan Hazine'ye aktarılacaktır. Bu sistem, tevkifat işlemlerini daha hızlı, verimli ve düşük maliyetli hale getirerek parasal akışın verimli olmasına katkıda bulunacaktır (Deloitte, 2017, s.11).

Ayrıca blokzincir teknolojisi, dijital tedarik zincirlerinde tarafların fiili davranışlarını kaydederek, transfer fiyatlandırması politikalarının senkronize edilmesine ve grup içi kazançların belirlenmesine yardımcı olabilecektir. Akıllı sözleşmeler ve dağıtılmış defterler, tarafların faaliyetlerini gerçek zamanlı olarak izleyip, transfer fiyatlandırması ve vergi analizlerini doğrulamak için hukuki ve vergisel kanıt sunabilecektir. Böylece transfer fiyatlandırması yoluyla örtülü kazanç dağıtımı<sup>53</sup> riski gerçek zamanlı olarak incelenerek

---

<sup>53</sup>“Transfer fiyatlandırması, “ilişkili kişiler arasında yapılan mal veya hizmet alım ya da satımında uygulanan fiyat veya bedeldir.” Örtülü kazanç dağıtımı ise “kurum kazancının vergilendirilmeden kurum dışına aktarılmasıdır.” Bu tanımlamalardan hareketle, transfer fiyatlandırması yoluyla örtülü kazanç dağıtımı; “ilişkili kişilerin aralarında yaptıkları mal veya hizmet alım ya da satım işlemlerindeki fiyat veya bedeli, emsallerinden farklı tespit etmek suretiyle vergi matrahını aşındırmaları ve kurum kazancının vergilendirilmeden ortaklara veya diğer ilişkili kişilere aktarılmasıdır.” (GİB, 2010, s.2).

vergi mükelleflerinin işlemlerinin daha şeffaf ve doğru hale getirebilmesi sağlanacaktır (Asrav, 2019, s.259).

Son olarak blokzincir teknolojisi; KDV sisteminde tahsil edilen vergilerin doğrudan hazineye aktarılmasını ve KDV iadelerinin anlık bir şekilde yapılmasını sağlayabilecek, böylece KDV üzerinden yapılabilecek yanlış beyan, vergi kaybı ve kaçakçılığı önemli ölçüde azaltabilecektir. Ayrıca akıllı sözleşmeler sayesinde sınır ötesi işlemler ve sahte belgelerin tespiti daha kolay hale gelerek, KDV sistemindeki mevcut sorunlar çözülebilecektir (Asrav, 2019, s.261).

Vergi sürecinde blokzincir teknolojisi kullanımının olası avantajları doğrultusunda bazı ülkelerde uygulanabilirliğe ilişkin çalışmalarda bulunmaktadır. Örneğin, Çin hükümeti vergilendirme ve elektronik fatura düzenleme alanlarında blokzincir teknolojisinden yararlanılacağını ifade etmiştir. Finlandiya ise gayrimenkul ile ilgili vergileri takip etmek için blokzincir teknolojisi üzerinden bankalarla çalışmakta, ayrıca blokzincir teknolojisine dayalı bir KDV sistemi etkinliğini ölçen bir pilot proje yürütmektedir (Ağcakaya vd., 2022, s.67).

Blokzincir teknolojisi, özellikle dağıtık defter yapısı ve işlemlerin otomatikleştirilmesini sağlayan akıllı kodlama özellikleri ile vergi alanında kullanım için önemli bir potansiyel sunmaktadır. Vergi sistemlerinde idari yükün hafifletilmesi ve vergilerin daha düşük maliyetle toplanmasını sağlayan bir araç olarak kullanılması mümkündür. Ayrıca bu teknoloji, vergi açığının daraltılmasına ve dolandırıcılığın minimize edilmesine yardımcı olmak üzere de etkili bir şekilde uygulanabilecektir (Hoffman, 2018, s.1182). Özetle; blokzincir teknolojisi, muhasebenin vergilemeye dair bilgi üretme süreçlerini hızlandırarak güvenilirliğini artıracaktır (Gül, 2019, s.193). Bu sayede muhasebenin vergi yükümlülükleri, daha kolay yerine getirilirken; denetçilerin bu yükümlülüklerle ilişkin tasdik hizmetleri de kolaylaşacaktır. Böylece vergi denetimi daha verimli ve otomatik hale gelerek hem mükellefler hem denetçiler hem de vergi otoriteleri için daha hızlı ve güvenli bir sistem sağlanacaktır.

### **4.3 BLOKZİNCİR TEKNOLOJİSİNİN FİNANSAL BİLGİ MANİPÜLASYONU UYGULAMALARINA ETKİSİ**

Çalışmanın önceki bölümlerinde, blokzincir teknolojisine dayalı bir muhasebe ve denetim ekosisteminin uygulanabilirliği ve potansiyel özellikleri kapsamlı bir şekilde ele alınmıştır. Blokzincir teknolojisinin sağladığı merkeziyetsizlik, şeffaflık, izlenebilirlik, değişmezlik, kurcalamaya dayanıklılık, güvenilirlik, denetlenebilirlik, inkâr edilemezlik ve otomasyon özellikleri, finansal işlemlerin geleneksel kayıt, raporlama ve doğrulama süreçlerini önemli ölçüde dönüştürme niteliğine sahiptir. Bu değişen süreçler, daha hızlı ve etkili muhasebe uygulamaları ve denetim imkânı sunmanın yanı sıra finansal bilgi manipülasyonlarını azaltma, hatta önleme potansiyeli de taşımaktadır. Ancak henüz gelişme aşamasında olan bu teknolojinin muhasebe ve denetim alanında benimsenmesine yönelik olumlu görüşler olduğu kadar olumsuz eleştiriler de bulunmaktadır. Bu çerçevede çalışmanın bu bölümünde, blokzincir teknolojisinin finansal bilgi manipülasyonlarını önlemeye yönelik sunduğu fırsatlar ile teknolojinin uygulanması halinde karşılaşılabilecek tehdit ve riskler ele alınacaktır.

#### **4.3.1 Finansal Bilgi Manipülasyonlarını Azaltmaya Yönelik Avantajları**

Blokzincir teknolojisinin sağladığı şeffaflık, değişmezlik ve otomasyon özellikleri, finansal kayıtların güvenilirliğini artırarak, manipülasyon risklerini minimize etme potansiyeli ile dikkat çekmektedir. Bu bağlamda, blokzincir teknolojisinin muhasebe hata ve hilelerini azaltmaya yönelik sunabileceği avantajlar aşağıda maddeler halinde açıklanmaktadır:

- a. Muhasebe Bilgi Kalitesini Artırma: Muhasebecilerin mesleki yetersizlikleri, kişisel çıkarların etkisi, GKGMİ'ne ve yasal mevzuata uygunluk eksiklikleri, gerçek finansal verilerin gizlenmesi, muhasebe bilgi kalitesinin düşük olması vb. gibi etkenler objektif olmayan, gerçek dışı finansal raporların üretilmesine zemin hazırlamaktadır. Blokzincir teknolojisinin orijinal işlem bağlantısında ve muhasebe bilgi işleme bağlantısında iki katmanlı blokzincir teknolojisinin inşası yoluyla işlem bilgileri kaynaktan ve süreçten sağlamlaştırılmakta, böylece muhasebe bilgilerinin değiştirilmesi ve tahrif edilmesi imkânsız hale gelmektedir (Zheng, 2021, s.3-4). Bu durum, finansal bilgilerin gerçekliğinin ve güvenilirliğinin, dolayısıyla muhasebe bilgi kalitesinin büyük ölçüde artmasını sağlamaktadır (Yu vd., 2018, s.45).

- b. Hatalı İşlemleri Azaltma: Dağıtık defterde, işlemin kaydı ve işlem olayının kendisi aynı anda tetiklenir. (ACCA, 2017, s.24). Dolayısıyla işlem doğrulanarak gerçekleştiğinde, işlemin değiştirilemez kaydı da yapılmış olmaktadır. Bu değiştirilemez işlemlerin zincir üzerinde ortak bir deftere doğrulanarak kaydedilmesi işlevi, yüksek düzeyde otomatikleştirilmiş yapı ile birleştiğinde; finansal raporlama sürecinde insan müdahalesi azalmakta, böylece manuel hata ve kayıp riski düşmektedir. Diğer yandan mutabakat protokolünde ağırlık çoğunluğunun onayı ile işlemlerin doğruluğunun onaylanması sayesinde hataların tespit edilme olasılığı da artmaktadır (COSO, 2020, s.14).
- c. Hileli İşlemlerin Kolaylıkla Tespit Edilmesi: Blokzincir teknolojisinde mutabakat protokolü, işlemin meşru olduğunu doğrulamaktadır. İşlem blokzincirine zaman damgalı olarak dijital bir imza ile girmektedir. Blokzincir ağına paylaşılan genel defterde işlemin her iki tarafı için özdeş bir hash değeri bulunmaktadır. Denetçi işlemlerin doğruluğunu tespit etmek için blokzincirde eşit bir hash dizesi taraması yaptığında, eşleşen bir hash değeri bulamazsa, bu durum verilerin değiştirildiğine dair bir kırmızı bayrak belirteci olarak değerlendirilecektir. Çünkü uyumsuz bir hash değeri, verinin bütünlüğünün bozulduğuna dair bir göstergedir. Bu benzersiz hash değeri, şüpheli işlemlere ilişkin denetim kanıtı elde edilmesinde denetçilere önemli bir kolaylık sağlamaktadır (Giang vd., 2023, s.4).
- d. Belge Dolandırıcılığını Engelleme: Geleneksel muhasebe sisteminde bir işlemin yapıldığını kanıtlamak amacıyla yasal belgeler kullanılmaktadır. Ancak elektronik ortamda sahte belge düzenlemek ve düzenlenen belgeler üzerinde tahrifat yapmak ise oldukça kolaydır. Blokzincir teknolojisi ile işlemler ağırlık çoğunluk mutabakatı ile değiştirilemez şekilde kaydedilmektedir. Çoğunluk mutabakatı işlemin gerçekliğini doğrulamaktadır. Dolayısıyla blokzincir ağına gerçek olmayan bir işlem için sahte belge düzenlenmesi mümkün olmamaktadır. Diğer yandan gerçek bir işleme ait belgede değişiklik yapılmaması da hash fonksiyonları ile güvence altına alınmaktadır. Bu nedenle blokzincir teknolojisi, dijital ödeme yöntemlerinin güvenliğini, şeffaflığını ve doğruluğunu artırarak dijital belge sahteciliğini engelleme ve diğer dolandırıcılık risklerini azaltma imkânı sağlamaktadır (Giang vd., 2023, s.4).
- e. Varlıkların Kötüye Kullanımını Azaltma: Çalışan hileleri, satışların, alacakların ve iadelerin fazla veya eksik kaydedilmesi yoluyla nakdin çalınması veya alacaklı

değiştirme, sahte maaş ödemeleri ve hayalet çalışanlar gibi hileli harcamalar şeklinde varlıkların kötüye kullanımı olarak değerlendirilmektedir. Blokzincir teknolojisine dayalı bir sistemde, deftere herkesin erişebilmesi ve işlemlerin gerçekliğinin ağın mutabakatı ile doğrulanması, nakit giriş çıkışını etkileyen bu tür kötüye kullanımların gerçekleştirilmesini imkânsız hale getirmektedir. Diğer yandan blokzincir teknolojisi, nakit dışı hilelerden varlıkların şahsi kullanımı gibi durumların engellenmesi konusunda yeterli bir çözüm sunamayabilir; ancak stok hırsızlığı gibi nakit dışı hilelerin yapılmasını, tokenize edilen varlık hareketlerini izleyerek, kötüye kullanımı proaktif bir şekilde caydırma potansiyeline sahiptir (Wang vd., 2018, s.5).

- f. İlişkili Taraf İşlemlerinin Tespiti: Blokzincir teknolojisinin sağladığı gerçek zamanlı muhasebe, gözlemcilerin şüpheli varlık transferlerini ve çıkar çatışmalarını ifade eden diğer işlemleri anında tespit etme imkânı sağlayabilmektedir. Birçok ülke uygulamalarında, şüpheli varlık transferleri ve çıkar çatışmaları gibi ilişkili taraf işlemlerinin beyan edilmesi, yönetimin yükümlülüğündedir. Ancak hangi işlemlerin beyan gerektirecek kadar önemli olduğu konusundaki farklı bakış açıları, beyanlarda uyumsuzluklara neden olmaktadır. Blokzincir teknolojisinin sağladığı gerçek zamanlı muhasebe, söz konusu ilişkili taraf işlemlerini tespit etme imkânı sağlayabilmektedir. Blokzincir teknolojisinin sağladığı şeffaflık, içeridekilerin varlıkları firma dışına çıkarma kabiliyetlerini azaltmakta ve kreditorlerin, mali açıdan sıkıntılı firmaların yöneticileri tarafından yapılan hileli devirlere karşı gerçek zamanlı gözetim yapmalarına imkân sağlamaktadır (Yermack, 2017, s.25). Ayrıca işletmelerin çok sayıda bireysel işlemi kamuya açıklamak zorunda kalmaları halinde akıllı sözleşmeler ile bu sürecin otomatikleştirilmesi de mümkün olabilmektedir.
- g. Bilgi Asimetrisini Azaltma: Muhasebe araştırmalarında, vekâlet teorisi "firmayı yöneten yöneticiler ile dış yatırımcılar arasında potansiyel bilgi asimetrilerine yol açan belirsizlik koşullarını" vurgulayan bir yaklaşımdır (Walker, 2013, s.448). Bilgi asimetrisi ise bilginin gizli tutulması, saklanması veya bir karar veya işlemin sonucunu etkilemek için yöneticiler tarafından stratejik olarak açıklanması durumunda ortaya çıkmaktadır (Williamson, 1979). İşletme yöneticileri, sahip oldukları çok fazla bilgiyi kendi çıkarlarını maksimize etmek amacıyla manipülasyon yapmada kullanabilmektedirler. Dolayısıyla bilgi asimetrisi, etik riskler yaratarak birçok küresel finansal skandala

sebebiyet vermektedir. Bu bağlamda blokzincir teknolojisi, şeffaflık, değiştirilemezlik ve hesap verebilirlik özellikleri sayesinde bilgi asimetrisini ve temsilcilik sorunlarını azaltmak için muhasebe verilerini kontrol etme ve izleme konusunda yenilikçi bir çözüm yaratma potansiyeline sahiptir. Ayrıca yapay zekâ teknolojisi yardımıyla olası anormallikleri belirleme imkânı sağlanırken; akıllı sözleşmelerle süreçler otomatikleştirilerek, yönetsel manipölasyonun ve fırsatçı davranışların azaltılması imkânı da sunulmaktadır (Han vd., 2023, s.5).

- h. Kazanç Yönetimini Azaltma: Geleneksel muhasebe uygulamalarında, kayıt, sunum ve açıklama süreçleri muhasebe ilkelerine uygun olmalıdır. Yine de işletmelerin, muhasebe politikaları, tahminleri ve yargıları gibi bazı muhasebe yöntemlerini belirleme konusunda takdir yetkileri bulunmaktadır. Bu takdir yetkilerine dayalı finansal tabloları hazırlarken izledikleri muhasebe süreçlerini ise açıklamadan, yalnızca nihai finansal raporları dış kullanıcılara sunmaktadırlar. Bu durum, şirketlerin bazı bilgilerini gizli tutabilmelerini sağlamakta ve kişisel çıkarlar doğrultusunda manipölasyon yapılabilmesine olanak yaratmaktadır (Yu vd., 2018, s.42). Blokzincir teknolojisine dayalı bir muhasebe sistemi sayesinde ise muhasebe standartları ve varsayımlar akıllı sözleşmelere kodlanarak kaydetme ve raporlama süreci otomatikleştirilebilecek ve böylece yöneticilerin takdir yetkisi devre dışı bırakılabilecektir. Ayrıca sağladığı şeffaflık ile bilgi kullanıcıları, izlenen muhasebe politikaları hakkında bilgi sahibi olabileceklerdir.

Bununla birlikte blokzincir dağıtık defterinde işlemin dijital kaydı, işlemin kendisine sıkı sıkıya bağlıdır. Yani bir işlem olayı ve o işlemin kaydı eşzamanlı gerçekleşmektedir. Bu durum; bir hesap dönemine ait olmayan bir işlemin, başka bir döneme (önceki veya sonraki) ait kayıtlarda gösterilmesini imkânsız hale getirmektedir (ACCA, 2017, s.24). Dolayısıyla blokzincir teknolojisinin sağladığı gerçek zamanlı muhasebe, firmaların raporlanan kazançları manipüle etmek için muhasebe hilesi yapma fırsatlarını büyük ölçüde azaltma potansiyeli yaratmaktadır. Geri döndürülemez, zaman damgalı işlemler sayesinde yöneticilerin, satış sözleşmelerini sonraki bir raporlama dönemine ertelemek ya da hemen giderleştirilmesi gereken işletme giderlerini amortismanına tabi tutarak gelecek dönemlere aktarmak gibi stratejileri uygulayabilmeleri mümkün olmamaktadır (Yermack, 2017, s.25).

Diğer yandan işletmenin finansal tablo hilesi yapması durumunda ise blokzincir teknolojisine dayalı muhasebe bilgi sisteminde ilgili tüm işlemlerin kayıtlarına erişilebildiğinden, muhasebe usulsüzlüklerini gösteren geçerli kanıtlar elde edilebilmektedir. Örneğin, satış gelirlerinin muhasebeleştirilmesinden önce tüm şartların yerine getirildiğinden emin olmak için akıllı sözleşmelere muhasebeleştirme kriterleri tanımlanabilmekte ve anormal yüksek hacimli bir yılsonu satışından hemen sonra yüksek bir getiri oranının gerçekleşmesi durumunda sistemin uyarı vermesi şeklinde bir kodlama yapılabilmektedir (Wang vd., 2018, s.6).

Ek olarak finansal tablo sunumundaki gecikmeler, muhasebenin zorluğu veya kötü finansal yönetim gibi "teknik" nedenler sonucu olabilmekteyken, yönetimin takdir yetkisini kullanarak özellikle geciktirmesinden de kaynaklanabilmektedir. Takdir yetkisinin kullanılarak finansal tablo sunumunun geciktirilmesi, çoğunlukla zarar veya yüksek borçluluk durumunun yatırımcılar üzerindeki olumsuz etkisini dağıtmak amacıyla uygulanmaktadır (Potekhina vd., 2017, s.18). Blokzincir teknolojisi ile yatırımcılar istedikleri an kendileri gerçek zamanlı ve otomatik olarak finansal tablo elde edebildiklerinden bu şekilde yönlendirmelerden ve manipülasyonlardan korunarak daha şeffaf ve güvenilir bilgilere ulaşabilmektedirler.

Bir başka olası etkisi ise menkul kıymetler borsası dolandırıcılığına yöneliktir. Blokzincir teknolojisi, yönetici sahipliğini son derece şeffaf hale getirmekte ve böylece içerden alım ve satımların gerçek zamanlı ve otomatik olarak tespit edilebilmesine imkânı tanımaktadır. Ayrıca kurumsal oylamanın daha şeffaf, doğru ve hızlı olmasını da sağlamaktadır (Wang vd., 2018, s.6).

- i. Yasa Dışı ve Etik Dışı Faaliyetlerin Engellenmesi: Blokzincir teknolojisinin dağıtık defter yapısı, işletme yönetiminin muhasebe kayıtları üzerindeki nihai yetkisini devre dışı bırakmakta böylece muhasebe sahtekarlığı ve veri manipülasyonu önlenmektedir. Dolayısıyla birçok etik dışı ve yasadışı faaliyetin gerçekleştirilmesi de çok zor hatta imkânsız hale gelmektedir. Örneğin, birçok teşvik sistemi, yöneticinin tazminatının bir kısmını hisse senedi veya opsiyon vererek hisse fiyatı performansına bağlamaktadır. Bu opsiyon teşvik planları, hissedarların zararına yöneticilere kişisel kazanç sağlamada kullanılma potansiyeli taşımaktadır. Bu kapsamda opsiyonların, fiyatın en düşük olduğu tarihi seçmek için geriye dönük olarak kullanılması bilinen bir uygulamadır, ancak yasa



dışı bir manipölasyondur. Blokzincir teknolojisine dayalı bir sistemde ise geriye dönük işlem yapmak pratikte imkânsız olduğundan opsiyon teşvik planlarının yasadışı şekilde kullanılması engellenebilmektedir. Diğer yandan blokzinciri defterlerinin yüksek düzeyde şeffaf olması ve şirket hakkındaki hayati bilgileri hissedarlarına sunarak yönetimin daha fazla hesap verebilir olmasını sağlaması sebebiyle etik dışı faaliyetlerin önlenmesine de katkıda bulunmaktadır (Potekhina vd., 2017, s.38). Ayrıca blokzincir teknolojisinin bu şeffaflık özelliği, düzenleyiciler ve firma yönetimi arasındaki yolsuzluk veya rüşvet davranışı fırsatlarını da azaltma potansiyeli sunmaktadır (Wang vd., 2018, s.6).

#### **4.3.2 Finansal Bilgi Manipölasyonlarına Yönelik Yeni Tehdit ve Riskler**

Henüz gelişme aşamasında olan blokzincir teknolojisinin, finansal bilgi manipölasyonlarını azaltmasına yönelik olumlu görüşler olduğu kadar yeni manipölasyon yöntemleri geliştirileceğine dair olumsuz eleştiriler de bulunmaktadır. Bu bağlamda blokzincir teknolojisinin muhasebe ve denetim süreçlerinde kullanılmasının finansal bilgi manipölasyonlarına yönelik yaratabileceği olası yeni tehdit ve riskler aşağıda maddeler halinde açıklanmaktadır:

- a. İşlem Kaynağının Gerçekliği Riski: Blokzincir teknolojisi, işlem biçimlerinin otomatik olarak doğrulanmasını sağlamasına rağmen ilgili dijital kaydın dayandığı verilerin gerçek olduğunu göstermemektedir (CPA Canada, 2016, s.19). Bir başka deyişle bir varlık transferinin blokzincirine kaydedilmiş olması, gerçek dünyada varlığın transfer edildiğini veya takas edildiğini, ödemelerin yapıldığını ve işlemlerin kaydedildiğini garanti etmemektedir (Schmitz vd., 2019, s.335). Ayrıca blokzincir teknolojisinin doğrulama mekanizması, çifte harcamayı önlemekle birlikte muhasebe açısından işlemlerin geçerliliği için yeterli bir doğrulama sağlamamaktadır. Bu kapsamda blokzincir üzerindeki bir varlık transferinin tarafları arasındaki anlaşma hakkındaki bilgiye erişilememektedir (Coyne vd., 2017, s.109). Örneğin blokzincire, bitcoin ile bir şey satın alındığı kaydedilebilmekte, ancak bunun bir araba mı yoksa bir hediye mi olduğu hakkında bilgi sahibi olunamamaktadır (Giang vd., 2023, s.5). Ek olarak blokzincir, verileri depolarken altta yatan destekleyici belgeleri saklayamamaktadır (CPA Canada, 2016, s.19) ve dijital para, yanlışlıkla veya kasıtlı olarak yanlış veya yetkisiz bir alıcıya gönderildiğinde, işlemin geri alınması da mümkün olmamaktadır

(Saifi, 2020, s.4). Bu durum işlemin başlangıcından itibaren hileli olması riskini doğurmakta; ancak böyle bir hile, değiştirilemez hile olarak kayıtlarda görünmektedir. Dolayısıyla blokzincir teknolojisi ile dolandırıcılıkların tamamen engellenebilmesi mümkün olmasa da gerçek zamanlı olarak tespit edilmesine imkân tanınmaktadır (Schmitz vd., 2019, s.336). Bu noktada işlem gerçekleşmeden önce yapılması gereken doğrulamalar önem kazanmaktadır (Saifi, 2020, s.4).

- b. Akıllı Sözleşmelerin Hatalı Kodlanması Riski: Akıllı sözleşmeler, muhasebe ve denetim sürecinde otomasyonu sağlayarak finansal bilgi manipülasyonu risklerini azaltma potansiyeli taşımaktadır. Ancak aynı zamanda da risk unsurunun bir parçasıdır. Bunun nedeni akıllı sözleşmelerin blokzincir içindeki bir kod parçası yani bir program olmasından dolayı yanlış geliştirilmeleri veya manipüle edilmeleri halinde geçersiz ve yanlış işlemlerin otomatik olarak yürütülmesine ve kaydedilmesine sebebiyet verecek olmasıdır. Akıllı sözleşmeler, bir kez uygulamaya konulduğunda kendi kendilerini yürüttüklerinden ve işlemlerin de geri dönüşü olmadığından dolandırıcılık amacıyla olası bir hatalı kodlama durumunda büyük kayıplara yol açabileceklerdir (COSO, 2020, s.11-12). Bu kapsamda blokzincir teknolojisine dayalı muhasebe ve denetim süreçleri akıllı sözleşmeler ile otomatik olarak yürütülüyorsa, akıllı sözleşme kodlarının doğrulanması için bir güvence sağlayıcıya da ihtiyaç olacaktır (Ünkaracalar, 2021, s.21).
- c. İşletme Varlıklarının Kaybedilmesi Riski: Bir blokzincir ağında işlem yapılabilmesi için kripto cüzdan sahibi olunması gerekmektedir. Kripto cüzdanlar ile hem işlem yapılmakta hem de temsil ettiği varlıklara erişim sağlanmaktadır. Kripto cüzdan sahibinin kimlik doğrulanması da özel anahtar ile yapılmaktadır. Özel anahtarın ise saklandığı merkezi bir sistem bulunmamaktadır. Dolayısıyla blokzincirde dijital varlıkların kontrolü özel anahtara sahip olanlar üzerinden sağlanmaktadır ve kaybedilmesi halinde varlıklara tekrar erişilmesi mümkün olmamaktadır. Bu kapsamda işletmenin dijital varlıklarına erişim sağlanabilmesi, işletmenin özel anahtarının korunmasına ve kontrolüne bağlı bulunmaktadır. Özel anahtarlar üzerinde uygun kontrollerin olmaması, işletme varlıklarının kaybedilmesi veya kötüye kullanılması riskini yaratmaktadır (COSO, 2020, s.11).
- d. İşletme Mahremiyetinin Tehlikeye Girmesi: Blokzincir teknolojisi, merkezi olmayan yapısı ile kullanıcı kimliklerinin isteğe bağlı ifşası için mahremiyeti sağlamakla birlikte,

işlemlere ilişkin yüksek derecede şeffaflık sunmaktadır. Dolayısıyla blokzincirde ifade edilen mahremiyet bireylere yönelik olup işletmeleri özellikle halka açık işletmeleri kapsamamaktadır (Tapscott, 2016 Akt. Potekhina vd., 2017, s.18). İşletmeler için mahremiyet ise özellikle finansal veri gizliliği ve ticari sırların korunması söz konusu olduğunda büyük önem taşımaktadır. Ancak halka açık bir blokzincirde, tüm katılımcılar, her bir işlemin kopyasına sahip olduklarından işletme mahremiyeti tehlikeye girmektedir. Bu risk dolayısıyla özel (izinli) blokzincir<sup>54</sup> geliştirilmiştir. Diğer yandan özel blokzincir nispeten kapalı, güvenli bir iş ortamı sağlasa da yöneticilerin blokzincir üzerinde tam kontrole sahip olması nedeniyle kurcalamaya karşı direnci sınırlayabilecek veri şeffaflığından ve kamu katılımından ödün vermektedir. Bu nedenle yönetimin işlem verilerini kişisel kazanç için manipüle edebilmesi durumunda özel blokzincir kurcalamaya karşı direnci garanti edememektedir (Wang vd., 2018, s.2). Bu kapsamda karşılaşılabilecek riskleri; halka açık bir blokzincir için, işletmenin tescilli bilgisinin herhangi biri tarafından görüntülenerek yüksek mülkiyet maliyeti riski yaratması (Yu vd., 2018, s.43); izinli bir blokzincir için ise gizli anlaşma riskini doğurması (Barandi vd., 2020 Akt. Selg, 2023, s.35) olarak örneklendirebiliriz. Dolayısıyla işletmelerin, kurcalamaya karşı direnci azalmış özel bir blokzinciri ile mahremiyet ihlali riskine maruz kalan halka açık bir blokzincir arasında bir seçim yapması gerekmektedir (Wang vd., 2018, s.2).

- e. Güvenlik İhlali Riski: Blokzincir teknolojisi veri güvenliğini mutabakat mekanizmaları ile sağlamaktadır. Genel blokzincirde mutabakat mekanizması<sup>55</sup>, ağ katılımcılarının çoğunluğunun doğrulamasına göre zincire veri kaydedilmesi şeklinde işlemektedir. Dolayısıyla ağ katılımcılarının %51'ini kontrol eden bir hilekarın varlığı halinde dijital varlıkları çalmak için muhasebe verileri değiştirilebilmekte veya blokzincir manipüle edilebilmektedir (Selig, 2023, s.35). Bu kapsamda %51 gücüne sahip olan bir yönetici, kurumsal bilgi ifşası hisse senedi fiyatını etkilemede önemli olduğundan, hisse senedi fiyatını manipüle etmek ve tek seferlik kar elde etmek için blokzincire yanlış bilgi ekleyerek finansal bilgi manipülasyonu fırsatı elde edebilmektedir (Yu vd., 2018, s.43). Diğer yandan %51 riskini bertaraf etmek için halka açık değil de özel blokzincir tercih

---

<sup>54</sup> “Blokzincir türleri” hakkında detaylı bilgi için bkz. s.100.

<sup>55</sup> “Mutabakat mekanizması” hakkında detaylı bilgi için bkz. s.40.

edilmesi halinde ise bu sefer mutabakat üzerinde %100 kontrole sahip olunmaktadır. Ayrıca genel blokzincir tercih edilmesi durumunda karşılaşılan bir diğer risk ise muhasebe işlemlerinin doğrulanması için gereken bilgi ve yetenek dolayısıyla ortaya çıkmaktadır. Buna göre ağ katılımcıları yeterli bilgiye sahip olmadıklarından mutabakat sürecine katılmaktan imtina edip ağ kontrolünün çoğunluğunu firmaya bırakacaklar ve böylece yine özel blokzincirde karşılaşılan risk ortaya çıkacaktır (Coyne vd., 2017, s.109). Dolayısıyla blokzincir teknolojisinin mutabakat mekanizması, finansal bilgi manipülasyonu yapılmasını zorlaştırmakta, ancak güvenlik ihlali riskinin varlığı sebebiyle tamamen engelleyememektedir.

- f. Anonimliğin Yarattığı Yasadışı İşlem Riski: Blokzincir teknolojisi, şeffaflık ve geriye dönük işlem yapılamazlık özellikleriyle yasadışı faaliyetleri zorlaştırırken; aynı zamanda bünyesinde barındırdığı asimetrik şifreleme tekniği (dijital imza) sayesinde kullanıcı kimliklerine sağladığı anonimlik ve gizlilikle bu faaliyetleri kolaylaştırma riski de taşımaktadır. Bu kapsamda tarafların anonimliği, gizli anlaşma fırsatlarını artırabilmektedir (COSO, 2020, s.12). Ayrıca blokzincirin merkeziyetsiz yapısı, tarafları eylemlerinden sorumlu tutacak merkezi bir aracı, sistem veya gözetim organının olmamasına, yani "dükkâna bakan kimsenin olmamasına" yol açmaktadır. Dolayısıyla yasadışı bir faaliyet tespit edildiğine, anonim kimliklerin belirlenmesi için başvurulacak bir merci bulunmadığından, hesap verilebilirlik engellenmektedir. Bu durum da yönetim açısından ciddi bir tehdit meydana getirmektedir (COSO, 2020, s.8).

#### **4.4 BLOKZİNCİR TEKNOLOJİSİNE GEÇİŞİN SEKTÖRE ETKİLERİ**

Blokzincir teknolojisi, işletmelerin muhasebe ve denetim süreçlerini köklü bir şekilde dönüştürme potansiyeli taşıyan bir yenilik olarak öne çıkmaktadır. Dağıtık defter yapısı, değiştirilemezlik ve şeffaflık özellikleri sayesinde, finansal bilgi kalitesini artırarak, muhasebe sahtekarlıklarını ve veri manipülasyonlarını azaltma imkân sunmaktadır. Bununla birlikte teknolojinin gelişimi halen devam etmekte olup, aşılması gereken teknik, düzenleyici ve operasyonel zorluklar bulunmaktadır. Bu zorlukların, blokzincir teknolojisinin tam potansiyeline ulaşmasını engellemesi ve sektörün bu teknolojiyi benimseme sürecini yavaşlatması mümkündür. Dolayısıyla ilgili kapsamda çalışmanın bu bölümünde; blokzincir tabanlı uygulamaların muhasebe ve denetim sektörüne olası etkileri, işletmeler, meslek profesyonelleri ve kamu perspektifinden değerlendirilmektedir.

#### 4.4.1 İşletmelere Etkisi

Blokzincir teknolojisi, sunduğu merkeziyetsiz, değiştirilemez ve otonom işleyiş özellikleriyle işletmelerin ilgisini çekmekte ve bu doğrultuda yoğun bir şekilde geliştirilmeye devam edilirken aynı zamanda önemli ölçüde finansal destek ve sermaye akışı sağlamaktadır. Bu bağlamda muhasebe ve denetim süreçlerinde blokzincir teknolojisinin benimsenmesinin, işletmelere dört olumlu etkisinin olması beklenmektedir. Bunlar (Tyra, 2014; CA ANZ, 2017, s.31):

- a. İlk olarak, denetçiler finansal tabloların doğruluğunu hızlı ve kolay bir şekilde doğrulayabileceğinden, denetim maliyetleri ve süresi önemli ölçüde azalacaktır. Denetimler hala gerekli olsa da denetçiler daha yüksek riskli alanlara odaklanabilecekler, bu da denetim verimliliğini artıracaktır.
- b. İkinci olarak, şirketin finansal tablolarının bütünlüğü neredeyse tartışmasız olacaktır, çünkü işlemler, geçerli bir şifreli imza gerektirdiği için tahrif edilememektedir. Bu durum, sahte faaliyetleri engelleyecek ve manipülasyon maliyetlerini azaltacaktır. Sonuç olarak bu iyileştirmeler şirketlerin hisse senedi fiyatları, borçlanma oranları ve diğer finansal göstergeleri üzerinde olumlu bir etki yaratacaktır.
- c. Üçüncü olarak, işletmelerde operasyonel sadeleştirmeyi sağlayacaktır. Mükerrer ve manuel işlemlerin azalmasını sağlayarak, verimliliği artıracak ve maliyetleri düşürecektir. Ayrıca işletmelerin daha fazla katma değer yaratan görevlere odaklanabilmesi için yeni fırsatlar yaratacaktır.
- d. Ve son olarak, tedarik zinciri boyunca güveni artırarak ilişkilerin gelişmesine katkı sağlayabilecektir. Yeni veya bilinmeyen müşterilerle iş yapan işletmeler, karşı taraf riskleri ve ödeme süreleri gibi sorunlarla karşılaşabilmektedir. Blokzincir, bu riskleri azaltarak, ödeme sürelerini kısaltabilecek ve sermaye bağlanmasını engelleyerek nakit akışını iyileştirebilecektir. Bu da bilanço verimliliğinin artmasını sağlayacaktır.

Diğer yandan tüm yoğun geliştirme çalışmalarına, ilgiye ve yatırımlara rağmen blokzincir teknolojisinin işletmeler açısından yaygın olarak benimsenmesinin önünde hala aşılması gereken teknik, organizasyonel ve yasal zorluklar bulunmaktadır. Örneğin, depolama kapasitesi, enerji tüketimi, ölçeklenebilirlik, gizlilik, siber güvenlik, birlikte çalışabilirlik,

(Buterin, 2014; Gilbert, 2016; Bertino vd., 2019; O'Leary, 2019), kurumsal hazırlık, üst yönetim desteği, yönetim sorunları, fonlara erişim, teknik yeterlilik, (Clohessy ve Acton, 2019; Coyne ve McMickle, 2017) ve blokzincir standardizasyonunun eksikliği (Guo ve Liang, 2016; Hughes vd., 2019) en çok üzerinde durulan zorluklardır (Han vd., 2023, s.12).

Bununla birlikte muhasebe ve denetim süreçleri açısından blokzincir teknolojisinin benimsenmesinin, işletmeler üzerinde dört olumsuz etkisinin olması beklenmektedir. Bunlar (Yu vd.,2018, s.43; Potekhina vd., 2017, s.16; Han vd., 2023, s.12).

- a. Veri büyüklüğü ve yüksek maliyetler: Mevcut blokzinciri teknolojisi, firmaların muhasebe verilerinin büyüklüğünü yönetmekte zorluk yaşayabilir ve yüksek faturalama ücretleri nedeniyle maliyetler önemli ölçüde artar. Bu da teknolojiye geçiş yapmak isteyen firmalar için ciddi bir finansal yük oluşturur.
- b. Bilgi ifşası ve mülkiyet riskleri: Blokzincirinin kalıcılığı ve şeffaflık özellikleri, tescilli bilgilere sahip firmaların mülkiyet maliyetlerini artırabilir. Bilgilerin ifşası, ticari sırların sızdırılmasına yol açarak firmaların faaliyetlerini olumsuz etkileyebilir, bu da firmaların blokzincirini benimseme konusunda tereddüt etmelerine neden olabilir.
- c. Güvenlik ihlali riski: Ağ erişiminin herkese açık olması ve katılımcıların anonimliği, düzenlemeyi zorlaştırmakta ve %51 saldırısı gibi güvenlik açıklarına yol açmaktadır. Bu durum, katılımcıların hisse senedi fiyatlarını manipüle etmesine ve yanlış bilgi eklemesine olanak tanıyabilir, bu da şirketlerin blokzincirini kullanma konusunda çekincelerine yol açar.
- d. Geleneksel sistemler ile entegrasyon sorunu: Blokzincir teknolojisi, çoğu geleneksel iş modeliyle uyumsuz olabileceğinden, bu teknolojiyi entegre etmek isteyen işletmelerin, entegrasyon sürecinin verimli ve sürdürülebilir olabilmesi için gerekli altyapı ve iş süreçlerini yeniden yapılandırmaları gerekmektedir. Bu durum, maliyet artışlarına ve finansal yüklerin daha da ağırlaşmasına yol açabilir.

Özetle; kısa vadede tüm firmaların muhasebe ve denetim süreçlerini blokzincir teknolojisine dayalı olarak yürütmesi öngörülmemektedir. Ancak teknoloji olgunlaştıkça bu zorlukların aşılması mümkündür. İşletmeler, finansal bilgilerini ifşa etmenin maliyet ve faydalarını değerlendirerek uygun blokzincir türünü seçip, bilgi asimetrisini azaltarak sermaye

maliyetlerini düşürebilirler. Bu durum, daha fazla işletmenin blokzincir platformlarını gönüllü olarak kullanmasını teşvik edecektir (Yu vd., 2018, s.43).

#### **4.4.2 Meslek Profesyonellerine Etkisi**

Blokzincir teknolojisi, sunduğu dağıtık, değiştirilemez, kurcalamaya dayanıklı ve otonom işleyiş özellikleriyle muhasebe ve denetim süreçlerinde otomasyon sağlayarak meslek profesyonellerinin sorumluluklarının ve yetkinliklerinin doğasını değiştirme potansiyeline sahiptir. Bu kapsamda blokzincir teknolojisi ile mali müşavirlerin görevi, işlemleri kaydetmek ve finansal tablo düzenlemekten, kaynak belgelerin gerçekliğini ve muhasebe blokzincirinde kullanılan akıllı sözleşmelerin tekrarlanabilirliğini sağlamaya doğru değişecektir. Denetçilerin görevini ise işletmelerin büyük yanlış beyanlarını tespit etmekten, ticari işlemlerin ve olayların makullüğünü ve gerçekliğini analiz etmeye kaydıracaktır (Yu vd., 2018, s.38)

Ayrıca muhasebecilerin, muhasebe veri tabanının 'sahibi' olma rolleri de (Kroon vd., 2021, s.10) strateji geliştirme ve derinlemesine analiz gibi daha değerli faaliyetler üzerinde uzmanlıklarını ifa etmeye dönüşecektir. Dolayısıyla blokzincir teknolojisi muhasebecilerin veya denetçilerin yerini tamamen almayacak, gerçeğe uygun değer muhasebesinin ne olduğuna karar vermek, maddi olmayan varlıkları değerlendirmek, amortismanı değerlendirmek ve kiralama türlerini ayırt etmek vb. gibi yetkinlikleri ön plana çıkararak zamanlarını daha verimli alanlarda harcamalarını sağlayacaktır (Han vd.,2023, s.12).

Diğer yandan blokzincir teknolojisi ile kayıtlara yanlış veri girişi ve kayıtların silinmesi mümkün değildir. Bu durum, finansal verilerin istikrarını sağlamakla birlikte; muhasebe uygulayıcılarına, yöneticiler, ortaklar ve diğer kişiler tarafından gelen müdahaleleri engelleyecektir. Böylece muhasebe personelinin bağımsızlığını sağlayarak, meslek etiğine aykırı davranmak zorunda bırakılmasının önüne geçilecektir (Shi, 2021, s.89).

Ek olarak çevrimdışı ödemelerle ilgili olarak blokzincir teknolojisini kullanan şirketlerin işlemin gerçek dünyada gerçekleştiğine dair kesin bir garantileri bulunmamaktadır. Ancak muhasebe uzmanları bu durumu, blokzincir tarafından kaydedilen işlemler ile gerçek ödemeleri uzlaştıracak mekanizmaları araştırarak çözebilecekleri önemli bir fırsat olarak değerlendirebilirler (Schmitz vd., 2019, s.336).

Bununla birlikte blokzincir teknolojisinin yeniliği ve karmaşıklığı, yetkin personel bulmanın zor olmasına ve yetkinlik taahhüdünün garanti edilmesinin veya değerlendirilmesinin zor olmasına sebep olacaktır (COSO, 2020, s.9). Bu kapsamda muhasebe uzmanlarının bu değişikliklere ayak uydurmak, rekabetçi kalabilmek ve müşterilere daha iyi hizmet sunabilmek için teknolojiyi öğrenmesi ve blokzincir tabanlı süreçlere uyum sağlaması gerekecektir (Liu vd., 2024, s.13).

#### **4.4.3 Kamuya Etkisi**

Blokzincir teknolojisinin, muhasebe ve denetim sektörüne olası etkilerine kamu (devlet) perspektifinden yaklaştığımızda; düzenleyiciler, vergi, ihtiyati önlemler ve kurumsal uyum gibi işlemlerin yanı sıra sağlanan verilerin geçerliliğinden ve bütünlüğünün bozulmadığından emin olmak istemektedirler. Blokzincir teknolojisi de veri güvenliği ve bütünlüğüne ilişkin garanti sağlarken dolandırıcılık ve sahtecilik fırsatlarını da zor hale getirmektedir. Dolayısıyla düzenleyiciler, blokzincir teknolojisi sayesinde daha detaylı gözetim yapma imkânı sağladıklarından, olası belirsizlikler azaltılacak veya ortadan kaldırılacak ve böylece anlaşmazlık riskleri minimize edilebilecektir. Ayrıca verilere gerçek zamanlı olarak erişilmesi, düzenleyicilerin daha hızlı tepki vererek, daha etkin kararlar almalarını da sağlayacaktır (CA ANZ, 2017, s.31).

Bununla birlikte nakit para kullanımının olmadığı, tüm parasal işlemlerin dijital ortamda gerçekleştiği bir sistemde, blokzincir platformu üzerinde çalışan akıllı sözleşmeler sayesinde vergi hesaplaması ve tahsilatı gerçek zamanlı ve doğru bir şekilde yapılabilecektir. Dijital ortamda işleyen bu süreçler ile vergi kaçırma olasılığı azaltılabilecek, kayıt dışı ekonomi ortadan kaldırılabilir ve vergi toplama işlemi daha hızlı ve düşük maliyetli hale getirilebilecektir (Kılıç, 2020, s.20). Örneğin; bir satış işleminde KDV oranı akıllı sözleşmeler aracılığıyla otomatik olarak hesaplanarak doğrudan vergi idaresinin kripto cüzdan adresine gönderilebilecek veya KDV iade işlemleri herhangi bir rapora bağlı olmadan aynı hızla gerçekleştirilebilecektir (WU/New Economy Taxation Team, 2017 Akt. Ulucan Özkul vd., 2020, s.232).

Diğer yandan teknolojinin sağladığı daha fazla şeffaflık, düzenleyiciler ve düzenlemeye tabi kuruluşlar arasındaki iş birliğinin artmasını da sağlayacaktır. Özellikle finansal piyasalar



açısından, düzenleyicilerin, finansal piyasaların yasallığını, güvenliğini ve istikrarını sağlama görevlerini daha iyi yerine getirebilmeleri mümkün olacaktır (CA ANZ, 2017, s.33).

Bu avantajlarının yanı sıra blokzincir teknolojisinin belirsiz yasal çerçevesi ve hükümet düzenlemeleri teknolojiinin benimsenmesi önünde önemli bir zorluk teşkil etmektedir. Özellikle blokzincir çözümleri için gerekli olan kripto para birimlerinin yasal bir değişim aracı olarak tanınması için düzenleyici çerçevelerin ayarlanması gerekmektedir. New York'un Bitlicense'ı, blokzincir kullanan şirketler için KYC (know your customer - müşterini tanı) gerekliliklerini belirleyerek bu soruna çözüm sunmaya çalışmaktadır. Ancak farklı ülkelerdeki düzenleyici yaklaşımların çeşitliliği, muhasebe uygulamalarını düzenlemek üzere uluslararası anlaşmaların geliştirilmesini zorlaştırmaktadır. Bir diğer konu da vergilendirme uygulamalarının eşler arası paylaşım ekonomisini kapsayacak şekilde düzenlenmesidir. Bu kapsamda vergilendirme sisteminin de gözden geçirilmesi gerekecektir (Potekhina vd., 2017, s.16).

## **5. ARAŞTIRMANIN KURAMSAL ÇERÇEVESİ**

Çalışmanın bu bölümünde, araştırmanın kuramsal çerçevesi; araştırmanın konusu, amacı, önemi, varsayımları, sınırları ve soruları itibarıyla tanımlanmış ve literatüre sağladığı katkı, blokzincir teknolojisinin benimsenmesine ilişkin Teknoloji Kabul Modeli kullanılarak yapılan araştırmalar açısından değerlendirilmiştir.

### **5.1 ARAŞTIRMANIN KONUSU**

Bu çalışma ile blokzincir teknolojisinin ortaya çıkabilecek finansal bilgi manipülasyonlarını önlemede ne derece etkili olduğu ile İstanbul'daki mali müşavir meslek mensuplarının yeni teknolojik gelişmelere ne kadar hazırlıklı oldukları ve blokzincir teknolojisinin finansal bilgi manipülasyonunu önlenmesine yönelik görüşleri araştırılarak, gelişmekte olan literatüre İstanbul örneklemiyle katkıda bulunmak istenilmektedir.

### **5.2 ARAŞTIRMANIN AMACI VE ÖNEMİ**

Dijitalleşme, internet ve iletişim teknolojilerindeki hızlı gelişmeler, işletmeleri akıllı hale getirirken, aynı zamanda muhasebe, finansman ve denetim süreçlerinin de dijital dönüşüme uğramasına neden olmaktadır. Bu dönüşüm süreci, ilgili literatürde çeşitli araştırmacılar tarafından genel hatlarıyla ele alınmıştır. Ancak blokzincir teknolojisinin finansal bilgi manipülasyonlarını önlemedeki potansiyeli üzerine yeterli sayıda çalışma bulunmamaktadır. Bu bağlamda mevcut araştırma ile blokzincir teknolojisinin muhasebe ve denetim süreçlerine etkileri üzerine derinlemesine bir inceleme yapılarak; blokzincir uygulamalarının, işletmelerin finansal süreçlerini nasıl daha güvenilir ve şeffaf hale getirebileceğine dair literatüre önemli bir katkı sağlanması amaçlanmaktadır.

Ayrıca bu çalışma ile mali müşavir meslek mensuplarının yeni bir araç olan blokzincir teknolojisi hakkındaki farkındalıkları arttırılarak finansal bilgi manipülasyonunu (muhasebe hilelerini) önlemede ilgili teknolojiyi kullanmalarını sağlamak yoluyla potansiyel mesleki yetkinliklerinin ve iş alanlarının geliştirilmesi açısından meslek mensuplarına büyük katkılarının olacağı öngörülmektedir.

### 5.3 ARAŞTIRMANIN VARSAYIM VE SINIRLARI

#### 5.3.1 Araştırmanın Varsayımları

Araştırmada dikkate alınan varsayımlar aşağıda sıralandığı gibidir :

- a. Araştırmaya destek olan SMMM ve YMM’lerin gönüllü olarak ankete katılım sağladıkları varsayılmıştır.
- b. İstanbul ilindeki SMMM ve YMM Odalarına kayıtlı SMMM ve YMM’lerin anket sorularına tarafsız, gerçeğe uygun ve tutarlı yanıtlar verdikleri varsayılmıştır.
- c. Araştırma evreninin, en az 408 kişilik mali müşavir meslek mensubu örneklem büyüklüğü ile yeterli düzeyde temsil edileceği varsayılmıştır.
- d. İstanbul’da faaliyet gösteren SMMM meslek mensupları evreninden, en az 1 yıllık mesleki uzmanlık ve tecrübeye sahip olanların araştırmaya katılımlarının araştırma sonuçlarının doğruluk ve geçerliliğini yansıtacağı varsayılmıştır.
- e. İstanbul ilindeki SMMM ve YMM Odalarına kayıtlı mali müşavir meslek mensuplarının;
  - i. Blokzincir teknolojisini kabul düzeylerinin “*Teknoloji Kabul Modeli (Technology Acceptance Model-TAM)*” ölçeği ile,
  - ii. Blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemede kullanımına yönelik eğilimlerinin ise “*The Association of Certified Fraud Examiner (ACFE)*”nin hile araştırmalarında kullanmış olduğu ölçek ile literatürde geçerliliği kanıtlanmış ölçeklerden oluşturulan sorular aracılığıyla oluşturulmuş ve daha önce İşgüden Kılıç & Anadolu (2018) tarafından yazılan *Dijital Çağın Yarattığı Muhasebe Uygulamalarının Muhasebe Hilelerinin Önlenmesine Etkisi* konulu makalede kullanılmış geçerliliği kanıtlanmış olan ölçek” ile

araştırma amacına yönelik uygun veri setine ulaşılmasında ihtiyaç duyulan koşulların sağlandığı varsayılmıştır.

### 5.3.2 Araştırmanın Sınırları

Araştırmanın ideal evrenini Türkiye’de faaliyet gösteren SMMM ve YMM’ler oluşturmaktadır. Ancak bu ideal evrene ulaşmada Türkiye’de bulunan 77 adet SMMM Odası ve 8 adet YMM Odası olmak üzere toplam 85 adet mali müşavir meslek odasına kayıtlı meslek mensuplarına ulaşılabilmesi için her bir Oda Başkanlığı ile tek tek iletişime geçilerek işbirliklerinin talep edilmesi ve olumlu cevap alınabilmesi kısıtı ile karşılaşılmaktadır.

Ayrıca 06.02.2023 tarihinde gerçekleşen Kahramanmaraş depremleri sebebiyle büyük yıkım yaşanan Kahramanmaraş, Kilis, Diyarbakır, Adana, Osmaniye, Gaziantep, Şanlıurfa, Adıyaman, Malatya ve Hatay illerinde faaliyet gösteren meslek mensuplarının hem mücbir sebepleri hem de yas sürecinin devam etmesi nedeniyle araştırmaya katılmama ihtimalleri de bir diğer kısıt olarak karşımıza çıkmaktadır.

Dolayısıyla mücbir sebep dahilindeki 10 il de hariç tutulduğunda İSMMMO ve İYMMO’nun Türkiye’deki en yüksek üye sayılarına sahip olmaları sebebiyle Türkiye genelini diğer odalara nazaran en kapsamlı olarak yansıtacağı varsayımıyla araştırma evreni İstanbul’da faaliyet gösteren SMMM ve YMM’ler ile sınırlandırılmıştır.

Bir başka sınırlama ise mali müşavir meslek mensuplarının blokzincir teknolojisini faaliyetlerinde kullanımlarına yönelik kabullerindeki ve finansal bilgi manipülasyonu ile karşılaşma sıklığı üzerinden blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemede kullanılmasına yönelik eğilimlerindeki farkın ölçülebilmesi için uzmanlık düzeyinde mesleki bilgi ve birikim sahibi olarak farklı teknolojik uygulamalar ile mesleklerini belirli bir süredir icra ediyor olmaları gerektiği üzerinedir. Bu nedendir ki söz konusu mesleki uzmanlık ve tecrübe kısıtları sebebiyle SMMM stajyerleri ve Serbest Muhasebeciler (SM) araştırma örneklemine dâhil edilmemişlerdir.

Son olarak araştırmada kullanılan veri toplama yöntemi; zaman (mali müşavirlerin iş yoğunluğu nedeniyle randevu alınamaması), ulaşım (İstanbul ilinde nüfus ve yüz ölçümü özellikleri sebebiyle karşılaşılan trafik unsuru) ve maliyet kısıtlamaları sebebiyle başlangıçta çevrimiçi anket uygulaması ile sınırlandırılmış ancak SMMM’lerin çevrimiçi anket katılım oranlarının düşük gerçekleşmesi sebebiyle yüz yüze anket uygulaması da yapılarak veri toplama yöntemi kapsamı genişletilmiştir. Buradan hareketle SMMM’lerin anket uygulamasına katılım isteği de bir diğer kısıt olarak karşımıza çıkmış bulunmaktadır.

#### 5.4 ARAŞTIRMA SORULARI

Bu çalışmaya dayanak olan araştırma soruları aşağıdaki gibidir:

- a- Blokzincir teknolojisi nedir, işleyişi, özellikleri, türleri, avantaj ve dezavantajları nelerdir?
- b- Finansal bilgi manipülasyonu nedir, yapılma nedenleri ve yöntemleri nelerdir?
- c- Finansal bilgi manipülasyonunu engellemeye yönelik güncel yaklaşımlar nelerdir?
- d- Blokzincir teknolojinin muhasebe ve denetim uygulamalarına etkileri nelerdir?
- e- Blokzincir teknolojisi finansal bilgi manipülasyonunu engellemede etki ediyor mu?
- f- İstanbul'daki mali müşavirlerin blokzincir teknolojisini kullanmaya yönelik niyetleri, tutumları ve davranışlarını algıladıkları kullanım kolaylığı, algıladıkları fayda ve engeller etkiliyor mu?
- g- İstanbul'daki mali müşavirlerin farklı demografik ve mesleki özelliklere sahip olması blokzincir teknolojisi kabulüne yönelik tutum, niyet ve gerçekleşen davranış düzeyleri arasında farklılık yaratıyor mu?
- h- İstanbul'daki mali müşavirlerin demografik ve ünvan, çalışma şekli, çalışma süresi, mükellef sayısı gibi mesleki özellikleri, finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklıklarında farklılık yaratıyor mu?
- i- İstanbul'daki mali müşavirlerin demografik ve ünvan, çalışma şekli, çalışma süresi, mükellef sayısı gibi mesleki özellikleri, blokzincir teknolojinin finansal bilgi manipülasyonunu önlemedeki rolüne yönelik görüşlerinde farklılık yaratıyor mu?

## 5.5 ARAŞTIRMANIN LİTERATÜRE SAĞLADIĞI KATKI

Finansal bilgi manipölasyonu bir diğör adıyla muhasebe hileleri, birçok ölkede ve farklı dönemlerde sürekli olarak tekrarlanmakta ve büyük ekonomik zararlara sebep olmaktadır. Dünya çapında büyük şirketlerde Enron, WorldCom, Global Crossing, Parmalat, Tyco International, Xerox, Toshiba vb. gibi örneklerine rastladığımız muhasebe skandalları; mikro düzeyde yatırımcı, borç veren, satıcılar ve çalışanların zarar görmesine neden olurken, makro düzeyde ise kaynakların yanlış yere aktarılmasına ve tüm toplumun zararına neden olmaktadır (Hatunoğlu, Koca & Kılılı, 2012, s. 177). Nitekim Association of Certified Fraud Examiners (ACFE)'nin yayınlamış olduđu “Occupational Fraud 2024: A Report To The Nations” raporunda, dünya üzerinde 138 ölkeden 1.921 adet vaka incelendiğinde 3,1 milyon \$’dan fazla kaybın gerçekleştiğı ve her yıl işletmelerin, gelirlerinin yaklaşık %5’ini muhasebe hilesi sonucu kaybettiğı belirtilmiştir (ACFE, 2024, s.9).

Şirketler ise bu kayıplarla mücadele etmek için iç denetim, iç kontrol, bağımsız denetim, anonim ihbar hatları gibi birtakım araçlardan yararlanarak muhasebe hata ve hilelerini önlemeye ve ortaya çıkarmaya çalışmaktadırlar. Ancak bu geleneksel araçların istenildiğı kadar etkili olmaması hile incelemesi, kurumsal yönetim, veri madenciliğı, nitelikli finansal raporlama gibi çağdaş araçların sisteme dahil olmasına yol açmıştır (Kandemir&Kandemir, 2012, s.1). Bu anlamda hile ve hata tespitinde proaktif yaklaşımlar benimsenerek; istatistiki yöntemler, mali analiz yöntemleri, bilgisayar destekli denetim teknikleri, yapay zekâ, bulanık mantık, uzman sistemler, dijital analiz yöntemleri (Benford Kanunu) ve veri madenciliğı yöntemi gibi yöntemler kullanılmaktadır (İşğüden Kılıç & Anadolu, 2018, s.62).

Endüstri 4.0’ı tetikleyen ve gelecekteki sanayi üretimini şekillendirecek olan dokuz temel teknolojik gelişme yaşanmıştır. Bunlar; akıllı robotlar, büyük veri ve analiz, yatay/dikey entegrasyon, simölasyon, bulut teknolojisi, siber güvenlik, eklemeli üretim, artırılmış gerçeklik ve nesnelerin internetidir (TÜSİAD, 2016 s.25). Üretim bandında kullanılan robotik teknoloji, onları organize eden ve üretimi yöneten bir yapay zekâ, üretim sürecine dair tüm verilerle birlikte esnek tüketimin sağlanabilmesi için tüketim verilerinin de aktarıldığı büyük veri, tüm yazılım ve donanımların birbirleriyle iletişim kurabilmesini sağlayan nesnelerin interneti ve veri depolama birimi olarak kullanılan bulut bilişim. Endüstri 4.0’ın başlıca beş dinamiğı, akıllı fabrikayı oluşturmak üzere kullanılmaktadır (Turan, 2018, s.55). Endüstri 4.0 ile modüler yapılı akıllı fabrikalar kapsamında, fiziksel

işlemleri siber-fiziksel sistemlerle izlemek, fiziksel dünyanın sanal bir kopyasını oluşturmak ve merkezi olmayan kararların verilmesi hedeflenmektedir (Türkiye'nin Endüstri Platformu, <https://www.endustri40.com/endustri-tarihine-kisa-bir-yolculuk/>). Bu merkezi olmayan yapının inşa edilebilmesi de endüstri 4.0'ın bir diğer itici gücü, dağıtık (merkezi olmayan) ve ortak bir veri kayıt sistemi (Özalp, 2018, s.293) olan blokzincir teknolojisi ile mümkün olabilmektedir.

Dijitalleşme, internet ve iletişim alanındaki bu teknolojik gelişmeler bir yandan işletmeleri akıllandırırken diğer yandan işletmenin muhasebe, finansman ve denetim süreçlerini de dijital dönüşüme uğratmaktadır. Bu dönüşüme ilişkin genel hatlar ilgili yazında araştırmacılar tarafından ele alınmıştır. Ancak blokzincir teknolojisinin muhasebe hata ve hilelerini önlemede kullanılmasına ilişkin yeterli çalışma bulunmamaktadır.

Bu sebeplerden ötürü, bu çalışmanın işletme literatürüne katkıları açısından temel iki amacı bulunmaktadır. Birincisi, blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemede nasıl kullanılabileceğinin tespit edilmesidir. İkincisi ise bu süreci yönetmede aktif rol oynayan meslek mensupları mali müşavirlerin sosyo-demografik ve meslek özellikleri çerçevesinde yeni teknolojik gelişmelere (blokzincir teknolojisi) ne kadar hazırlıklı ve açık olduklarının Teknoloji Kabul Modeli (Technology Acceptance Model – TAM) kapsamında değerlendirilmesi ve finansal bilgi manipülasyonu ile karşılaşma sıklıkları ve muhasebe hilelerinin önlenmesinde blokzincir teknolojisinin rolüne ilişkin görüşleri üzerine gelişmekte olan literatüre İstanbul örneklemiyle katkıda bulunmaktır.

### **5.5.1 Teknolojinin Benimsenmesinde Kullanılan Modeller**

Hızlı teknolojik gelişmeler ve dijitalleşme, hayatımızın hemen her alanında araştırmacıların dikkatlerini bireylerin teknoloji kabullerini açıklayan etkenlere yöneltmesine yol açmıştır. Bu dikkat hem davranışsal niyet hem de teknolojilerin etkin kullanımını tanımlayan birçok teorik modelin geliştirilmesini sağlamıştır. (Scherer & Teo, 2019, s.2387) Teknolojinin benimsenmesinde kullanılan bu modelleri, geliştirilme sıralamasına göre aşağıdaki gibi sınıflandırabiliriz :

- a. Yenilik Yayılım Teorisi (Diffusion of Innovation Theory - DOI)
- b. Sebepli Davranış Teorisi (Theory of Reasoned Action - TRA)
- c. Planlı Davranış Teorisi (Theory of Planned Behavior - TPB)
- d. Teknoloji Kabul Modeli (Technology Acceptance Model - TAM)
- e. Teknoloji – Organizasyon – Çevre Modeli (Technology – Organization - Environment – TOE)
- f. İş-Teknoloji Uygunluk Modeli (Task Technology Fit- TTF)
- g. Teknoloji Kabul Modeli 2 (Technology Acceptance Model 2 - TAM 2)
- h. Birleştirilmiş Teknoloji Kabul ve Kullanım Modeli (Unified Technology Acceptance and Use Theory - UTAUT )
- i. Teknoloji Kabul Modeli 3 (Technology Acceptance Model 3 - TAM 3)
- j. Birleştirilmiş Teknoloji Kabul ve Kullanım Modeli 2 (Unified Technology Acceptance and Use Theory - UTAUT 2)

Teknolojinin benimsenmesinde kullanılan söz konusu modeller; geliştirenler, model açıklaması ve model (şekilleri) başlıkları kullanılarak düzenlenen Tablo 5.1 aracılığıyla aşağıda kısaca tanımlanmışlardır.



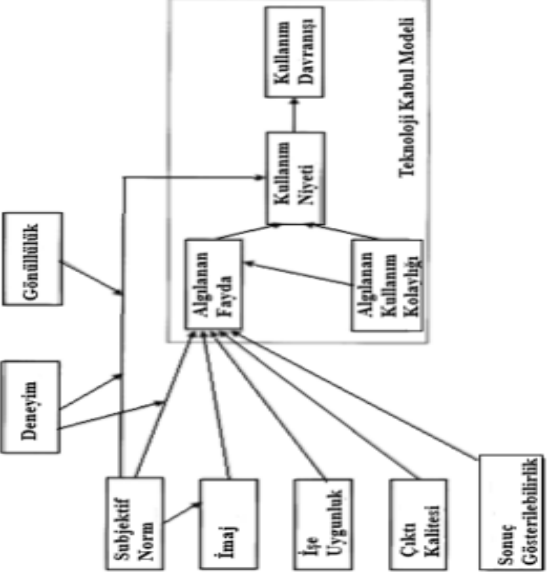
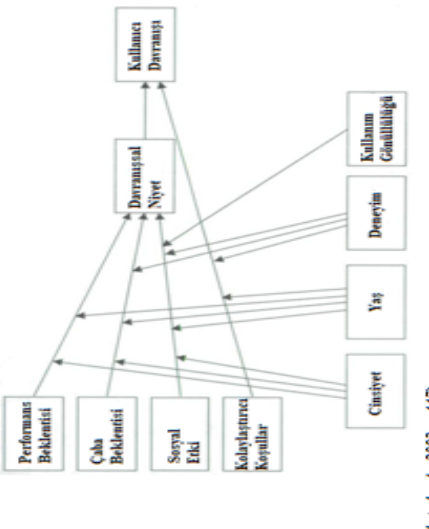
**Tablo 5.1:** Teknolojinin Benimsenmesinde Kullanılan Modeller.

| Teknolojinin Benimsenmesinde Kullanılan Modeller               | Geliştiriciler                     | Model Açıklaması                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Modeli                                                           |
|----------------------------------------------------------------|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Yenilik Yayılım Teorisi (Diffusion of Innovation Theory - DOI) | Ryan & Gross (1943), Rogers (1995) | Rogers (2003)'a göre yenilik yayılımı, bir yeniliğin, sosyal sistemin üyeleri arasında zaman içinde belirli kanallar aracılığıyla iletiildiği bir süreçtir. (Kamışlı, 2011, s.5) Yayılımın temelinde yenileşme, iletişim kanalları, zaman ve sosyal sistem olmak üzere dört öge bulunmaktadır. Yeniliğin algılanması ile başlayan yenileşme süreci bireyin benimsene veya reddetme kararı ile sonuçlanmaktadır. Bu karar verilirken bilgi, ikna, karar, uygulama ve onay olmak üzere beş aşamadan geçmektedir. İletişim kanalları aracılığıyla aktarılan yenileşme mesajı, bireyin, yeniliğe ilişkin göreceli avantaj, uygunluk, kolaylık/karmaşıklık, denenebilirlik ve gözlenebilirlik algılan ve içinde bulunduğu sosyal sistem üzerinden yeniliğe yönelik tutumlarını şekillendirerek yeniliğe uyum hızını ve kararını etkilemektedir. (Karahanna vd., 1999) | <p>(Rogers, 1995; Akt. Kılıçer, 2011, s.18)</p>                  |
| Sebepli Davranış Teorisi (Theory of Reasoned Action-TRA)       | Fishbein ve Ajzen (1975)           | TRA, geniş alan çeşitliliği karşısında davranış tahmini etme ve açıklamada başarsız kalmamış ve iyi araştırılmış bir niyet modelidir. Bu teoriye göre, bir kişinin belirli bir davranışta bulunması, o kişinin evlene geçmesindeki davranışsal niyetine göre gerçekleşmektedir. Ve davranışsal niyetin ise "kişinin davranışa yönelik olumlu veya olumsuz duyguyu ve inançları" olan <i>tutum</i> ve "kişinin söz konusu davranışı gerçekleştirip gerçekleştirmediğiyle ilgili önemli gördüğü kişilerin düşüncesine ilişkin (sosyal baskı) algısı" olan <i>özel normlar</i> dan birlikte etkilendiği varsayılmaktadır. (Fishbein & Ajzen, 1975; Akt. Davis vd., 1989, s.983-984)                                                                                                                                                                                 | <p>(Fishbein &amp; Ajzen, 1975; Akt. Davis vd., 1989, s.984)</p> |
| Planlı Davranış Teorisi (Theory of Planned Behavior-TPB)       | Ajzen (1985)                       | TPB, TRA'ı geliştirilmiştir. Özgün modelin, insanları eyleme iten etkenlerin kontrolünden kaynaklanan (para, zaman, yetenek vb. gibi) davranışsal tahmin etme kısıtı dolayısıyla modele <i>algılanan davranışsal kontrol</i> değişkeni ilave edilmiştir. Bu teoriye göre, bir davranışın gerçekleşmesi, niyetlerin ve algılanan davranışsal kontrolün ortak bir işlevidir. (Ajzen, 1991, s.185)                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <p>(Ajzen, 1991, s.182)</p>                                      |

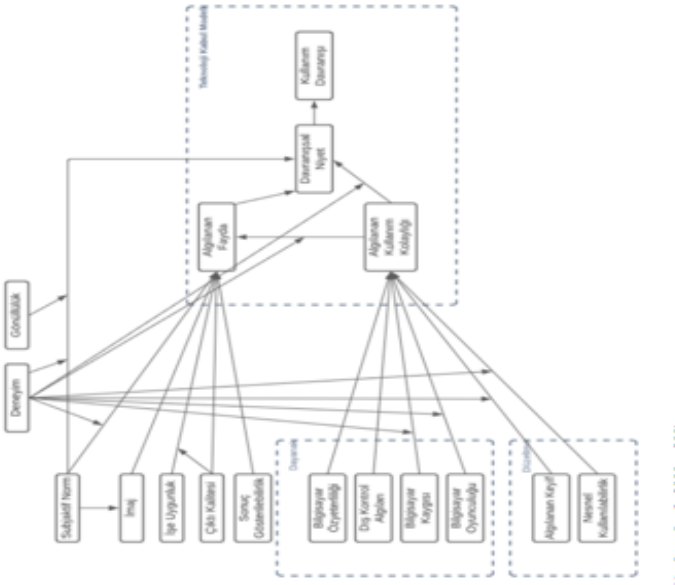
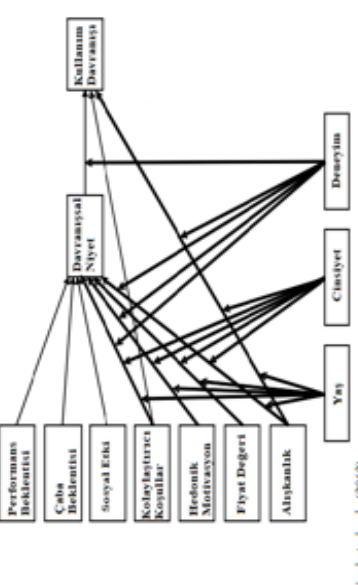
**Tablo 5.1:** Teknolojinin Benimsenmesinde Kullanılan Modeller (Devam).

| Teknolojinin Benimsenmesinde Kullanılan Modeller                                        | Geliştirilenler             | Model Açıklaması                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Modeli                                         |
|-----------------------------------------------------------------------------------------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| Teknoloji Kabul Modeli (Technology Acceptance Model-TAM)                                | Davis (1986)                | TAM, bilgi sistemlerinin kullanıcı kabuluine ilişkin TRA üzerine yapılan bir model uyarlamasıdır. Bu modelde; teknoloji kabul davranış, öncelikle olarak dış etkenlere göre değişen "olası kullanıcının, herhangi bir uygulamanın kullanımını iş performansını arttırmasına yönelik algısı" olan <i>algılanan fayda (U)</i> ve "olası kullanıcının, çaba sarf etmeden söz konusu teknolojiyi kullanabilme beklentisinin derecesi" olan <i>algılanan kullanım kolaylığı (E)</i> olmak üzere iki temel inancın etkilendiği modeldir. TAM' da TRA' da olduğu gibi teknoloji kullanımı, davranışsal niyetten (BI) etkilendiği modeldir. Ancak farklı olarak davranışsal niyetin (BI) sadece kullanıma yönelik tutumdan (A) değil aynı zamanda algılanan faydadan (U) da etkilendiği varsayılmaktadır. Ayrıca diğer temel etken olan algılanan kullanım kolaylığının aynı zamanda algılanan faydayı da etkilediği belirtilmektedir. (Davis vd., 1989) | <p>(Davis vd., 1989, s.985)</p>                |
| Teknoloji – Organizasyon – Çevre Modeli (Technology – organization – environment – TOE) | Tomatzky & Fleischer (1990) | TOE'ye göre bir organizasyonun yeni bir teknolojiyi kabul etmesinde üç unsur etkili olmaktadır. Bunlar Teknoloji, Çevre ve Organizasyon'dur. <i>Teknoloji</i> ; organizasyonda mevcut teknoloji ile organizasyon dışı erişilebilir teknolojilerin <i>organizasyonu</i> ; örgütün faaliyet alanı, büyüklüğü, kurumsallaşma, yönetim yapısı, merkezleşme düzeyi, insan kaynakları kalitesi gibi organizasyonu tanımlayan unsurları ve <i>çevre</i> ise; firmanın faaliyette bulunduğu endüstri, sektörel rakipleri ve devletle ilişkileri ifade etmektedir. (Tomatzky & Fleischer, 1990)                                                                                                                                                                                                                                                                                                                                                           | <p>(Tomatzky &amp; Fleischer, 1990, s.154)</p> |
| İş-Teknoloji Uygunluk Modeli (Task Technology Fit- TTF)                                 | Goodhue & Thompson (1995)   | TTF; bir teknolojinin, bireyin işe yönelik görevlerini yerine getirmede bireye yardım etme derecesini açıklamaktadır. TTF ile bilgi teknolojilerinin bireysel performans olumlu etkisinin olduğu, teknolojinin mutlaka kullanılması gerektiği ve teknolojinin mutlaka desteklediği iş ile uyumlu olması gerektiği iddia edilmektedir. Bu bağlamda <i>iş özellikleri</i> ve <i>teknolojik özelliklerin</i> teknolojinin işe uyumunu belirlediği, <i>iş-teknoloji uyumu</i> nun da hem gelişmiş verimlilik, etkinlik ve daha yüksek kaliteyi ifade eden <i>performans etkisini</i> hem de <i>teknoloji kullanımını</i> etkilediği varsayılmaktadır. (Goodhue & Thompson, 1995)                                                                                                                                                                                                                                                                     | <p>(Goodhue &amp; Thompson, 1995, s.220)</p>   |

**Tablo 5.1:** Teknolojinin Benimsenmesinde Kullanılan Modeller (Devam).

| Teknolojinin Benimsenmesinde Kullanılan Modeller                                                       | Geliştirilenler          | Model Açıklaması                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Modeli                                                                                                                 |
|--------------------------------------------------------------------------------------------------------|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Teknoloji Kabul Modeli 2 (Technology Acceptance Model 2 - TAM2)                                        | Venkatesh & Davis (2000) | TAM2, algılanan fayda değişkeninin kullanımı niyetinin temel belirleyicisi olduğuna ilişkin yapılan tutarı çalışmalar neticesinde, algılanan faydayı etkileyen değişkenleri belirlemek amacıyla geliştirilmiş bir modeldir. Bu amaçla TAM'a, algılanan fayda ve kullanımı niyetini etkileyen sosyal etki (subjektif normlar, gönüllülük ve imaj) ve bütünsel etki (işe uygunluk, çıktı kalitesi, sonuç gösterilebilirliği ve algılanan kullanımı kolaylığı) süreçleri dahil edilmiştir. <i>Subjektif norm</i> ; kişinin söz konusu davranışı gerçekleştireceğiyle ilgili önemli gördüğü kişilerin düşüncesine ilişkin algıdır. <i>Gönüllülük</i> ; olası kullanıcının, zorunlu olmayan benimsenme kararını almasıdır. <i>İmaj</i> ; kişinin sosyal sistemi içindeki itibarını arttırmak için yenilik kullanımını algılamaya dercesidir. <i>İşe uygunluk</i> ; hedef sistemin işe uygulanabilirliğiyle ilgili kişinin algıdır. <i>Çıktı kalitesi</i> ; sistemin yapabildiği görevlerin ne kadar işe uygun ve iyi olduğunun dercesidir. <i>Sonuç gösterilebilirlik</i> ise; yenilik kullanımını ile somut sonuçların elde edilmesi olarak tanımlanmaktadır. Modelde ayrıca zaman içerisinde artan <i>deneyim</i> in subjektif normların şiddetini artırarak algılanan fayda ve kullanımı niyetini etkilediği de varsayılmaktadır. (Venkatesh vd., 2000) |  <p>(Venkatesh vd., 2000, s.188)</p>  |
| Birleştirilmiş Teknoloji Kabul ve Kullanım Modeli (Unified Technology Acceptance and Use Theory-UTAUT) | Venkatesh vd., (2003)    | UTAUT; Sebepli Davranış Teorisi (TRA), Teknoloji Kabul Modeli (TAM), Motivasyon Modeli (MM), Planlı Davranış Teorisi (TPB), PC Kullanım Modeli, Yenilik Yayılım Teorisi (DOI), Sosyal Biliş Teorisi ve TAM ve TPB birleştirildiği bir model olmak üzere sekiz modelin gözden geçirilmesiyle oluşturulmuş bir modeldir. UTAUT'a göre, dört anahtar düzenleyici olan cinsiyet, yaş, deneyim ve kullanımı gönüllülüğü belirleyicilerinden etkilenen performans beklentisi, çaba beklentisi, sosyal etki ve kolaylaştırıcı koşullar olmak üzere dört temel değişken teknoloji kullanımına dair davranışsal niyet üzerinde etkilidir. <i>Performans beklentisi</i> ; sistem kullanımının iş hayatında kazanç elde etmesine yardımcı olacağına ilişkin bireyin inanç dercesidir. <i>Çaba beklentisi</i> ; teknoloji kullanımını kolaylık dercesidir. <i>Sosyal etki</i> ; bireyin, önemli kişilerin onun yeni teknolojiyi kullanması gerektiğine inanıyor olmalarına ilişkin algısının dercesidir. <i>Kolaylaştırıcı koşullar</i> ; bireyin, sistem kullanımını destekleyen bir örgütsel ve teknik altyapının var olduğuna inanma dercesidir. (Venkatesh vd., 2003)                                                                                                                                                                                         |  <p>(Venkatesh vd., 2003, s.447)</p> |

**Tablo 5.1:** Teknolojinin Benimsenmesinde Kullanılan Modeller (Devam).

| Teknolojinin Benimsenmesinde Kullanılan Modeller                                                           | Geliştirenler           | Model Açıklaması                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Modeli                                                                                                                 |
|------------------------------------------------------------------------------------------------------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Teknoloji Kabul Modeli 3 (Technology Acceptance Model 3 - TAM3)                                            | Venkatesh & Bala (2008) | <p>TAM3; TAM2 ve algılanan kullanım kolaylığı değişkenleri (bilgisayar özyeterliliği, dış kontrol algısı, bilgisayar kaygısı, bilgisayar oyunculuğu, algılanan keyif ve nesnel kullanılabilirlik) (Venkatesh, 2000) birleştirilerek geliştirilmiş bir entegre teknoloji kabul modelidir (Venkatesh vd., 2008, s.278) <i>Bilgisayar özyeterliliği</i>; kişinin bilgisayar kullanarak belirli bir görevi yerine getirebilme yeteneğine sahip olduğuna inanma derecesidir (Compeau&amp;Higgins, 1995a, 1995b, Akt. Venkates vd., 2008). <i>Dış kontrol algısı</i>; kişinin, sistem kullanımında desteklenmesi için organizasyonel ve teknik kaynakların var olduğuna inanma derecesidir (Venkates, 2003, Akt. Venkates vd., 2008). <i>Bilgisayar kaygısı</i>; kişinin bilgisayar kullanma olasılığı ile karşı karşıya kaldığındaki endişe hatta korku derecesidir (Venkates, 2000, Akt. Venkates vd., 2008). <i>Bilgisayar oyunculuğu</i>; mikrobilgisayar etkileşimindeki bilişsel spontanlık derecesidir (Webster&amp; Martocchio, 1992, Akt. Venkates vd., 2008). <i>Algılanan keyif</i>, <i>sistemi kullanmaktan kaynaklanan herhangi bir eylem sonucu haric, belirli bir sistemi kullanma faaliyetinin kendi başına eğlenceli olarak algılanma derecesidir</i> (Venkates, 2000, Akt. Venkates vd., 2008). <i>Nesnel kullanılabilirlik</i> ise; belirli görevleri tamamlamak için gereken gerçek çaba düzeyine (algılardan ziyade) dayalı sistemlerin karşılaştırılması (Venkates, 2000, Akt. Venkates vd., 2008) şeklinde tanımlanmaktadır. Modele göre; algılanan fayda değişkenlerinin algılanan kullanım kolaylığı üzerinde herhangi bir etkisi bulunmamaktadır. Diğer yandan TAM2’de subjektif normlar üzerinden sadece algılanan fayda ve kullanım niyetine etkisinin ölçüldüğü <i>deneyim</i> faktörü TAM3’de üç farklı varsayımı daha dikkate alınmıştır: algılanan kullanım kolaylığı üzerinden hem (i) algılanan faydayı hem de (ii) davranışsal niyeti etkilemektedir. Ayrıca, (iii) bilgisayar kaygısı üzerinden de algılanan kullanım kolaylığını etkilemektedir (Venkates, 2008).</p> |  <p>(Venkatesh vd., 2008, s.280)</p> |
| Birleştirilmiş Teknoloji Kabul ve Kullanım Modeli 2 (Unified Technology Acceptance and Use Theory-UTAUT 2) | Venkatesh vd. (2012)    | <p>UTAUT2; UTAUT’ın teknoloji kabul ve kullanımın rüketici bağlamında ölçülmesine yönelik geliştirilmiş halidir. Bu model; hedonik motivasyon, fiyat değeri ve alışkanlık olmak üzere üç yapıyı UTAUT bünyesine dâhil etmiştir. Bu yapıların, bireysel farklılıklar (yaş, cinsiyet ve deneyim gibi) aracılığıyla davranışsal niyet ve teknoloji kullanımını etkilediği varsayılmıştır. <i>Hedonik motivasyon</i>; teknoloji kullanımından türemiş eğlence veya haz olarak tanımlanmaktadır, ve teknoloji kabulü ve kullanımın belirlenmesinde önemli bir rol oynayarak kendini göstermektedir. <i>Fiyat değeri</i>; uygulamanın algılanan yarar ile kullanımın parasal maliyeti arasındaki rüketicilerin bilişsel değiş tokuşu olarak tanımlanmıştır. <i>Alışkanlık</i> ise; insanların öğrenme sebebiyle otomatik davranma eğiliminin kapsamı olarak tanımlanmaktadır (Venkatesh vd., 2012)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  <p>(Venkatesh vd., (2012)</p>      |



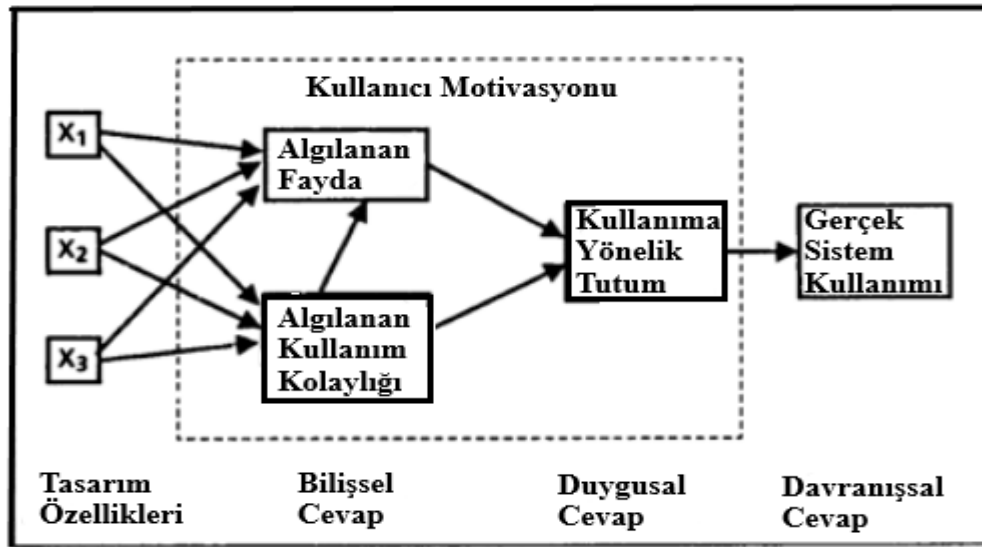
### 5.5.2 Teknoloji Kabul Modeli (Technology Acceptance Model – TAM/TKM)

Fred D. Davis'in, 1985 yılında doktora tezinde önerdiği Teknoloji Kabul Modeli (TKM), bilgisayar teknolojilerinin kullanıcı kabulünü etkileyen unsurların araştırılmasında literatürde yaygın olarak kullanılan bir modeldir. TKM, Sebepli Davranış Teorisi (Theory of Reasoned Action-TRA)'nden türetilmiştir. TRA'ya göre; olumlu veya olumsuz inançlar, tutumları etkilemekte; bu tutumlar, kullanım niyeti yaratmakta; niyetler de davranışları yönlendirmekte ya da oluşturmaktadır. Söz konusu bu inanç-tutum-niyet-davranış ilişkisi TKM ile bilgisayar teknolojisi kullanıcı kabul modeline uyarlanmaktadır.

TKM'de, algılanan fayda (U) ve algılanan kullanım kolaylığı (E) olmak üzere iki özel inancın bilgisayar kabul davranışları üzerinde birincil etkiye sahip olduğu varsayılmaktadır. Algılanan fayda (U), potansiyel kullanıcının yeni teknolojiyi kullanmanın iş performansını artıracağına ilişkin algısını ifade ederken; algılanan kullanım kolaylığı (E) ise, potansiyel kullanıcının, çaba sarfetmeden yeni teknolojiyi kullanabilme beklentisinin düzeyini ifade etmektedir. Modele göre; dış değişkenlerden etkilenen iki temel inanç: algılanan fayda (U) ve algılanan kullanım kolaylığı (E), olası kullanıcıların teknoloji kullanımına yönelik tutumlarını (A) olumlu veya olumsuz olarak etkilemektedir. Kullanıma yönelik tutum (A) ise gerçekleşen davranışı yönlendiren niyet (BI) üzerinde belirleyici olmaktadır. TKM bu aşamada TRA'dan farklılaşarak, niyet üzerinde sadece tutumun etkisi olduğunu değil; aynı zamanda algılanan faydanın (U) da niyet (BI) üzerinde doğrudan belirleyiciliği olduğunu ileri sürmektedir. Ayrıca temel inançlar arasında da etkileşim olduğu ve algılanan kullanım kolaylığının (E), algılanan faydayı (U) etkilediği varsayılmaktadır (Davis vd., 1989, s.985).

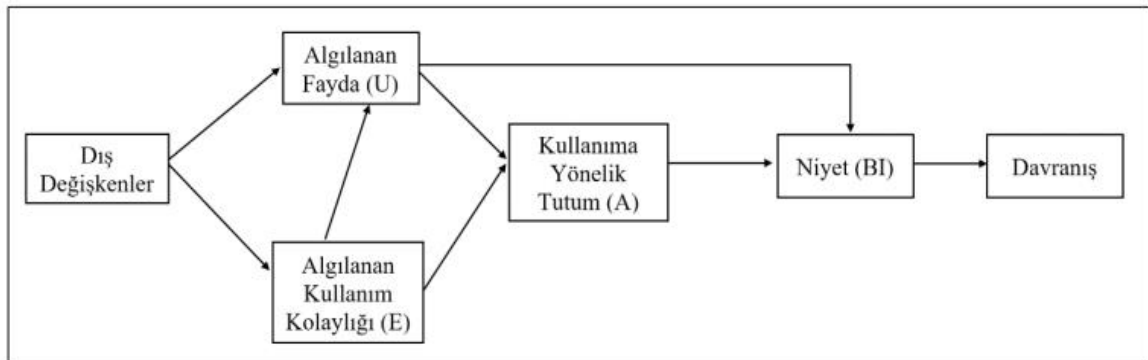
TRA'dan farklı olan TKM'deki algılanan fayda (U) ve kullanıma yönelik niyet (BI) ilişkisi, insanların iş performanslarını artıracağına inandıkları davranışlara yönelik niyetler geliştirmelerine dayanmaktadır. Bunun nedeni, artan performansın, çeşitli ödüllerin (terfi, ücret artışı vb. gibi) elde edilmesinde etkili olmasıdır. Bazı durumlarda ise performansa bağlı ödüllerle ilişkili olumlu duygulanım harekete geçirilemeyebilmektedir. Böyle bir durumda belirli bir teknolojiyi kullanma kararı verilirken; kişinin tutumu, performansa dair düşüncelerinin niyet üzerindeki etkisini doğru bir şekilde yansıtamamaktadır. Dolayısıyla U-BI doğrudan ilişkisi; belirli bir teknolojinin kullanımına yönelik niyetin, performansı nasıl artıracağına dair bilişsel bir değerlendirmeye dayalı olarak oluştuğu varsayımı ile ortaya çıkan doğrudan etkiyi temsil etmektedir (Davis vd., 1989, s.986).

Diğer yandan temel inanç değişkenlerinden algılanan kullanım kolaylığının (E) tutum üzerinde doğrudan etkisi olduğu gibi; diğer bir inanç değişkeni olan algılanan fayda (U) aracılığıyla da tutum üzerinde etki gösterebilmektedir. Burada algılanan fayda (U) üzerindeki etkisi, yeni teknolojinin kullanım kolaylığının sağladığı çaba tasarrufunun, aynı zamanda performansın artışına katkı sağlaması varsayımından kaynaklanmaktadır. Yani yeni teknoloji, bir kişinin sarfettiği aynı çaba düzeyinde daha yüksek performans sağlayarak ödül elde etmesini mümkün kılabilir. Bu da kullanıma yönelik tutumu dolayısıyla niyeti etkileyebilmektedir (Davis vd., 1989, s.987).



Şekil 5.1: Orijinal Teknoloji Kabul Modeli.

[Davis, 1985, s.24]



Şekil 5.2: Yaygın Kullanılan Teknoloji Kabul Modeli.

[Davis vd., 1989, s.985]

Özetle TKM'nin temel amacı; dış faktörlerin iç inançlar (algılanan fayda ve algılanan kullanım kolaylığı), tutumlar ve niyetler üzerindeki ve dolayısıyla da gerçekleşen davranış üzerindeki etkisinin tespit edilmesini sağlamaktır. Söz konusu model, ilk geliştirilen ve literatürde yaygın kullanılan gösterimleri itibarıyla Şekil 5.1 ve Şekil 5.2'de verilmiştir.

### 5.5.3 Teknoloji Kabul Modeli ve Blokzincir ile ilgili Çalışmalar

Blokzincir teknolojisi kabulünün teknoloji kabul modeli ile ölçülmesi konulu çalışmaların araştırılması amacıyla sistematik literatür taraması yapılmıştır. Bu amaçla EBSCO Host, Scopus ve Web of Science (WOS) veri tabanları 2008<sup>56</sup> yılı itibarıyla ve sadece İngilizce ve Türkçe kaynaklar olmak üzere ilk aşamada öncelikle {*“Blockchain Technology” AND “Technology Acceptance Model”*} ve ikincil olarak {*And Not “Theory of planned behavior” OR “Theory of reasoned action” OR “UTAUT” OR “education” OR “election”*} arama sorgusu ile taranmıştır. İkinci aşamada ise *“Blockchain - Blockchain Technology - Technology Acceptance Model – TAM – Technology Adoption”* anahtar kelimeleri ve Scopus'da *“Business, Management and Accounting, Social Sciences ve Economics, Econometrics and Finance”* ile WOS'da *“Management, Business, Social Sciences Interdisciplinary ve Economics”* alanları filtrelenerek tarama yapılmıştır.

EBSCO Host, Scopus ve WOS veri tabanlarına en son güncel olarak 28.03.2024 tarihinde erişim sağlanmıştır. Başlangıçta yapılan gelişmiş kaynak taraması sonucunda ilk aşamada Ebsco Host'ta 24 adet, Scopus'da 43 adet ve WOS'da 33 adet yayına ulaşılmıştır. Bu yayınların anahtar kelime ve alan açısından yapılan ikinci taramaları sonrasında da “Blokzincir teknolojisinin benimsenmesinde teknoloji kabul modeli uygulamasını” içeren Ebsco Host'ta 11 adet, Scopus'da 17 adet ve WOS'da 16 adet yayın tespit edilmiştir.

Toplam 44 adetlik yayın listesi içinde mükerrer olan 10 adet yayın bulunmaktadır. Mükerrer olanlar birleştirildikten sonra söz konusu veri tabanlarında tespit edilen yayınlara ait künye ve çalışma alanları Tablo 5.2'de sıralanmıştır:

---

<sup>56</sup> Blokzincir kavramının 2008 yılı itibarıyla ortaya çıkması sebebiyle başlangıç tarihi 2008 yılı olarak dikkate alınmıştır.

**Tablo 5.2:** Blokzincir Teknolojisi Kabulünün Teknoloji Kabul Modeli (TKM) ile Ölçülmesi  
Konusunda Yapılan Yayınlar ve Çalışma Alanları.

|   | Yazar                                         | Çalışmanın Başlığı                                                                                                                         | Yayın Yeri                                                        | Yayın Yılı | Veri Tabanı | Çalışma Alanı                                                                                                |
|---|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|------------|-------------|--------------------------------------------------------------------------------------------------------------|
| 1 | Chen                                          | Extending the Technology Acceptance Model: A New Perspective on the Adoption of Blockchain Technology.                                     | Human Behavior & Emerging Technologies                            | 2023       | EBSCO HOST  | Tayvan - Menkul Kıymetler Borsası şirketleri                                                                 |
| 2 | Altalhi & Basiouni                            | Blockchain Technology Adoption in Canadian Pharmaceutical Sectors: An empirical analysis for a future outlook                              | Journal of Pharmaceutical Negative Results                        | 2022       | EBSCO HOST  | Kanada - Eczacılık Kuruluşları                                                                               |
| 3 | Zhang, Shi & Zhang                            | Blockchain-enabled Q&A communities: the impact of task technology matching on willingness to share knowledge.                              | Neural Computing & Applications                                   | 2024       | EBSCO HOST  | Blokzincir teknolojisine dayalı çevrimiçi platformlarda kullanıcıların bilgi paylaşımı kabulü                |
| 4 | Chowdhury, Rodriguez-Espindola, Dey & Budhwar | Blockchain technology adoption for managing risks in operations and supply chain management: evidence from the UK                          | Annals of Operations Research                                     | 2022       | EBSCO HOST  | Birleşik Krallık - Operasyon ve Tedarik Zinciri Yöneticileri                                                 |
| 5 | Semenova                                      | Technology Adoption Theories In Examining The Uptake Of Blockchain Technology In The Framework Of Functionalist And Interpretive Paradigms | Budapest Management Review                                        | 2020       | EBSCO HOST  | Tedarik Zinciri sistematik literatür taraması                                                                |
| 6 | Kumar Bhardwaj, Garg & Gajpal                 | Determinants of Blockchain Technology Adoption in Supply Chains by Small and Medium Enterprises (SMEs) in India                            | Mathematical Problems in Engineering                              | 2021       | EBSCO HOST  | Hindistan - İmalat ve hizmet sektöründeki KOBİ'lerin Tedarik Zinciri Yönetiminde blokzincir kabulü           |
| 7 | Yang                                          | Maritime shipping digitalization: Blockchain based technology applications, future improvements, and intention to use                      | Transportation Research Part E: Logistics & Transportation Review | 2019       | EBSCO HOST  | Tayvan- Deniz taşımacılığı tedarik zincirinde blokzincir teknolojisi kabulü                                  |
| 8 | Mohd Nor, Abdul-Majid & Esrati                | The role of blockchain technology in enhancing Islamic social finance: the case of Zakah management in Malaysia                            | Foresight                                                         | 2021       | EBSCO HOST  | Malezya-Zekât kurumları, JAWHAR ve üniversitelerde zekât yönetim sisteminde blokzincir teknolojisinin kabulü |
| 9 | Palos-Sanchez, Saura & Ayestaran              | An Exploratory Approach to the Adoption Process of Bitcoin by Business Executives                                                          | Mathematics                                                       | 2021       | EBSCO HOST  | Madrid - İspanyol işletme yöneticilerinin Bitcoin kripto para birimini kabulü                                |



**Tablo 5.2:** Blokzincir Teknolojisi Kabulünün Teknoloji Kabul Modeli (TKM) ile Ölçülmesi Konusunda Yapılan Yayınlar ve Çalışma Alanları (Devam).

|    | Yazar                                             | Çalışmanın Başlığı                                                                                                         | Yayın Yeri                                            | Yayın Yılı | Veri Tabanı         | Çalışma Alanı                                                                                                |
|----|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|------------|---------------------|--------------------------------------------------------------------------------------------------------------|
| 10 | Corne, Massot & Merasli                           | The determinants of the adoption of blockchain technology in the tourism sector and metaverse perspectives.                | Information Technology and Tourism                    | 2023       | SCOPUS              | Turizm konaklama sektöründe turizm yönetimi mezunlarının ve profesyonellerinin blokzincir teknolojisi kabulü |
| 11 | Bandinelli, Scozzafava, Bindi & Fani              | Blockchain and consumer behaviour: Results of a Technology Acceptance Model in the ancient wheat sector.                   | Cleaner Logistics and Supply Chain                    | 2023       | SCOPUS              | İtalya - Tarımsal gıda sektöründe antik buğday tedarik zincirinde blokzincir kullanımında tüketici kabulü.   |
| 12 | Tseng, Liang & Nguyen                             | Blockchain technology adoption and business performance in large enterprises: A comparison of the United States and China. | Technology in Society                                 | 2023       | SCOPUS / WOS        | ABD ve Çin - Fortune 500 şirketleri                                                                          |
| 13 | Shbail, Bani-Khalid, Ananzeh, Al-Hazaima & Shbail | Technostress impact on the intention to adopt blockchain technology in auditing companies.                                 | Journal of Governance and Regulation                  | 2023       | SCOPUS              | Ürdün - Denetim firması çalışanları                                                                          |
| 14 | Esfahbodi, Pang & Peng                            | Determinants of consumers' adoption intention for blockchain technology in E-commerce.                                     | Journal of Digital Economy                            | 2022       | SCOPUS              | Çin - E-ticarette tüketicilerin blokzincir teknolojisi kabulü                                                |
| 15 | Sciarelli, Prisco, Gheith & Muto                  | Factors affecting the adoption of blockchain technology in innovative Italian companies: an extended TAM approach.         | Journal of Strategy and Management                    | 2022       | SCOPUS / WOS        | İtalya - yenilikçi KOBİ'ler                                                                                  |
| 16 | Singh, Jain, Kumar & Hashimy                      | Blockchain Technology in the Fashion Industry: Virtual Proximity to Business.                                              | Journal of Electronic Commerce in Organizations       | 2022       | SCOPUS / WOS        | Hindistan - Lüks giyim sektöründe blokzincir kullanımının çevrimiçi tüketiciler tarafından kabulü            |
| 17 | Moghrabi & Benameur                               | Determinants for the utilisation of blockchain technologies for accounting in Kuwait                                       | International Journal of Business Information Systems | 2022       | SCOPUS              | Kuveyt - Muhasebe uygulamalarında blokzincir teknolojisi kullanımının benimsenmesi                           |
| 18 | Ben Amor & Ben Yahia                              | Investigating Blockchain Technology Effects on Online Platforms Transactions: Do Risk Aversion and Technophilia Matter?    | Journal of Internet Commerce                          | 2022       | EBSCO HOST / SCOPUS | Blokzincir tabanlı çevrimiçi platformların tüketiciler tarafından kabulü                                     |

**Tablo 5.2:** Blokzincir Teknolojisi Kabulünün Teknoloji Kabul Modeli (TKM) ile Ölçülmesi  
Konusunda Yapılan Yayınlar ve Çalışma Alanları (Devam).

|    | Yazar                                            | Çalışmanın Başlığı                                                                                                                                      | Yayın Yeri                                                                                       | Yayın Yılı | Veri Tabanı  | Çalışma Alanı                                                                                                |
|----|--------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|------------|--------------|--------------------------------------------------------------------------------------------------------------|
| 19 | Tan & Sundarakan                                 | Assessing Blockchain Technology application for freight booking business: a case study from Technology Acceptance Model perspective.                    | Journal of Global Operations and Strategic Sourcing                                              | 2021       | SCOPUS / WOS | Singapur - ECU Worldwide nakliye şirketi                                                                     |
| 20 | Kamble, Gunasekaran, Kumar, Belhadi & Foropon    | A machine learning based approach for predicting blockchain adoption in supply Chain                                                                    | Technological Forecasting and Social Change                                                      | 2021       | SCOPUS / WOS | Hindistan - İmalat sektöründe tedarik zincirinde blokzincir kullanımının benimsenmesi                        |
| 21 | Hsieh & Poh                                      | Factors influencing the adoption of blockchain technology in supply chain management: a preliminary study                                               | Proceedings of the 25th International Conference of Hong Kong Society for Transportation Studies | 2021       | SCOPUS       | Tedarik zincirinde blokzincir teknolojisi kabulü                                                             |
| 22 | Albayati, Kim & Rho                              | Accepting financial transactions using blockchain technology and cryptocurrency: A customer perspective approach.                                       | Technology in Society                                                                            | 2020       | SCOPUS / WOS | Küresel çapta bankacılık ve finans sektöründe blokzincir teknolojisinin benimsenmesi                         |
| 23 | Jain, Singh, Chaturvedi & Rakesh                 | Blockchain in logistics industry: in fizza customer trust or not                                                                                        | Journal of Enterprise Information Management                                                     | 2020       | SCOPUS / WOS | Hindistan - Lojistik sektöründe tedarik zincirinde blokzincir teknolojisinin benimsenmesi                    |
| 24 | Nuryyev, Wang, Achyldurdyeva, Jaw, Yeh, Lin & Wu | Blockchain technology adoption behavior and sustainability of the business in tourism and hospitality SMEs: An empirical study.                         | Sustainability (Switzerland)                                                                     | 2019       | SCOPUS       | Tayvan - Turizm ve konaklama sektöründe KOBİ'ler arası kripto para ödemelerinin benimsenmesi                 |
| 25 | Lou & Li                                         | Integrating innovation diffusion theory and the technology acceptance model: The adoption of blockchain technology from business managers' perspective. | Proceedings of the International Conference on Electronic Business (ICEB)                        | 2017       | SCOPUS       | Tayvan - işletme yöneticilerinin blokzincir teknolojisini kullanma niyetlerini etkileyen unsurları belirleme |

**Tablo 5.2:** Blokzincir Teknolojisi Kabulünün Teknoloji Kabul Modeli (TKM) ile Ölçülmesi  
Konusunda Yapılan Yayınlar ve Çalışma Alanları (Devam).

|    | Yazar                               | Çalışmanın Başlığı                                                                                                                                   | Yayın Yeri                                          | Yayın Yılı | Veri Tabanı      | Çalışma Alanı                                                                                                                                   |
|----|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 26 | Liu & Ye                            | Empirical research on the blockchain adoption-based on TAM                                                                                           | Applied Economics                                   | 2021       | SCOPUS / WOS     | Öğrenci, öğretmen ve işletme çalışanları - Blokzincir teknolojisinin teknik özelliklerinin kullanıcı kabulü üzerindeki etkilerinin belirlenmesi |
| 27 | Amor & Yahia                        | Investigating Blockchain Technology Effects on Online Platforms Transactions: Do Risk Aversion and Technophilia Matter?                              | Journal of Internet Commerce                        | 2021       | WOS              | Tüketicilerin, blokzincir teknolojisine dayalı çevrimiçi platformları benimsemesi                                                               |
| 28 | Prisco, Abdallah, Morande & Gheith  | Factors affecting blockchain adoption in Italian companies: the moderating role of firm size.                                                        | Technology Analysis & Strategic Management          | 2022       | EBSCO HOST / WOS | İtalyan şirketlerinde blokzincir teknolojisinin benimsenmesi                                                                                    |
| 29 | Bracci, Tallaki, Ievoli & Diplotti  | Knowledge, diffusion and interest in blockchain technology in SMEs                                                                                   | Journal of Knowledge Managment                      | 2022       | WOS              | İtalya- KOBİ'lerin blokzincir teknolojisi kabulü                                                                                                |
| 30 | Maniam, Prentice, Sassenberg & Soar | Identifying an Optimal Model for Blockchain Technology Adoption in the Agricultural Sector                                                           | Logistics                                           | 2023       | WOS              | Avustralya- Tarım sektöründe tedarik zincirinde blokzincir teknolojisinin kabulü                                                                |
| 31 | Kabir                               | Behavioural intention to adopt blockchain for a transparent and effective taxing system                                                              | Journal of Global Operations and Strategic Sourcing | 2021       | WOS              | Bangladeş- vergi sistemi paydaşlarının blokzincir teknolojisi kabulü                                                                            |
| 32 | Giri & Mannhar                      | Factors influencing the acceptance of private and public blockchain-based collaboration among supply chain practitioners: a parallel mediation model | Supply Chain Management: An International Journal   | 2023       | WOS              | Hindistan - İmalat ve lojistik sektörlerinde tedarik zincirinde özel ve kamu blokzincir teknolojisi tabanlı iş birliklerinin kabul              |
| 33 | Mofokeng, Mbeya & Maduku            | Bitcoin adoption in online payments: examining consumer intentions and word-of-mouth recommendations                                                 | Future Business Journal                             | 2024       | WOS              | Güney Afrika- Çevrimiçi işlemlerde tüketicilerin Bitcoin kullanımını benimsemesi                                                                |
| 34 | Shahzad, Xu, Lim, Hasnain & Nusrat  | Cryptocurrency awareness, acceptance, and adoption: the role of trust as a cornerstone                                                               | Humanities And Social Sciences Communicati ons      | 2024       | WOS              | Pakistan- Lahor kentinde yaşayan üniversite öğrencileri, çalışanlar ile işletme sahiplerinin kripto para birimini kullanım kabulü               |

TKM aracılığıyla blokzincir teknolojisi kullanımının benimsenmesine yönelik yapılan ve Tablo 5.2’de verilen listede yer alan 34 adet yayının alanları ve yayın sayılarına göre dağılımını incelediğimizde; tedarik zinciri yönetiminde 11 adet, pazarlama alanında 6 adet, genel işletme süreçlerinde 6 adet, finans sektöründe 5 adet, turizm sektöründe 2 adet ve sağlık, vergi, muhasebe ve denetim alanlarında birer adet çalışma bulunduğu görülmektedir. Buna göre; TKM ile blokzincir teknolojisi kabulü, en çok tedarik zinciri yönetiminde, en az ise sağlık sektöründe araştırılmıştır. Sağlık sektörünün çalışma alanı dışında olması dikkate alındığında; vergi, muhasebe ve denetim alanlarının literatürde en az çalışılan alanlar olduğu anlaşılmaktadır. Diğer yandan Türk yazınında TKM ile blokzincir teknolojisi kabulünün ölçülmesine yönelik yapılmış herhangi bir çalışma bulunmamaktadır. Dolayısıyla sistematik literatür tarama sonuçları itibarıyla bu çalışma, mali müşavirlerin TKM ile blokzincir teknolojisi kabulünü ölçen alan yazındaki nadir çalışmalardan biri iken; Türk literatüründeki ilk çalışma olma özelliğini taşımaktadır.

## 6. ARAŞTIRMANIN YÖNTEMİ

Bu bölümde araştırmanın yöntemi açıklanmaktadır. Bu kapsamda kullanılan ölçeklere bağlı olarak oluşturulan araştırma modeli ve hipotezlerine, araştırma evreni ve örneklem planına, veri toplama yöntemlerine ve araştırmada kullanılan veri analiz yöntemlerine ilişkin açıklamalar yer almaktadır.

### 6.1 ARAŞTIRMANIN MODELİ VE HİPOTEZLERİ

#### 6.1.1 Araştırmanın Hipotezleri

Belirlenmiş olan toplam 37 adet araştırma hipotezi, kullanılan ölçekler bazında aşağıda sıralanmış olan dört gruba ayrılarak oluşturulmuştur :

- a. Teknoloji Kabul Modeli Hipotezleri (Technology Acceptance Model-TAM): Hipotez 1'den Hipotez 12'ye kadar olan 12 adet hipotezi içermektedir.
- b. Sosyo-Demografik ve Mesleki Özellikler - Teknoloji Kabul Modeli Boyutları Hipotezleri: Hipotez 13'ten Hipotez 24'e kadar olan 12 adet hipotezi içermektedir.
- c. ACFE (The Association of Certified Fraud Examiner) Hile Araştırmaları Ölçeği Hipotezleri: Hipotez 25'ten Hipotez 30'a kadar olan 6 adet hipotezi içermektedir.
- d. İşgüden Kılıç & Anadolu (2018) Tarafından Hazırlanan Muhasebe Hilelerinin Önlenmesinde Kullanılan Araçlara Yönelik Makalede Kullanılan Ölçek Hipotezleri: Hipotez 31'den Hipotez 37'ye kadar olan 7 adet hipotezi içermektedir.

##### 6.1.1.1 Teknoloji Kabul Modeli hipotezleri

Araştırma kapsamında Davis (1989) tarafından geliştiren Teknoloji Kabul Modeli'nde yer alan dışsal değişkenler olarak, yeni teknolojinin benimsenmesinin önündeki engeller modele eklenerek, dış değişkenlerin tutumu, niyeti ve davranışı negatif yönde etkilediği algılanan kullanım kolaylığı ile algılanan faydanın tutum, niyet ve davranış biçimlerini pozitif yönde etkisinin olduğu düşünülmektedir. Bu araştırmada bağımsız değişken olan Niyet, Tutum, Engeller, Algılanan Kullanım Kolaylığı ile Algılanan Faydanın, bağımlı değişken olan Davranışı etkileyip etkilemediği araştırılmıştır. Yapılan bu araştırma nicel bir araştırma deseni olarak tasarlanmıştır.

**H1:** Dış deęişkenler (engeller), mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumunu negatif yönde etkilemektedir.

**H2:** Algılanan fayda, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumunu pozitif yönde etkilemektedir.

**H3:** Algılanan kullanım kolaylığı, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumunu pozitif yönde etkilemektedir.

**H4:** Dış deęişkenler, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik niyetini negatif yönde etkilemektedir.

**H5:** Algılanan fayda, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik niyetini pozitif yönde etkilemektedir.

**H6:** Algılanan kullanım kolaylığı, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik niyetini pozitif yönde etkilemektedir.

**H7:** Mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumları, niyetlerini pozitif yönde etkilemektedir.

**H8:** Dış deęişkenler (engeller), mali müşavirlerin blokzincir teknolojisi kullanım davranışını negatif yönde etkilemektedir.

**H9:** Algılanan fayda, mali müşavirlerin blokzincir teknolojisi kullanım davranışını pozitif yönde etkilemektedir.

**H10:** Algılanan kullanım kolaylığı, mali müşavirlerin blokzincir teknolojisi kullanım davranışını pozitif yönde etkilemektedir.

**H11:** Mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumları, kullanım davranışını pozitif yönde etkilemektedir.

**H12:** Mali müşavirlerin blokzincir teknolojisi kullanımına yönelik niyetleri, kullanım davranışını pozitif yönde etkilemektedir.

### **6.1.1.2 Demografik ve mesleki özelliklere göre Teknoloji Kabul Modeli boyutlarının farklılık analizine yönelik ölçek hipotezleri**

İstanbul'daki mali müşavirlerin (a) Cinsiyet ve (b) Ünvan demografik ve meslek özelliklerinin, Teknoloji Kabul Modeli kapsamında blokzincir teknolojisi kullanımına ilişkin (a) Dış Etkenler (Algılanan Engeller), (b) Algılanan Fayda, (c) Algılanan Kullanım Kolaylığı, (d) Tutum, (e) Niyet ve (f) Davranış değişkenleri üzerinde farklılık yaratıp yaratmadığı araştırılmıştır. Yapılan bu araştırma nicel bir araştırma deseni olarak tasarlanmıştır.

**H13:** Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımında algılanan dış etkenler (engeller) arasında anlamlı bir fark vardır.

**H14:** Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımında algılanan fayda arasında anlamlı bir fark vardır.

**H15:** Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımında algılanan kullanım kolaylığı arasında anlamlı bir fark vardır.

**H16:** Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik tutumları arasında anlamlı bir fark vardır.

**H17:** Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik niyetleri arasında anlamlı bir fark vardır.

**H18:** Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik davranışları arasında anlamlı bir fark vardır.

**H19:** Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımında algılanan dış etkenler (engeller) arasında anlamlı bir fark vardır.

**H20:** Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımında algılanan fayda arasında anlamlı bir fark vardır.

**H21:** Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımında algılanan kullanım kolaylığı arasında anlamlı bir fark vardır.

**H22:** Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımına yönelik tutumları arasında anlamlı bir fark vardır.

**H23:** Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımına yönelik niyetleri arasında anlamlı bir fark vardır.

**H24:** Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımına yönelik davranışları arasında anlamlı bir fark vardır.

#### **6.1.1.3 ACFE hile araştırmaları ölçeği hipotezleri**

İstanbul'daki mali müşavirlerin (a) Cinsiyet, (b) Eğitim Düzeyi, (c) Mesleki Ünvan, (d) Çalışma Şekli, (e) Mesleki Tecrübe ve (f) Mükellef Sayısı demografik ve mesleki özelliklerinin, finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklıkları üzerinde farklılık yaratıp yaratmadığı araştırılmıştır. Yapılan bu araştırma nicel bir araştırma deseni olarak tasarlanmıştır.

**H25:** Mali müşavirlerin cinsiyeti ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır.

**H26:** Mali müşavirlerin eğitim düzeyi ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır.

**H27:** Mali müşavirlerin mesleki ünvanı (SMMM – YMM) ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır.

**H28:** Mali müşavirlerin çalışma şekli (bağımlı – bağımsız) ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır.

**H29:** Mali müşavirlerin mesleki tecrübesi (çalışma süresi) ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır.

**H30:** Mali müşavirlerin mükellef sayısı ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır.



#### **6.1.1.4 İşgüden Kılıç & Anadolu (2018) tarafından hazırlanan muhasebe hilelerinin önlenmesinde kullanılan araçlara yönelik makalede kullanılan ölçek hipotezleri**

İstanbul'daki mali müşavirlerin (a) Cinsiyet, (b) Eğitim Düzeyi, (c) Mesleki Ünvan, (d) Çalışma Şekli, (e) Mesleki Tecrübe, (d) Mükellef Sayısı ve (e) Blokzincir Bilgi Düzeyi demografik ve meslek özelliklerinin, blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşlerinde farklılık yaratıp yaratmadığı araştırılmıştır. Yapılan bu araştırma nicel bir araştırma deseni olarak tasarlanmıştır.

**H31:** Mali müşavirlerin cinsiyeti ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.

**H32:** Mali müşavirlerin eğitim düzeyi ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.

**H33:** Mali müşavirlerin ünvanı ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.

**H34:** Mali müşavirlerin çalışma şekli (bağımlı – bağımsız) ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.

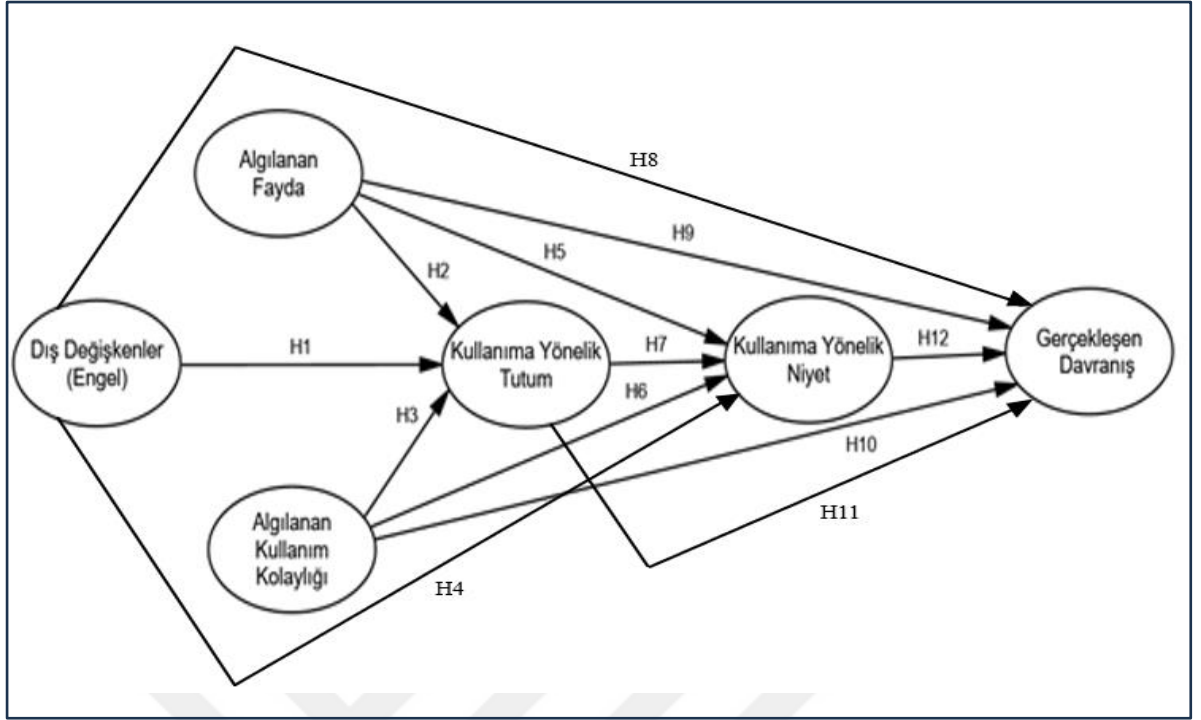
**H35:** Mali müşavirlerin mesleki tecrübesi (çalışma süresi) ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.

**H36:** Mali müşavirlerin mükellef sayısı ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.

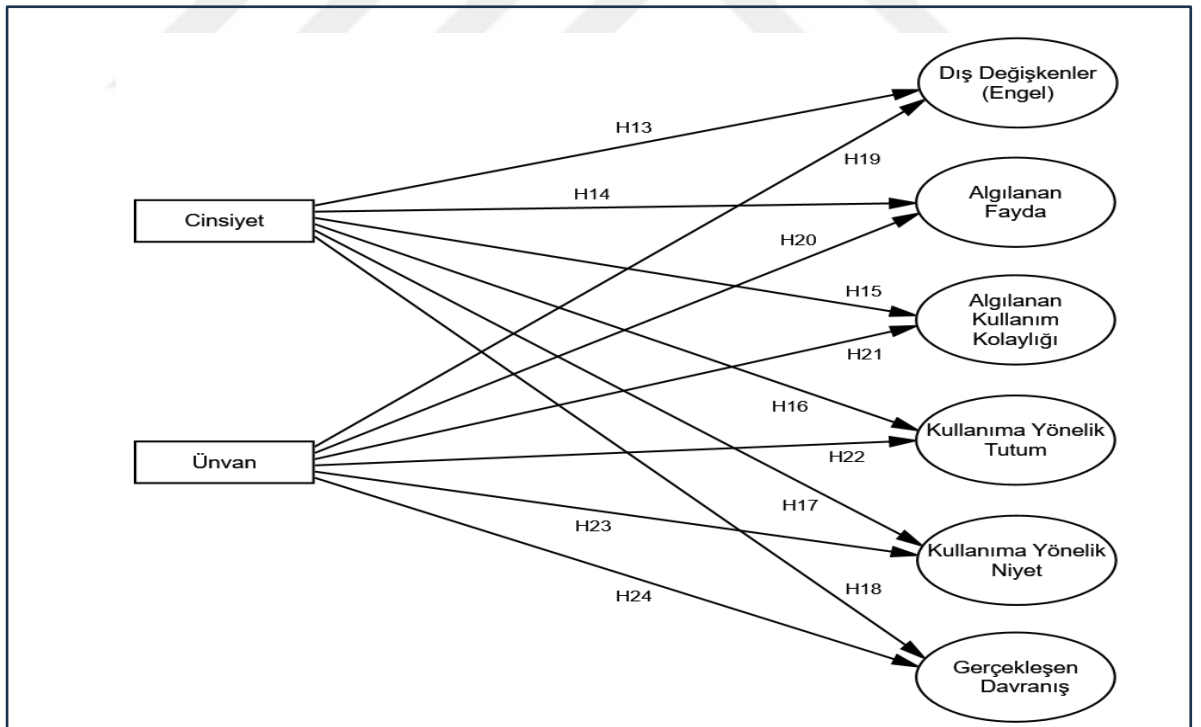
**H37:** Mali müşavirlerin blokzincir bilgi düzeyi ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.

#### **6.1.2 Araştırmanın Modeli**

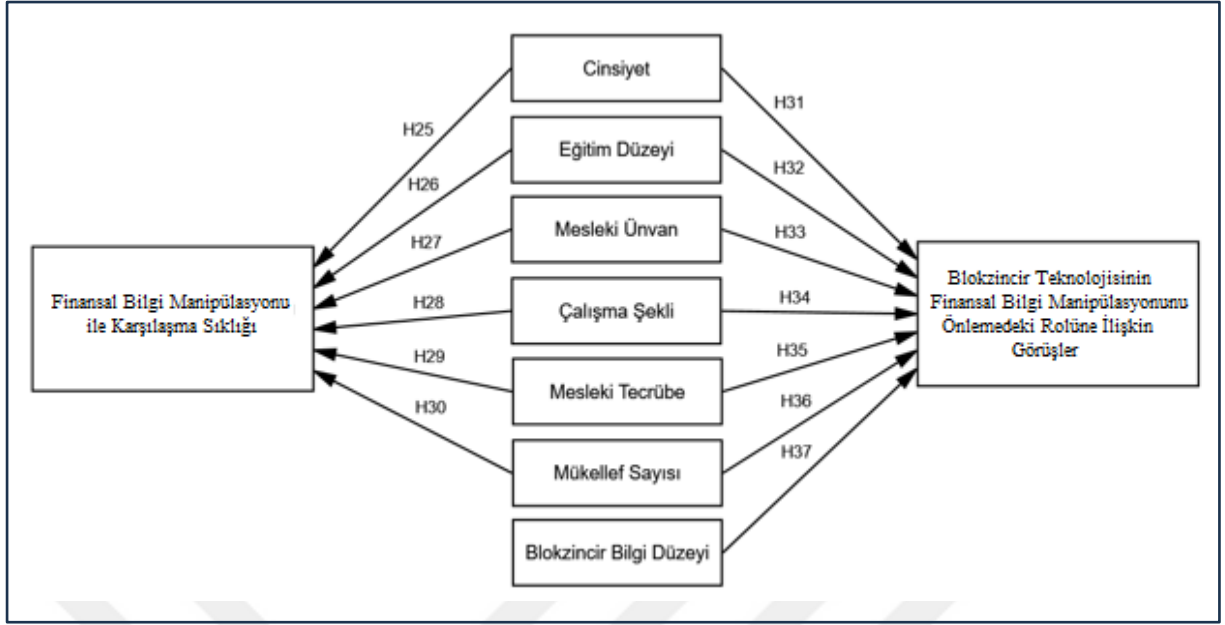
Bu çalışmada kullanılan TKM ve Hile Araştırmaları ölçekleri itibarıyla oluşturulan araştırma modelleri aşağıdaki Şekil 6.1, Şekil 6.2 ve Şekil 6.3'te gösterilmiştir.



Şekil 6.1: TKM Araştırma Modeli-1.



Şekil 6.2: TKM Araştırma Modeli-2.



Şekil 6.3: Hile Araştırmaları Ölçeği Araştırma Modeli.

## 6.2 ARAŞTIRMA EVRENİ VE ÖRNEKLEM PLANI

Bu araştırmanın evreni, örnekleme çerçevesi, örnekleme bireyleri, örnekleme yöntemi ve örneklem büyüklüğüne ilişkin bilgiler aşağıda maddeler halinde belirtilmiştir:

- Araştırma Evreni: İstanbul'daki Serbest Muhasebeci Mali Müşavirler (SMMM) ve Yeminli Mali Müşavirler (YMM)
- Örnekleme Çerçevesi: Türkiye Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali Müşavirler Odaları Birliği (TÜRMOB) Üye İstatistikleri (<https://turmob.org.tr/>)
- Örnekleme Bireyleri : 2023 yılı verilerine göre 46.888 kişisi SMMM ve 2.338 kişisi YMM olmak üzere İstanbul'daki toplam 49.226 adet meslek mensubu (<https://turmob.org.tr/>)
- Örneklem Büyüklüğü: Anakütledeki birey sayısının bilindiği durumlarda kullanılan aşağıdaki formül yardımıyla örneklem büyüklüğü hesaplanmıştır. Buna göre %95 güven düzeyinde ve %5 örneklem hatası ile SMMM ve YMM örneklem hacminin 381 (formül 1'e göre hesaplanan) meslek mensubu olması gerekmektedir.

$$n = \frac{N t^2 p q}{d^2 (N - 1) + t^2 p q} = \frac{49.226 (1.96)^2 (0.5) (0.5)}{(0.05)^2 (49.226 - 1) + (1.96)^2 (0.5) (0.5)} = 381 \quad (1)$$

**N:** Anakütle hacmi,

**n:** Örneklem hacmi,

**p:** İncelenen olayın görülme sıklığı,

**q:** İncelenen olayın görülmeme sıklığı,

**t:** Belirli bir güven düzeyinde, t tablosuna göre bulunan teorik değer,  
(%95 güven düzeyi için bu değer 1.96'dır.)

**d:** Örneklem hatası.

Diğer yandan Saunders, Lewis ve Thornhill (2003)'e göre 10.000 üzerindeki evren büyüklüklerinde, örneklem hacminin 370 ve üzeri olması da yeterli kabul edilmektedir (Gegez vd., 2023, s.341).

Bu çalışmada ise anket uygulamasına katılım gösteren 512 kişiye ulaşılmıştır. Ancak 62 kişi, yalnızca Bölüm 1: Demografik Bilgiler ve Bölüm 2: Teknolojik Ürünleri Kullanma Sıklığı sorularını cevaplandırmış; 42 kişi ise, blokzincir teknolojisi hakkında bilgi sahibi olmadıklarını belirterek Bölüm 3: Blokzincir Teknolojisinin Muhasebe Mesleğine Etkisi ve Bölüm 6: Blokzincir Teknolojisinin Muhasebe Hilelerini Önlemedeki Rolü sorularını cevaplandırmamışlardır. Söz konusu cevaplamama hatası dolayısıyla bu 104 adet katılımcı örneklem dışı bırakılmıştır. Bu durumda örneklem hacmi, 408 meslek mensubu olarak belirlenmiş olup bu sayı 370 adetlik asgari olması gereken büyüklüğü aştığından yeterli kabul edilmiştir.

- e. Örneklem Yöntemi: Örneklem seçiminde iki aşamalı örneklem yöntemi uygulanmıştır. İlk aşamada “tesadüfi zümrelere göre (tabakalı) örneklem yöntemi” uygulanmış ve örnek hacminin belirlenmesinde SMMM ve YMM’lerin toplam meslek mensupları içindeki payları dikkate alınarak “doğru orantılı oransal örneklem” ile örnek hacmi hesaplanmıştır. Türkiye Serbest Muhasebeci Mali Müşavirler ve Yeminli Mali Müşavirler Odaları Birliği (TÜRMOB) Üye İstatistikleri 2023 yılı verilerine göre İstanbul’da 46.888 adet SMMM ve 2.338 adet YMM olmak üzere toplam 49.226 adet

mali müşavir meslek mensubu bulunmaktadır. Dolayısıyla toplam meslek mensupları içinde SMMM’lerin payı  $\%95,25 \cong \%95$  iken, YMM’lerin payı  $\%4,75 \cong \%5$ ’tir. Buna göre SMMM başına  $381 * 0,95 = 362$  ve YMM başına  $381 * 0,05 = 19$  adetten oluşan örnek hacmi belirlenmiştir. İkinci aşamada ise “tesadüfi olmayan kolayda ve kartopu örneklem yöntemleri” uygulanarak asgari toplam 381 adetlik katılımcı hacmine ulaşılması hedeflenmiştir. Cevaplamama hataları dolayısıyla örneklem dışı bırakılan örnekler sonrasında ise 374 adet SMMM ve 34 adet YMM katılımı ile örnekleme gerçekleşmiş ve bu sayılar oransal örnekleme ile tespit edilen asgari büyüklükleri aştığından yeterli kabul edilmiştir.

Ayrıca örneklem seçiminde, İstanbul’da faaliyet gösteren tüm mali müşavir meslek mensupları evreninden, en az 1 yıllık mesleki uzmanlık ve tecrübenin araştırma sonuçlarının doğruluk ve geçerliliğini arttıracak gerekçesi ile Haziran 2022 öncesinde Serbest Muhasebeci Mali Müşavirlik (SMMM) ruhsatı almış olanlar ile dışta bırakma olmaksızın YMM ruhsatı olanlar (kanunen YMM olmadan önce SMMM olunması gerektiğinden - istisnai durumlar hariç – uzmanlık ve tecrübe kriteri sağlanmaktadır) dikkate alınmıştır. SMMM stajyerleri ve Serbest Muhasebeciler (SM) ise uzmanlık ve tecrübe kısıtı sebebiyle örnekleme dâhil edilmemişlerdir.

### **6.3 ARAŞTIRMADA KULLANILAN VERİ TOPLAMA YÖNTEMLERİ**

Bu araştırmada tanımlayıcı araştırma yöntemi kullanıldığından nicel veri toplama yöntemleri uygulanmıştır. Kullanılan veri toplama yöntemleri nedenleri ile birlikte aşağıda sınıflandırılmıştır.

#### **6.3.1 Döküman İnceleme**

Bu yöntem, finansal bilgi manipülasyonu, blokzincir teknolojisi ve teknoloji kabul modelleri kavramlarının literatür taramalarına ilişkin veri toplamak amacıyla kullanılmıştır. Toplanan veri ikincil veri niteliğinde olduğundan döküman inceleme yöntemi kullanılmıştır.

### 6.3.2 Anket

Bu yöntem, hipotezlere (H1-H37) ilişkin veri toplamak amacıyla kullanılmıştır.

H1-H12 arasındaki hipotezler ile mali müşavirlerin algıladıkları engel, fayda ve kullanım kolaylıklarının blokzincir teknolojisi kabulüne ilişkin tutum, niyet ve davranışları üzerindeki etki boyutu; H13-H24 arasındaki hipotezler ile mali müşavirlerin “sosyo-demografik özellik” olan cinsiyet ve “mesleki özellik” olan unvan değişkenlerinin TKM boyutları üzerinde farklılık yaratıp yaratmadığı ve son olarak H25-H37 arasındaki hipotezler ile ise, demografik ve mesleki özelliklerinin finansal bilgi manipülasyonu ile karşılaşma sıklığı ve önleme faaliyeti olarak blokzincir teknolojisini kullanma eğilimi üzerinde farklılık yaratıp yaratmadığı ölçülmüştür.

#### 6.3.2.1 Anket formunun yapısı

Anket altı bölümden oluşmaktadır. İlk bölümde katılımcıların “Demografik Bilgilerine” yönelik sorular, ikinci bölümde “Teknolojik Ürün Kullanma Sıklığı”na yönelik sorular, üçüncü bölümde “Blokzincir Teknolojisinin Muhasebe Mesleğine Etkisi”ne yönelik sorular, dördüncü bölümde “Hile Belirtileriyle Karşılaşma Sıklığı”na yönelik sorular, beşinci bölümde “Muhasebe Hilelerinin Önlenmesine Yönelik Faaliyetlere” ilişkin sorular ve altıncı bölümde ise “Blokzincir Teknolojisinin Muhasebe Hilelerini Önlemedeki Rolü”ne yönelik sorular yöneltilmiştir.

Birinci bölümde; katılımcıların cinsiyet ve eğitim durumu bilgilerinin yanı sıra mesleki unvanı, çalışma şekli, tecrübesi, mükellef sayısı, bağlı olduğu meslek odası bilgileri ve blokzincir teknolojisi hakkındaki bilgi düzeylerinin sorulduğu toplam 8 adet sorunun yanıtlanması istenmiştir.

İkinci bölümde; katılımcılara, teknolojik ürünlerden kimler aracılığıyla haberdar olduklarından bu ürünleri iş ve özel yaşamda kullanma eğilimlerine kadar teknolojik ürünleri kullanım sıklıklarını ölçmek amacıyla toplam 11 adet soru yöneltilmiştir.

Üçüncü bölümde; katılımcıların, blokzincir teknolojisinin muhasebe mesleğine etkisini engeller, algılanan fayda, algılanan kullanım kolaylığı, tutum, niyet ve davranışları olmak üzere altı boyutta 1= Hiç Katılmıyorum’dan 5= Kesinlikle Katılıyorum’a doğru sıralanan 5’li Likert tipi ölçek aracılığıyla ölçen toplam 28 adet soruyu cevaplamaları istenmiştir.

Dördüncü bölümde; katılımcıların, mesleki faaliyetleri sırasında karşılaştıkları hile belirtileri ve bu belirtilerle karşılaşma sıklıklarını 5’li Likert tipi ölçek aracılığıyla cevaplamalarının istendiği tek bir soru sorulmuştur. Buna göre birden fazla hile belirtisini seçebildikleri soruda her bir hile belirtisi için Hiçbir zaman= 1, Nadiren= 2, Bazen= 3, Sıklıkla= 4, Her zaman= 5 seçeneklerinden birini seçmek suretiyle soruyu yanıtlamaları istenmiştir.

Beşinci bölümde; dördüncü bölümdeki soru yapısı esasları çerçevesinde katılımcıların muhasebe hilelerinin önlenmesine yönelik faaliyetlerin hangisi veya hangilerinin faydalı olduğu ve fayda düzeylerine ilişkin tercihlerine yönelik yine tek bir soru sorulmuştur. Farklı olarak 5’li Likert tipi ölçekte seçenekler 1= Hiç Katılmıyorum’dan 5= Kesinlikle Katılıyorum’a doğru sıralanmıştır.

Altıncı bölümde ise katılımcıların, blokzincir teknolojisinin muhasebe hilelerini önlemedeki rolüne ilişkin görüşlerini belirlemek amacıyla 1= Hiç Katılmıyorum’dan 5= Kesinlikle Katılıyorum’a doğru sıralanan 5’li Likert tipi ölçek aracılığıyla toplam 11 adet soru yöneltilmiştir.

Ayrıca anket formunun biçimsel yapısı dışında anket formu aracılığıyla ölçülmek istenen verilerin doğruluğunu kanıtlamak amacıyla ankette yer alan ölçeklerin güvenilirlik ve geçerliliğine ilişkin açıklamaların da yapılması gerekmektedir. İlgili anket formu aracılığıyla katılımcıların hem blokzincir teknoloji kabul düzeyleri hem de blokzincir teknolojisinin muhasebe hilelerini önlemede kullanılmasına yönelik görüşleri ölçülmek istenmiştir. Dolayısıyla anket formunda iki ayrı ölçek bulunmaktadır. Bu bağlamda ankette yer alan sorular anket bölümleri itibarıyla aşağıdaki açıklamalar nezdinde güvenilirlik ve geçerlilik koşulları açısından olumlu olarak değerlendirilmektedir :

- a- Bölüm 1’deki sorular demografik özelliklere ilişkin veri toplamak amacıyla sorulduğundan açıklama dışında tutulmuştur.
- b- Bölüm 2 ve Bölüm 3 soruları, bu çalışmanın “5.5.2 Teknoloji Kabul Modeli” bölümünde detaylı olarak anlatılmış olan “Teknoloji Kabul Modeli (TKM / Technology Acceptance Model - TAM)” kapsamında Ös (2021) tarafından hazırlanan muhasebe mesleğinin Endüstri 4.0’a uyumunu ölçmeye yönelik doktora tezinde kullanılan uyarlanmış sorulardır.

- c- Bölüm 4 soruları, ACFE (The Association of Certified Fraud Examiner) tarafından 1996, 2002, 2004, 2006 ve 2008 yıllarında tekrarlanarak yapılan hile araştırmalarında kullanılan sorulardır.
- d- Bölüm 5 soruları, Yıldız ve Başkan (2014) tarafından yazılan “Muhasebe Hilelerinin Önlenmesinde Kullanılan Araçlar: BİST Şirketleri Üzerine Bir Araştırma” konulu makalede kullanılan sorulardır.
- e- Bölüm 6 soruları ise, Tokatlı (2014) tarafından hazırlanan Xbrl raporlama dilinin muhasebe bilgi sistemine etkilerini ölçmeye yönelik yüksek lisans tezinde kullanılan sorulardır.
- f- Bölüm 4, 5 ve 6 sorularının birlikte değerlendirilerek ölçek dahiline alınması İşgüden Kılıç ve Anadolu (2018) tarafından yazılan “Dijital Çağın Yarattığı Muhasebe Uygulamalarının Muhasebe Hilelerinin Önlenmesine Etkisi” konulu makalede gerçekleştirilerek geçerliliği ölçülmüştür.

#### **6.3.2.2 Anketin uygulanması**

Anket uygulamasının yapılabilmesi için ise yasal prosedür takip edilerek Üniversitemiz Etik Kurulu’na 07.07.2023 tarihinde başvuru yapılmış ve 19.07.2023 tarihli 53446 sayılı Etik Kurul Kararı (EK A) ile izin alınmıştır.

Etik Kurul izninin alınmasının ardından İstanbul Serbest Muhasebeci Mali Müşavirler Odası (İSMMM) ve İstanbul Yeminli Mali Müşavirler Odası (İYMMO) Başkanlıkları ile iletişime geçilerek 26-27.08.2023 tarihlerinde başvurular yapılmış, onaylar alınmış ve ilgili kurumlar aracılığıyla meslek mensuplarına ulaşılabilmesi için yasal prosedür tamamlanmıştır.

Söz konusu anket uygulamasının çevrimiçi olarak yapılabilmesi amacıyla Google Forms (<https://docs.google.com/forms/u/0/?tgif=d>) uygulaması üzerinden online anket formu oluşturulmuştur. Ve bu anket formuna ilişkin erişim bağlantısı, İYMMO tarafından resmi bilgilendirme mesajı dahilinde e-posta yolu ile üyelerine gönderilmesi şeklinde, İSMMM tarafından ise İSMMM’nun üyelerine yönelik resmi web sitesinin duyurular alanında (<https://ismmmo.org.tr/Uye>) paylaşılması şeklinde örnekleme dâhil olan tüm mali müşavir meslek mensuplarının katılımına sunulmuştur. (EK B’de ham hali yer almaktadır.) Diğer



yandan çevrimiçi anket yöntemi ile SMMM meslek mensubu grubunda yeterli katılımcıya ulaşamadığından ayrıca yüz yüze anket uygulamasının yapılması gerekliliği doğmuştur. Bu amaçla İSMMMO Başkanlığından, Odanın İstanbul geneli kapsamında düzenlemiş olduğu “Enflasyon Düzeltmesi Eğitimleri”nde anket formunun dağıtılması yönünde destek alınarak kâğıt anket formu örnekleme dâhil olan SMMM meslek mensuplarının katılımına sunulmuştur.

Veri toplama sürecinin sonunda, verilerin 86 adetlik kısmı 10.08.2023 - 19.02.2024 tarihleri arasında çevrimiçi anket yöntemi ile 426 adetlik kısmı ise 19.02.2024 - 24.02.2024 tarihleri arasında yüz yüze anket yöntemi ile toplanmış olup ankete toplam 512 kişi katılmıştır.

#### **6.4 ARAŞTIRMADA KULLANILAN VERİ ANALİZ YÖNTEMLERİ**

Bu çalışmada; meslek mensuplarının “blokzincir teknolojisini kabul düzeylerinin” ve “blokzincir teknolojisinin muhasebe hilelerini önlemedeki rolüne ilişkin görüşlerinin” ölçülmesine yönelik olmak üzere temelde iki ölçek kullanılmıştır. Blokzincir teknolojisi kabul düzeylerini ölçmek amacıyla “Teknoloji Kabul Modeli” ölçeği kullanılmış olup bu ölçek, metrik bir ölçektir ve TKM ölçeğine ait veriler normal dağılım gösterdiğinden parametrik yöntemler aracılığıyla analiz edilmiştir. Diğer yandan meslek mensuplarının blokzincirin teknolojisinin hile önlemede kullanılmasına ilişkin kullanılan ölçek de metrik bir ölçek olmakla birlikte; bu ölçeğe ait veriler, normal dağılım göstermediğinden parametrik olmayan yöntemler aracılığıyla analiz edilmiştir<sup>57</sup>.

Dolayısıyla bu çalışmada hem parametrik hem de parametrik olmayan analiz yöntemlerinden faydalanılmıştır. Aşağıdaki Tablo 6.1’de, ilgili araştırma hipotezleri kapsamında kullanılan parametrik ve parametrik olmayan analiz yöntemleri özetlenmiş ardından da bölüm alt başlıklarında ilgili yöntemlere ilişkin açıklamalar yapılmıştır.

---

<sup>57</sup> İlgili ölçeklerin normal dağılım gösterip göstermediklerine ilişkin detaylı açıklamalar, Bölüm 7: Araştırma Bulguları ve Yorum’da “Normallik Testi ve Tanımlayıcı İstatistik Bulguları” alt başlıklarında yapılmıştır. Bknz. s.258 ve s.286.

**Tablo 6.1:** Araştırmada Kullanılan Analiz Yöntemleri.

| Hipotez                                  | Dağılım      | Veri Analiz Yöntemi                              |
|------------------------------------------|--------------|--------------------------------------------------|
| TKM boyutlarına                          | Normal       | Doğrulayıcı Faktör Analizi<br>Korelasyon Analizi |
| H1'den H12'ye                            | Normal       | Standart Çoklu Regresyon Analizi                 |
| H13'ten H24'e                            | Normal       | Farklılık Analizi : T testi                      |
| H25 - H27 - H28 - H31<br>H33 - H34       | Normal değil | Farklılık Analizi : Mann-Whitney U testi         |
| H26 - H29 - H30 - H32<br>H35 - H36 - H37 | Normal değil | Farklılık Analizi : Kruskal Wallis testi         |

#### 6.4.1 Parametrik Testler

Parametrik testlerin uygulanabilmesi için; (i) verinin normal dağılması, (ii) kullanılan ölçeğin aralıklı veya oran ölçeği olması, (ii) homojen varyansa sahip olması ve (iv) cevapların birbirini etkilememesi gerekmektedir (Field, 2005, s.64)

Bu araştırmada kullanılan TKM ölçeği ile teknolojik ürün kullanım sıklığı ölçeği söz konusu varsayımları sağladığından H1'den H24'e kadar olan hipotezler parametrik testler aracılığıyla test edilmiştir.

##### 6.4.1.1 Doğrulayıcı faktör analizi (DFA)

Faktör analizi, çok sayıda değişkenin birbiri ile ilişkisini analiz etmede kullanılan, değişkenlerden toplanan bilgileri özetleyerek yeni ve “*daha az sayıda boyutlar veya faktörler seti*” oluşturmayı amaçlayan bir istatistiki yaklaşımdır (Hair vd., 1998, s.95) Bu analiz yaklaşımı açıklayıcı (keşfedici) ve doğrulayıcı olmak üzere iki şekilde uygulanmaktadır. Açıklayıcı faktör analizi; çok sayıdaki ölçek maddesinin temelde ölçtüğü alt boyutların (faktörlerin), analiz sonucunda tespit edildiği ve araştırmacının belirlenen faktörler hakkında analiz öncesinde herhangi bir beklentisinin olmadığı bir analiz yöntemidir. Doğrulayıcı faktör analizi ise faktör yapısı hakkında ön beklentinin olduğu ve daha öncesinde belirlenmiş olan faktörlerin doğrulanmasına yönelik uygulanan bir analiz yöntemidir. Çoğunlukla ölçek geliştirme ve geçerliliğini test etme amacıyla kullanılmaktadır.

Doğrulayıcı faktör analizinin; (i) tek faktörlü, (ii) birinci düzey çok faktörlü ve (iii) ikinci düzey çok faktörlü olmak üzere üç farklı türü bulunmaktadır. “Tek faktörlü doğrulayıcı faktör analizi”nde modelde yer alan tüm gözlenen değişkenler, tek bir gizil değişkeni

ölçmekte; “birinci düzey çok faktörlü doğrulayıcı faktör analizi”nde modelde yer alan bazı gözlenen değişkenler bir gizil değişkeni, bazıları ise bir başka gizil değişkeni ölçmekte ve “ikinci düzey çok faktörlü doğrulayıcı faktör analizi”nde ise modeldeki birden fazla gizil değişken hep birlikte daha kapsamlı başka bir gizil değişkeni ölçmektedir (Gürbüz vd., 2015, s.335).

DFA işlem süreci, modelin; (i) belirlenmesi, (ii) tanımlanması, (iii) tahmini, (iv) değerlendirilmesi ve (v) yeniden tanımlanması olmak üzere beş aşamadan oluşmaktadır (Öngen, 2010, s.26). İlk aşamada, yol (path) diyagramı kullanılarak gözlenen değişkenler (ölçek maddeleri) ve ilgili oldukları gizil değişkenler (faktörler) gösterilerek model belirlenmektedir. İkinci aşamada, gözlenen ve gizil değişkenler arasındaki tüm ilişkiler kovaryans denklemi ile tanımlanmaktadır. Üçüncü aşamada, ölçüm modeli en küçük kareler yöntemi ile tahmin edilmektedir. Dördüncü aşamada; modelin gözlenen değişkenler ile uyumu, ki-kare analizinin yanı sıra diğer istatistikler (CFI, NFI, GFI, RMSEA vb. gibi) de uygulanarak bir bütün halinde uyum iyiliği indeksleri üzerinden değerlendirilmektedir. Son aşamada ise anlamsız katsayıları olan ve modifikasyon indeksleri itibarıyla aşırı tahmin edilen gözlenen değişkenler modelden çıkarılmakta veya daha önce modelden çıkarılan değişkenler tekrar eklenmekte ve model temel yapıya bağlı kalınarak yeniden belirlenmektedir. Ardından yeni model tekrar tahmin edilmekte ve uyum iyiliği sağlanması halinde faktör analizi doğrulaması gerçekleştirilmiş olmaktadır (Öngen, 2010, s.27-44).

Doğrulayıcı faktör analizi süreci dikkate alındığında doğrulamanın uyum iyiliği kriterlerine uygunluk üzerinden belirlendiği görülmektedir. Dolayısıyla literatürde sıklıkla atıfta bulunan bazı uyum iyiliği indeksleri ve eşik değerleri Tablo 6.2’de özetlenmiş ve ardından bu indeksler kısaca açıklanmıştır.

**Tablo 6.2:** DFA Uyum İndeksleri ve Eşik Değerleri.

| Uyum İndeksleri | İyi Uyum    | Kabul Edilebilir Uyum |
|-----------------|-------------|-----------------------|
| CMIN/DF         | $\leq 3$    | $\leq 5$              |
| RMSEA           | $\leq 0.05$ | $\leq 0.08$           |
| SRMR            | $\leq 0.05$ | $\leq 0.08$           |
| CFI             | $\geq 0.97$ | $\geq 0.90$           |
| NFI             | $\geq 0.95$ | $\geq 0.90$           |
| TLI             | $\geq 0.95$ | $\geq 0.90$           |
| GFI             | $\geq 0.90$ | $\geq 0.85$           |
| AGFI            | $\geq 0.90$ | $\geq 0.85$           |

**Kaynak:** [Byrne, M.B., 2011; Gürbüz vd., 2015, s. 337]

### ***Ki-Kare (Chi- square - $\chi^2$ ) Testi***

Ki-kare ( $\chi^2$ ) testi, “sıfır hipotezi anlamlılık testi (Null Hypothesis Significance Test – NHST)” olarak da adlandırılan ve tüm modelin, gözlenen değişkenler ile uygunluğunu test eden bir model tahmincisidir. Ki-kare değerinin istatistiksel anlamlılığı, modelin anlamlı olduğunu göstermekte ve bu değer sıfıra eşit olması verinin modele mükemmel uyumunu göstermektedir. Dolayısıyla ki-kare değeri ne kadar küçük ise model uyumu o kadar iyidir. Ayrıca örnek hacmi ve model büyüklüğü, ki-kare değeri üzerinde etkilidir; örnek hacmi ve model büyüklüğü azaldıkça ki-kare değeri düşmekte, tam tersi örnek hacmi ve model büyüklüğü arttıkça ki-kare değeri yükselmektedir. Buna göre, örnek hacmi ve model büyüdükçe model uyumu kötüleşmektedir. Diğer yandan serbestlik derecesi, ki-kare testinde önemli bir kriter olarak dikkate alınmaktadır ve ki kare değerine oranı, uyum kriteri olarak kullanılmaktadır (Erkorkmaz vd., 2013, s.213). Söz konusu CMIN/DF (Kİ-Kare/ Serbestlik derecesi -  $\chi^2 / df$ ) oranının, Tablo 6.2’de özetlendiği üzere, 3’ten küçük olması iyi uyum ölçüsü olarak gösterilirken; 5’ten küçük olması kabul edilebilir uyum olarak nitelendirilmektedir (Byrne, M.B., 2011 Akt. Gürbüz vd., 2015, s. 337).

### ***GFI (Goodness of Fit Index – Uyum İyiliği İndeksi)***

Jöreskog ve Sorbom (1984) tarafından ki-kare testine alternatif olarak geliştirilen ilk uyum indeksidir. GFI, gözlenen değişkenin kovaryans matrisi ile model tarafından açıklanan kovaryans matrisinin, varyans ve kovaryans miktarlarının birbirine oranıdır (Erkorkmaz vd., 2013, s.213). Regresyon analizindeki  $R^2$ ’ye karşılık gelmektedir ancak farklı olarak  $R^2$  hata varyansını dikkate alırken, GFI gözlenen kovaryans oranını dikkate almaktadır. Ayrıca örneklem hacmi GFI değeri üzerinde etkilidir; örnek hacmi arttıkça GFI yükselmekte ve sonuçların doğruluğunu olumsuz etkilemektedir (Öngen, 2010, s.40). GFI değeri, 0 ile 1 arasında bir değer almakla birlikte, bu değer 1’e yaklaştıkça uyum iyiliği artmaktadır. GFI değerinin, Tablo 6.2’de özetlendiği üzere, 0.90’dan büyük olması iyi uyum ölçüsü olarak gösterilirken; 0.85’ten büyük olması kabul edilebilir uyum olarak nitelendirilmektedir (Byrne, M.B., 2011 Akt. Gürbüz vd., 2015, s. 337).

### ***AGFI (Adjustment Goodness of Fit Index – Düzeltilmiş Uyum İyiliği İndeksi)***

Serbestlik derecesi dikkate alınarak GFI değerinin düzeltildiği bir uyum indeksidir. AGFI değeri, 0 ile 1 arasında bir değer almakla birlikte, bu değer 1'e yaklaştıkça uyum iyiliği artmaktadır. AGFI değerinin, Tablo 6.2'de özetlendiği üzere, 0.90'dan büyük olması iyi uyum ölçüsü olarak gösterilirken; 0.85'ten büyük olması kabul edilebilir uyum olarak nitelendirilmektedir (Byrne, M.B., 2011 Akt. Gürbüz vd., 2015, s. 337).

### ***CFI (Comparative Fit Index- Karşılaştırmalı Uyum İndeksi)***

Karşılaştırmalı Uyum İndeksi (CFI); iç içe geçmiş modellerin,  $\chi^2$  değerleri arasındaki farkın serbestlik derecelerindeki fark ile test edildiği bir model tahmincisidir. CFI değeri, 0 ile 1 arasında bir değer almakla birlikte, bu değer 1'e yaklaştıkça uyum iyiliği artmaktadır (Demerouti, 2004, s.15 Akt. Öngen, 2010, s.41). CFI değerinin, Tablo 6.2'de özetlendiği üzere, 0.95'ten büyük olması iyi uyum ölçüsü olarak gösterilirken; 0.90'dan büyük olması kabul edilebilir uyum olarak nitelendirilmektedir (Byrne, M.B., 2011 Akt. Gürbüz vd., 2015, s. 337).

### ***NFI (Normed Fit Index – Ölçeklendirilmiş Uyum İndeksi)***

CFI'ya alternatif olarak Bentler ve Bonett (1980) tarafından geliştirilen NFI; varsayılan modelin,  $H_0$  hipoteziyle olan uygunluğunu araştırmaktadır (Öngen, 2010, s.41). Bu indekste değerlendirme, sıfır hipotezinin  $\chi^2$  değeri ile varsayılan modelin  $\chi^2$  değerini karşılaştırmak suretiyle yapılmaktadır. NFI değeri, 0 ile 1 arasında bir değer almakla birlikte, bu değer 1'e yaklaştıkça uyum iyiliği artmaktadır (Erkorkmaz vd., 2013, s.215). NFI değerinin, Tablo 6.2'de özetlendiği üzere, 0.95'ten büyük olması iyi uyum ölçüsü olarak gösterilirken; 0.90'dan büyük olması kabul edilebilir uyum olarak nitelendirilmektedir (Byrne, M.B., 2011 Akt. Gürbüz vd., 2015, s. 337).

### ***TLI (Trucker-Lewis Index)***

Ölçeklendirilmemiş Uyum İndeksi (Non Normed Fit Index – NNFI) olarak da bilinen Trucker ve Lewis (1973) tarafından geliştirilen TLI, NFI'nın örneklem büyüklüğünden etkilenmesine bağlı olumsuz değerlendirmeleri önlemek amacıyla geliştirilmiştir (Öngen, 2010, s.42). NFI değeri, 0 ile 1 arasında bir değer almakla birlikte, bu değer 1'e yaklaştıkça uyum iyiliği artmaktadır. NFI değerinin, Tablo 6.2'de özetlendiği üzere, 0.95'ten büyük

olması iyi uyum ölçüsü olarak gösterilirken; 0.90'dan büyük olması kabul edilebilir uyum olarak nitelendirilmektedir (Byrne, M.B., 2011 Akt. Gürbüz vd., 2015, s. 337).

***RMSEA (Root Mean Square Error of Approximation - Yaklaşık Hataların Kök Artık Kareler Ortalaması)***

Steiger ve Lind (1980) tarafından geliştirilen ve literatürde kötü uyum indeksi olarak tanımlanan RMSEA; modelden tahmin edilen kovaryans matrisinin, gözlemlenen değişkenlerden belirlenen kovaryans matrisine uygunluğunun test edildiği bir uyum indeksidir (Erkorkmaz vd., 2013, s.216). RMSEA değerinin, Tablo 6.2'de özetlendiği üzere, 0.05'e eşit veya 0.05'ten küçük olması iyi uyum ölçüsü olarak gösterilirken; 0.08'e eşit veya 0.08'den küçük olması kabul edilebilir uyum olarak nitelendirilmektedir (Byrne, M.B., 2011 Akt. Gürbüz vd., 2015, s. 337).

***RMR (Root Mean Square Residual - Kök Artık Kareler Ortalaması) ve SRMR (Standardized Root Mean Square Residual – Standartlaştırılmış Kök Artık Kareler Ortalaması)***

Kök Artık Kareler Ortalaması, uyumlu artıklar olarak adlandırılmaktadır ve gözlenen değişkenlere ait kovaryans matrisi ile modelden tahmin edilen kovaryans matrisi arasındaki uyumsuzluğun (farkın) kare kökünü ifade etmektedir. RMR değeri her bir gözlenen değişken için ayrı ayrı hesaplanmakta ve 0 ile 1 arasında bir değer almaktadır. Ki-kare değeri gibi 0'a ne kadar yakın yani değer ne kadar küçük ise model uyumu o kadar iyi kabul edilmektedir (Erkorkmaz vd., 2013, s.214).

Standartlaştırılmış Kök Artık Kareler Ortalaması ise RMR'nin gözlenen değişkenlerin kovaryans büyüklerine bağlı yorumlama sorununa çözüm getirmekte ve daha anlamlı yorumlama yapılmasını sağlamaktadır. SRMR de, RMR gibi 0 ile 1 arasında bir değer almakta ve 0'a ne kadar yakın ise model uyumu o kadar iyi kabul edilmektedir (Erkorkmaz vd., 2013, s.214). SRMR değerinin, Tablo 6.2'de özetlendiği üzere, 0.05'e eşit veya 0.05'ten küçük olması iyi uyum ölçüsü olarak gösterilirken; 0.08'e eşit veya 0.08'den küçük olması kabul edilebilir uyum olarak nitelendirilmektedir (Byrne, M.B., 2011 Akt. Gürbüz vd., 2015, s. 337).

Sonuç olarak bu araştırmada; kullanılan Teknoloji Kabul Modeli ölçeğinin, literatürde güvenilirliği ve geçerliliği kanıtlanmış bir ölçek olması sebebiyle, açıklayıcı faktör analizi uygulanmadan doğrudan DFA uygulanmıştır. Altı boyuttan (engel, algılanan fayda, algılanan kullanım kolaylığı, tutum, niyet ve davranış) oluşan ve gözlenen değişkenlerin farklı altı gizil değişkeni ifade etmesi dolayısıyla TKM'nin geçerliliğinin test edilmesi amacıyla “birinci düzey çok faktörlü doğrulayıcı faktör analizi” uygulanmış ve Ki-kare uyum iyiliği değerlerinin yanı sıra CFI, NFI, TLI, GFI, AGFI, RMSEA, SRMR uyum iyiliği indeksleri ve modifikasyon indeksleri itibarıyla değerlendirmeler yapılmıştır.

#### 6.4.1.2 Korelasyon analizi

Korelasyon analizi, bağımlı ve bağımsız iki değişken arasındaki matematiksel ilişkiyi belirlemeye yönelik yapılan bir analizdir. Korelasyon analizi ile bir değişkenin, diğer değişkende yarattığı etkinin nedeni ölçülmeyip değişkenlerin birlikte aynı (pozitif) veya farklı (negatif) yönde hareket ettiklerine dair ilişki ortaya konulmaktadır. Korelasyon katsayısı (r) ile ölçülmekte ve r değerinin aldığı değerlere göre değişkenler arası olası ilişki yorumlanmaktadır. Buna göre (Gegez, vd., 2023, s.548-553);

- a.  $r = 0$  ise; değişkenler arası ilişki yoktur.
- b.  $r > 0$  ise; pozitif yani aynı yönde ilişki vardır. Biri artarken diğeri de artar.
- c.  $r < 0$  ise; negatif yani zıt yönde ilişki vardır. Biri artarken diğeri azalır.
- d. İlişkinin gücü  $\pm 1$ 'e yakınlık ile ölçülmekte; (i)  $\pm 0.20$ 'ye kadar ilişki yok, (ii)  $\pm 0.21 - \pm 0.40$  arası zayıf, (iii)  $\pm 0.41 - \pm 0.60$  arası orta, (iv)  $\pm 0.61 - \pm 0.80$  arası güçlü ve (v)  $\pm 0.81 - \pm 1$  arası çok güçlü ilişki düzeyini göstermektedir.

Eğer değişkenlerin ikisi de aralıklı veya oran ölçek ise korelasyon analizinde Pearson korelasyon katsayısı kullanılırken; değişkenlerden en az biri ordinal ölçek ise Spearman korelasyon katsayısı kullanılmaktadır.

Bu araştırmada; Teknoloji Kabul Modeli boyutlarının (engel, algılanan fayda, algılanan kullanım kolaylığı, tutum, niyet ve davranış) birbirleri ile ilişkilerinin ortaya konulması amacıyla korelasyon analizi uygulanmış ve değişkenlerin hepsi de aralıklı ölçek olduğundan Pearson korelasyon katsayısı kullanılmıştır.

#### 6.4.1.3 Çoklu regresyon analizi

Regresyon analizi, bir veya daha fazla bağımsız değişkenin, bağımlı değişken üzerinde yarattığı değişimi ölçen bir analiz yöntemidir. Bu yöntem; (i) değişkenler arasında doğrusal ilişkinin olması, (ii) değişkenlerin aralıklı veya oran ölçek ile ölçülmesi, (iii) verinin normal dağılması ve (iv) hata terimlerinin bağımsız ve normal dağılmış olması varsayımlarına dayanmaktadır. Veri tahmini, en küçük kareler yöntemi ile yapılmaktadır. Regresyon analizinde; determinasyon katsayısı ( $R^2$ ), bağımsız değişken veya değişkenlerdeki birlikte değişimin bağımlı değişkende yüzde (%) kaçlık bir değişiklik yarattığını ortaya koymakta ve 0 ile +1 arasında bir değer almaktadır. İyi bir ilişki tahmininde,  $R^2$  yüksek ve tahmin standart hatasının küçük olması gerekmektedir (Lehman vd., 1998, s.498). Dolayısıyla  $R^2$  değeri arttıkça ve 1'e yaklaştıkça bağımlı değişken ve bağımsız değişkenler arasındaki ilişki daha güçlü olmaktadır.

Regresyon denklemindeki her bir bağımsız değişkene ait katsayı, beta ( $\beta$ ) katsayısı ile gösterilmektedir ve bağımsız değişkendeki 1 birimlik değişikliğin bağımlı değişkende kaç birimlik değişiklik yaratacağını ifade etmektedir. Buna göre beta katsayısı, standartlaştırılmamış ve standartlaştırılmış olmak üzere iki şekilde hesaplanmaktadır. Standartlaştırılmamış beta değeri, iki değişkenli (bir bağımsız ve bir bağımlı) regresyon analizlerinde dikkate alınırken; standartlaştırılmış beta değeri, çok değişkenli (birden çok bağımsız ve bir bağımlı) regresyon analizlerinde dikkate alınmaktadır. Bununla birlikte bir değişkene ait beta katsayısının p değerinin (Asymptotic Sig.), 0.05 (%5)'e eşit veya 0.05'in altında olması halinde bağımsız değişkenin bağımlı değişkeni tahmin etmede iyi olduğu yani değişkenler arasında anlamlı bir ilişkinin bulunduğu, 0.05'ten fazla olması durumunda ise tahmin etmede iyi olmadığı yani anlamlı bir ilişkinin bulunmadığı sonucuna ulaşılmaktadır (Gegez vd., 2023, s.572-573).

Ayrıca çoklu regresyon analizinin; standart, hiyerarşik ve adımsal olmak üzere üç farklı türü bulunmaktadır. “Standart çoklu regresyonda”, tüm bağımsız değişkenler aynı anda birlikte analize alınmakta; “hiyerarşik çoklu regresyonda”, bağımsız değişkenler, bağımlı değişkeni tahmin etme etki düzeyleri dikkate alınarak belirli bir sırada analize alınmakta ve “adımsal çoklu regresyonda” ise, bağımsız değişkenler analiz programına tanımlandıktan sonra bu değişkenlerin bir kısmı veya tamamı program tarafından belirli kriterler dikkate alınarak sırayla analize alınmaktadır (Gegez vd., 2023, s.584-585).



Bu arařtırmada; Teknoloji Kabul Modeli bağımsız deęiřkenlerinin (engel, algılanan fayda, algılanan kullanım kolaylıęı, tutum ve niyet) tutum, niyet ve dolayısıyla davranıř üzerindeki etkilerinin ortaya konulması amacıyla standart çoklu regresyon analizi uygulanmıř ve H1’den H12’ye kadar olan hipotezler bu analiz türü ile test edilmiřtir.

#### **6.4.1.4 T testi**

T testi, verinin normal daęılması halinde iki bağımsız grup arasındaki farklılıkları test etmektedir. Farklılıęın yönü (pozitif veya negatif) dikkate alındığında tek kuyruklu (saę veya sol) t testi yapılırken; dikkate alınmadığında çift kuyruklu t testi uygulanmaktadır. Ayrıca “tek gruplu”, “bağımlı iki gruplu” ve “bağımsız iki gruplu” olmak üzere üç farklı yöntem kullanılmaktadır. P deęerinin (Asymptotic Sig.), 0.05 (%5)’e eřit veya 0.05’in altında olması halinde iki grup arasında farklılık olduęu, 0.05’ten fazla olması durumunda ise farklılık olmadığı sonucuna ulařılmaktadır (Gegez, vd., 2023, s.479-481).

Bu arařtırmada; H13’ten H24’e kadar olan hipotezler çift kuyruklu, bağımsız t testi ile test edilmiřtir.

#### **6.4.2 Parametrik Olmayan Testler**

Parametrik olmayan testler; (i) verinin normal daęılmadığının varsayılması ya da bilinmesi ve (ii) nominal ya da ordinal verilerin kullanılması durumlarından herhangi birinin gerçekteřmesi halinde uygulanmaktadır (Shao, 1999, s.436).

Bu arařtırmada kullanılan ACFE hile arařtırmaları ölçeęi ile İşğüden Kılıç ve Anadolu (2018)’nın muhasebe hilelerinin önlenmesine yönelik geliřtirdikleri ölçek verileri normal daęılım göstermediğinden, H24’ten H37’ye kadar olan hipotezler parametrik olmayan testler kullanılarak test edilmiřtir.

##### **6.4.2.1 Mann-Whitney U testi**

Mann-Whitney U testi, verilerin normal daęılım göstermemesi halinde iki bağımsız grup arasındaki farklılıkları test etmektedir. Bağımsız deęiřkenin nominal ölçek ile bağımlı deęiřkenin ise ordinal ölçek ile ölçüldüğü durumlarda normal daęılımda t testinin yaptıęı işlevin aynısını gerçekteřtirmektedir. 0.05 önem düzeyinde; z deęeri  $\pm 1.96$ ’nın dışında kaldığında veya p deęerinin (Asymptotic Sig.) 0.05 (%5)’in altında olması halinde iki grup arasında farklılık olduęu sonucuna ulařılmaktadır (Gegez vd., 2023, s.458-461).

Bu arařtırmada; H25, H27, H28, H31, H33 ve H34 hipotezleri Mann-Whitney U testi ile test edilmiřtir.

#### **6.4.2.2 Kruskal-Wallis testi**

Kruskal-Wallis testi, verilerin normal daęılım gstermemesi halinde  veya daha fazla baęımsız grup arasındaki farklılıkları test etmektedir. Mann-Whitney U testinin uzantısı nitelięinde olan bu testin normal daęılımdaki karřılıęı tek faktrl varyans analizidir. P deęerinin (Asymptotic Sig.) 0.05 (%5)'in altında olması halinde iki grup arasında farklılık olduęu sonucuna varılmaktadır (Gegez vd., 2023, s.475-477).

Bu arařtırmada; H26, H29, H30, H32, H35, H36 ve H37 hipotezleri Kruskal-Wallis testi ile test edilmiřtir.

## 7. ARAŞTIRMANIN BULGULARI VE YORUM

Bu bölümde; altıncı bölüm alt başlıklarında tanımlanmış olan ve bu araştırmada uygulanan veri analiz yöntemlerinin sonuçlarına ilişkin bulgular ve bu bulgulara dair yorumlar yer almaktadır. Bulgular, dört ana bölümde sınıflandırılmaktadır. Birinci bölümde, katılımcıların demografik bilgilerine ilişkin açıklamalar yapılmaktadır. İkinci bölümde, katılımcıların teknolojik ürün kullanım sıklıklarına ilişkin bulgular yer almaktadır. Üçüncü bölümde, Teknoloji Kabul Modeli'ne yönelik gerçekleştirilen doğrulayıcı faktör, ilişki ve farklılık analizleri sonuçları bulunmaktadır. Son olarak dördüncü bölümde ise, meslek mensuplarının hile ile karşılaşma sıklıklarına ve hilelerin önlenmesinde blokzincirin rolüne dair görüşlerine yönelik farklılık analizi bulguları yer almaktadır.

Anket uygulamasına toplam 512 kişinin katılmasıyla birlikte, yüz yüze ankete katılım sağlayan 104 adet katılımcıya ait verilerde cevaplamama hatası ile karşılaşıldığından bu katılımcılara ait veriler analiz dışı bırakılmış ve kalan 408 adet katılımcıya ait cevaplar analize tabi tutulmuştur. Veri analizi, IBM SPSS 27 ve AMOS 22 paket programları aracılığı ile gerçekleştirilmiştir.

### 7.1 DEMOGRAFİK BULGULAR

Araştırmanın demografik bulgularında; katılımcıların cinsiyeti, eğitim durumu, mesleki ünvanı, çalışma şekli, mesleki tecrübesi, mükellef sayısı ve blokzincir teknolojisi bilgi düzeylerine ilişkin bilgiler yer almaktadır. Bulgular frekans analizi ile elde edilmiş olup ilgili bilgilere ait dağılımlar oransal olarak Tablo 7.1'de verilmiştir. Söz konusu bulgulara ait yorumlar ise aşağıda maddeler halinde açıklanmaktadır.

Araştırmaya katılım sağlayan İstanbul ilinde faaliyet gösteren mali müşavir meslek mensuplarının;

- a. %30,6'sı kadın, %69,4'ü erkektir. Bu sonuçlara göre cinsiyetler arası karşılaştırma yapıldığında; İstanbul ilinde mali müşavirlik mesleğinin, yaklaşık 2 kat daha fazla erkekler tarafından icra edildiği söylenebilir.
- b. %2'si lise, %70,3'ü lisans, %25'i yüksek lisans ve %2,7'si doktora mezunudur. Meslek mensuplarının eğitim düzeyleri karşılaştırıldığında; bu sonuçlar, 3568 sayılı mali

müşavirlik meslek kanunu dolayısıyla ruhsat alınabilmesi için gerekli ön koşul olan en az lisans düzeyinde mezuniyet şartını ispat eder niteliktedir. Ön koşulu sağlamayan lise mezunu olan 8 kişinin ise SMMM olmakla birlikte anket formundaki asgari seçenek olan 21 yıl ve üzeri tecrübe düzeyleri dikkate alındığında bu kişilerin kanunla birlikte ünvan verilen meslek mensupları olduklarını söyleyebiliriz. Diğer yandan meslek mensuplarının %30,2'sinin asgari eğitim şartının üzerinde eğitimlerine devam etmiş olmaları sebebiyle yaklaşık 1/3'inin mesleki gelişime önem verdiklerini de ifade edebiliriz.

- c. %91,7'si SMMM ve %8,3'ü YMM'dir. Bu sonuçlara göre mesleki ünvanlar arası karşılaştırma yapıldığında; her iki meslek grubunun toplam üye sayısı içindeki oranları dikkate alınarak bu dağılımların oransal dağılıma uygun gerçekleştiğini söyleyebiliriz<sup>58</sup>.
- d. %71,3'ü serbest olarak çalışmakta ve kendi bürosundan faaliyetlerini yürütmekteyken, %28,7'si bir işverene bağlı olarak hizmet vermektedir. Bu sonuçlara göre meslek mensuplarının büyük çoğunluğunun bağımsız çalışanlar olduğunu söyleyebiliriz.
- e. %4,2'si 1-5 yıl arası, %7,8'i 6-10 yıl arası, %17,4'ü 11-15 yıl arası, %23,5'i 16-20 yıl arası ve %47,1'i 21 yıl ve üzeri mesleki tecrübeye sahiptir. Bu sonuçlara göre; katılımcıların büyük çoğunluğu yüksek mesleki tecrübeye sahiptir. Dolayısıyla muhasebenin gelişimine ve muhasebe hilelerine yönelik farklı yöntem ve teknolojileri deneyimleme ve karşılaştırabilme imkânı sağlamış olabileceklerini söyleyebiliriz.
- f. %24'ü 1-5 arası, %5,1'i 6-10 arası, %11,3'ü 11-20 arası, %14,5'i 21-30 arası ve %45,1'i 31 ve üzeri mükellef sayısına sahiptir. Bu sonuçlara göre; katılımcıların çoğunluğunun 31 ve üzeri mükellef sayısı mevcuttur. Dolayısıyla, muhasebe hileleri ile karşılaşma ve mücadele etme yöntemlerini kullanma deneyimi ve karşılaştırabilme imkânı sağlamış olabileceklerini söyleyebiliriz.
- g. %25,2'sinin çok az, %32,4'ünün orta, %12'sinin iyi ve %1,7'sinin ileri düzeyde blokzincir teknolojisi hakkında bilgisi mevcutken; %28,7'sinin bilgisi hiç yoktur. Bu sonuçlara göre; meslek mensuplarının blokzincir teknoloji hakkındaki bilgi düzeylerinin düşük olduğunu söyleyebiliriz.

---

<sup>58</sup> SMMM ve YMM katılımcı sayılarına ilişkin oransal dağılım için bkz. "Örnekleme Yöntemi" s.236.

**Tablo 7.1:** Katılımcıların Demografik Bilgilerine Göre Dağılımları.

| DEMOGRAFİK ÖZELLİKLER                     |                 | FREKANS | YÜZDE |
|-------------------------------------------|-----------------|---------|-------|
| CİNSİYET                                  | Kadın           | 125     | 30.6  |
|                                           | Erkek           | 283     | 69.4  |
|                                           | TOPLAM          | 408     | 100.0 |
| EĞİTİM                                    | Lise            | 8       | 2.0   |
|                                           | Lisans          | 287     | 70.3  |
|                                           | Yüksek Lisans   | 102     | 25.0  |
|                                           | Doktora         | 11      | 2.7   |
|                                           | TOPLAM          | 408     | 100.0 |
| MESLEKİ ÜNVAN                             | SMMM            | 374     | 91.7  |
|                                           | YMM             | 34      | 8.3   |
|                                           | TOPLAM          | 408     | 100.0 |
| ÇALIŞMA ŞEKLİ                             | Bağımlı         | 117     | 28.7  |
|                                           | Bağımsız        | 291     | 71.3  |
|                                           | TOPLAM          | 408     | 100.0 |
| MESLEKİ TECRÜBE                           | 1-5 yıl         | 17      | 4.2   |
|                                           | 6-10 yıl        | 32      | 7.8   |
|                                           | 11-15 yıl       | 71      | 17.4  |
|                                           | 16-20 yıl       | 96      | 23.5  |
|                                           | 21 yıl ve üzeri | 192     | 47.1  |
|                                           | TOPLAM          | 408     | 100.0 |
| MÜKELLEF SAYISI                           | 1-5             | 98      | 24.0  |
|                                           | 6-10            | 21      | 5.1   |
|                                           | 11-20           | 46      | 11.3  |
|                                           | 21-30           | 59      | 14.5  |
|                                           | 31 ve üzeri     | 184     | 45.1  |
|                                           | TOPLAM          | 408     | 100.0 |
| BLOKZİNCİR<br>TEKNOLOJİSİ BİLGİ<br>DÜZEYİ | Bilgim yok      | 117     | 28.7  |
|                                           | Çok az          | 103     | 25.2  |
|                                           | Orta            | 132     | 32.4  |
|                                           | İyi             | 49      | 12.0  |
|                                           | İleri           | 7       | 1.7   |
|                                           | TOPLAM          | 408     | 100.0 |

## 7.2 TEKNOLOJİK ÜRÜN KULLANIMINA AİT BULGULAR

Çalışmanın bu bölümünde; katılımcıların teknolojik ürün kullanım sıklıklarına ilişkin bulgular yer almaktadır. Bulgular frekans analizi ile elde edilmiş olup ilgili bilgilere ait dağılımlar oransal olarak Tablo 7.2’de verilmiştir. Söz konusu bulgulara ait yorumlar ise aşağıda maddeler halinde açıklanmaktadır.

Araştırmaya katılım sağlayan İstanbul ilinde faaliyet gösteren mali müşavir meslek mensuplarının;

- a. %14,71'i meslektaşları, %23,53'ü sosyal çevreleri, %29,9'u meslek odaları ve %31,86'sı diğer çeşitli kaynakları aracılığıyla mesleki teknolojik ürünlerden haberdar olmaktadır. Bu sonuçlara göre; meslek mensuplarının mesleki teknolojik gelişmeler hakkında birbirleriyle paylaşımlarının az olduğunu söyleyebiliriz. Diğer yandan ikinci en çok kullanılan kaynağın meslek odaları olmasına rağmen; meslek mensuplarının yaklaşık 1/3'ine ulaşılabilen olması dolayısıyla odalarca etkin bir eğitim politikası yürütülmediğini de ifade edebiliriz.
- b. %23,28'i önemli, %75,74'ü ise çok önemli ifadelerini seçtiklerinden dolayı meslek mensupları için gündelik hayatta yeni teknolojik ürünlerin yerinin çok önemli olduğunu söyleyebiliriz.
- c. %79,66'sı her gün, %10,54'ü haftada bazı günler ve %6,13'ü haftada birkaç gün mesleki araştırmalarında teknolojik ürünleri kullanmaktayken; %3,68'i ise çok nadir kullanmaktadır. Bu sonuçlara göre; meslek mensuplarının mesleki faaliyetlerinde sıklıkla teknoloji kullandıklarını söyleyebiliriz.
- d. %73,77'si çok önemli ve %23,28'i ise önemli ifadelerini seçtiklerinden dolayı meslek mensupları için teknolojik ürünlerin mesleki araştırmalarında çok önemli bir yeri olduğunu söyleyebiliriz.
- e. %13,48'inin her yıl, %3,43'ünün yeni bir ürün üretildiğinde, %4,41'inin her ay ve %78,68'inin ise ihtiyaç olduğunda mesleki teknolojik ürünleri satın aldıkları tespit edilmiştir. Bu sonuçlara göre; meslek mensuplarının büyük çoğunluğunun ihtiyaç doğduğunda teknolojik ürün satın alımına yöneldiği ve bunun için ayrıca bütçe oluşturmadığı söylenebilir.
- f. %91,18'i ihtiyacı olması halinde satışa çıkan genel bir teknolojik ürünü satın aldıklarını ifade etmişlerdir. Dolayısıyla meslek mensuplarının büyük çoğunluğunun genel bir teknolojik ürün alımı için de bütçe oluşturmadığını söyleyebiliriz.
- g. %12,75'i arkadaşlarından, %71,81'i program satıcılarından, %12,01'i meslektaşlarından ve %3,43'ü ise meslek odalarından mesleki teknolojik ürünlerin kullanılması hakkında

teknik destek almaktadır. Bu sonuçlara göre; meslek odalarının, meslek mensuplarına teknolojik ürünlere ilişkin teknik destek konusunda yeterli hizmeti sağlayamadıklarını söyleyebiliriz.

- h. %5,64'ü 0-1 saat arası, %26,23'ü 1-3 saat arası, %30,39'u 3-5 saat arası ve %37,75'i 5 saatten fazla gündelik hayatında akıllı telefon kullanmaktadır. Dolayısıyla meslek mensupları gündelik hayatlarında da teknolojiyi yoğun bir şekilde kullanmaktadırlar.
- i. %97,06'sı iş hayatında her gün internet ile işlem yapmakta olduklarını ifade etmişlerdir. İnternet kullanmayan veya internette işlem yapmayan meslek mensubu ise bulunmamaktadır. Bu sonuca göre, mesleki faaliyetlerin internet kullanılarak gerçekleştirildiğini söyleyebiliriz.
- j. %52,45'inin 1-20 arası, %21,08'inin 21-40 arası, %12,50'sinin 41-60 arası ve %12,97'sinin 60 ve üzeri mükellefine ait işlemler için teknolojik ürünleri kullanmak zorunda oldukları tespit edilmiştir. Dolayısıyla en fazla teknolojik ürünleri kullanmak zorunda kalan mükellef sayısının 1 ile 20 arasında olduğunu söyleyebiliriz.
- k. %31,62'si kamunun, %37,01'i müşterinin, %22,79'u sektörün ve %8,58'i meslektaşın direnci dolayısıyla muhasebe alanında blokzincir teknolojisinin benimsenmediğini ifade etmişlerdir. Bu sonuçlara göre; meslek mensupları açısından blokzincir teknolojisinin benimsenmesinde en büyük engelin müşteri direnci olduğunu söyleyebiliriz. Meslektaşın direnci ise en düşük engel olarak görülmektedir. Bu durumu; özellikle müşterinin ve sonrasında kamunun ikna edilmesi halinde meslektaşın bu yeni teknolojiye uyuma direnç göstermeyeceği şeklinde değerlendirebiliriz.

**Tablo 7.2:** Katılımcıların Teknolojik Ürün Kullanım Sıklığına Göre Dağılımları.

| Teknolojik Ürün Kullanma Sıklığı                                                                |                            | Frekans | Yüzde  |
|-------------------------------------------------------------------------------------------------|----------------------------|---------|--------|
| Mesleki teknolojik ürünlerden haberdar olma kaynağı                                             | Meslektaşlarımdan          | 60      | 14.71  |
|                                                                                                 | Sosyal çevreden            | 96      | 23.53  |
|                                                                                                 | Meslek Odalarından         | 122     | 29.90  |
|                                                                                                 | Diğer çeşitli kaynaklardan | 130     | 31.86  |
|                                                                                                 | Toplam                     | 408     | 100.00 |
| Yeni teknolojik ürünlerin gündelik hayattaki önem düzeyi (Akıllı Telefon, Laptop, PC, vb. gibi) | Çok önemsiz                | 1       | 0.25   |
|                                                                                                 | Önemsiz                    | 3       | 0.74   |
|                                                                                                 | Önemli                     | 95      | 23.28  |
|                                                                                                 | Çok önemli                 | 309     | 75.74  |
|                                                                                                 | Toplam                     | 408     | 100.00 |

**Tablo 7.2:** Katılımcıların Teknolojik Ürün Kullanım Sıklığına Göre Dağılımları (Devam).

| Teknolojik Ürün Kullanma Sıklığı                                                                                             |                                | Frekans | Yüzde  |
|------------------------------------------------------------------------------------------------------------------------------|--------------------------------|---------|--------|
| Mesleki araştırmalarda teknolojik ürünleri kullanma sıklığı (E Defter, E Fatura, E Arşiv, vb. gibi)                          | Çok nadir                      | 15      | 3.68   |
|                                                                                                                              | Haftada birkaç gün             | 25      | 6.13   |
|                                                                                                                              | Haftada bazı günler            | 43      | 10.54  |
|                                                                                                                              | Her gün                        | 325     | 79.66  |
|                                                                                                                              | Toplam                         | 408     | 100.00 |
| Teknolojik ürünlerin mesleki araştırmalardaki önemi                                                                          | Çok önemsiz                    | 0       | 0.00   |
|                                                                                                                              | Önemsiz                        | 10      | 2.45   |
|                                                                                                                              | Kararsızım                     | 2       | 0.49   |
|                                                                                                                              | Önemli                         | 95      | 23.28  |
|                                                                                                                              | Çok önemli                     | 301     | 73.77  |
|                                                                                                                              | Toplam                         | 408     | 100.00 |
| Mesleki teknoloji ürünlerin satın alınması için bütçe oluşturma sıklığınız                                                   | Her yıl                        | 55      | 13.48  |
|                                                                                                                              | Her ay                         | 18      | 4.41   |
|                                                                                                                              | İhtiyaç olduğunda              | 321     | 78.68  |
|                                                                                                                              | Yeni bir ürün üretildiğinde    | 14      | 3.43   |
|                                                                                                                              | Toplam                         | 408     | 100.00 |
| Genel bir teknolojik ürün satışa çıktığında (Akıllı Telefon, Laptop, PC vb.)                                                 | Hemen satın alırım             | 10      | 2.45   |
|                                                                                                                              | Birkaç ay beklerim             | 22      | 5.39   |
|                                                                                                                              | İhtiyaç olduğunda satın alırım | 372     | 91.18  |
|                                                                                                                              | Satın almam                    | 4       | 0.98   |
|                                                                                                                              | Toplam                         | 408     | 100.00 |
| Mesleki teknoloji ürünlerinin kullanılmasında teknik destek alımı (Akıllı Telefon, Laptop, PC vb.)                           | Arkadaşımdan                   | 52      | 12.75  |
|                                                                                                                              | Program satıcılarından         | 293     | 71.81  |
|                                                                                                                              | Meslektaşlarımdan              | 49      | 12.01  |
|                                                                                                                              | Meslek odalarından             | 14      | 3.43   |
|                                                                                                                              | Toplam                         | 408     | 100.00 |
| Gündelik hayatta akıllı telefon kullanma sıklığınız                                                                          | 0-1 saat                       | 23      | 5.64   |
|                                                                                                                              | 1-3 saat                       | 107     | 26.23  |
|                                                                                                                              | 3-5 saat                       | 124     | 30.39  |
|                                                                                                                              | 5 saat ve üzeri                | 154     | 37.75  |
|                                                                                                                              | Toplam                         | 408     | 100.00 |
| İş hayatında internette işlem yapma sıklığınız                                                                               | İnternet kullanmıyorum         | 0       | 0.00   |
|                                                                                                                              | Kullanmıyorum                  | 0       | 0.00   |
|                                                                                                                              | Nadiren                        | 12      | 2.94   |
|                                                                                                                              | Her gün                        | 396     | 97.06  |
|                                                                                                                              | Toplam                         | 408     | 100.00 |
| İş hayatınızda teknolojik ürünleri kullanmak zorunda olduğunuz mükellef sayısı (E-Arşiv, E-Fatura, E-Defter, E-İrsaliye vb.) | 1-20                           | 214     | 52.45  |
|                                                                                                                              | 21-40                          | 86      | 21.08  |
|                                                                                                                              | 41-60                          | 51      | 12.50  |
|                                                                                                                              | 60 ve üzeri                    | 57      | 13.97  |
|                                                                                                                              | Toplam                         | 408     | 100.00 |
| Blokzincir teknolojisinin muhasebe alanında benimsenmesinde en büyük engel                                                   | Kamunun direnci                | 129     | 31.62  |
|                                                                                                                              | Müşterinin direnci             | 151     | 37.01  |
|                                                                                                                              | Sektörün direnci               | 93      | 22.79  |
|                                                                                                                              | Meslektaşın direnci            | 35      | 8.58   |
|                                                                                                                              | Toplam                         | 408     | 100.00 |



### 7.3 TEKNOLOJİ KABUL MODELİNE AİT BULGULAR

Çalışmanın bu bölümünde, teknoloji kabul modeli ölçeğine uygulanan çeşitli analiz yöntemlerine ait bulgular açıklanmıştır. Bu bağlamda; öncelikle güvenilirlik ve normal dağılım kontrolü gibi ön analizler yapılmış ve bu ön analizlerin sonucuna göre uygulanacak analiz yöntemleri belirlenmiştir. Daha sonra TKM modelinin test edilmesi için yapısal eşitlik modeli (YEM) çerçevesinde doğrulayıcı faktör analizi uygulanarak model doğrulanmış ardından sonuçlarına göre korelasyon ve çoklu regresyon analizleri uygulanarak bulgular özetlenmiş ve yorumlanmıştır. İlişki analizlerinin yanı sıra ise TKM boyutlarının katılımcıların demografik özelliklerine göre farklılıkları araştırılmıştır. Bu kapsamda da t testi uygulanmış ve sonuçları özetlenerek yorumlanmıştır.

#### 7.3.1 Güvenilirlik Analizine Ait Bulgular

Güvenilirlik analizi, bir ölçüm aracının güvenilirliğinin değerlendirilmesi için kullanılan istatistiksel bir yöntemdir. Ölçeğin güvenilirliğini ise ölçek maddelerinin birbiriyle bütünlüğünü ifade eden iç tutarlılık değeri belirlemektedir. Farklı iç tutarlılık testleri kullanılmakla birlikte en çok raporlanan güvenilirlik endeksi “Cronbach Alfa katsayısı”dır. Cronbach alfa katsayısı; *“bir ölçekte yer alan maddelerin ya da soruların her birinin birbiri ile ne kadar iyi ilişkilendirilmiş olduğunu araştıran bir testtir. Alfa katsayısı, 0 ile 1 arasında bir değer alır. Genel kabul görmüş Cronbach alfa altı sınırı ise 0.70’tir”* (Gegez vd., 2023, s.267-268).

Bu çalışmada da güvenilirlik analizi, Cronbach alfa katsayısı referans alınarak gerçekleştirilmiştir. Buna göre; Teknoloji Kabul Modeli ölçeğine ilişkin alfa değeri 0.830 olarak hesaplanmış olup 0.70 alt sınırı aştığından ölçek iç tutarlılığı sağlanmıştır. Dolayısıyla TKM ölçeği güveniliridir.

#### 7.3.2 Normallik Testi ve Tanımlayıcı İstatistik Bulguları

Normal dağılım, *“teorik olasılık dağılımını göstermektedir”*. Bir veri setinin belirli bir özellik için ortalama etrafında simetrik olarak dağıldığı durumları tanımlamaktadır. Normal dağılımda; ortalama, medyan ve mod aynı değeri taşımaktadır. Çan şeklinde bir eğri ile temsil edilmekte ve eğrinin ortası, verinin ortalamasını göstermektedir. Normal dağılımda;

verilerin %68,26'sı ortalamadan  $\pm 1$  standart sapma, %95'i  $\pm 2$  standart sapma ve %99,72  $\pm 3$  standart sapma alanı içinde yer almaktadır (Gegez vd., 2023, s.405-411).

Normal dağılıma uygunluğu test etmek üzere birçok istatistiki test kullanılmaktadır. Bunlardan en yaygın kullanılanları “Kolmogorov-Smirnov, Shapiro-Wilk ve Lilifeors” testleridir. Gözlem sayısı (n), 29’dan küçük ise Shapiro-Wilk; büyük ise Kolmogorov-Smirnov ve Lilifeors testleri genellikle kullanılmaktadır. Diğer yandan bu testlerin sonuçlarına göre normal dağılıma uygunluğun sağlanmadığı durumlarda; dağılımın belirli çarpıklık (skewness) ve basıklık (kurtosis) değerlerini karşılaması halinde de normal dağılıma uygun olduğu kabul edilmektedir. Buna göre verinin normal dağılıma uygun olduğu; (i) normallik testleri için p değerinin 0.05 (%5)’ten fazla olması (73.Tokol, s.2000, s.96) ve (ii) çarpıklık ile basıklık değerlerinin  $\pm 2$  arasında olması (Field vd., 2006, s.238) koşullarını sağlaması halinde kabul edilmektedir (Gegez vd., 2023, s.412).

Bu çalışmada, TKM değişkenlerine ilişkin normallik testi, gözlem sayısının 408 olması yani 29’dan büyük olması nedeniyle Kolmogorov-Smirnov testi ile yapılmış ve p değeri 0.05’in altında bulunmuştur. Buna rağmen ölçek değişkenlerine ilişkin çarpıklık ve basıklık değerlerinin, kabul edilebilir aralık olan  $\pm 2$  arasında olması sebebiyle uygunluk koşulları sağlanmıştır. Dolayısıyla TKM değişkenlerine ait dağılım, normal dağılım göstermektedir.

Aşağıdaki Tablo 7.3’te, “Engeller, Algılanan Fayda, Algılanan Kullanım Kolaylığı, Tutum, Niyet ve Davranış” değişkenleri çerçevesinde normallik testi ve tanımlayıcı istatistik bulguları gösterilmektedir.

**Tablo 7.3:** TKM Ölçeğine İlişkin Normallik Testi ve Tanımlayıcı İstatistik Bulguları.

| Değişkenler                  | n   | Min. | Max. | Ortalama | Standart Sapma | Çarpıklık | Basıklık | K-S Sig. |
|------------------------------|-----|------|------|----------|----------------|-----------|----------|----------|
| Engeller                     | 408 | 1    | 5    | 3.3819   | 0.70123        | -0.663    | 1.909    | < 0.001  |
| Algılanan Fayda              | 408 | 1    | 5    | 3.7703   | 0.88853        | -0.917    | 1.070    | < 0.001  |
| Algılanan Kullanım Kolaylığı | 408 | 1    | 5    | 3.1039   | 0.81733        | -0.079    | 0.313    | < 0.001  |
| Tutum                        | 408 | 1    | 5    | 2.5572   | 0.88419        | 0.322     | 0.107    | < 0.001  |
| Niyet                        | 408 | 1    | 5    | 3.5528   | 0.87908        | -0.669    | 0.805    | < 0.001  |
| Davranış                     | 408 | 1    | 5    | 2.4659   | 0.94470        | 0.262     | -0.249   | < 0.001  |

### 7.3.3 Doğrulayıcı Faktör Analizine Ait Bulgular

Bu araştırmada, mali müşavir meslek mensuplarının blokzincir teknolojisi kullanımına yönelik tutum, niyet ve davranışlarının ölçümü amacıyla Teknoloji Kabul Modeli (TKM) ölçeği kullanılmıştır. Söz konusu ölçeğin geçerliliği ve güvenilirliği literatürde kanıtlanmış olduğundan bu çalışmada "Açıklayıcı Faktör Analizi" uygulanmadan, blokzincir teknolojisinin kabul düzeyine yönelik modelin uygunluğunu test etmek amacıyla "Doğrulayıcı Faktör Analizi" yapılmıştır.

İlk oluşturulan modelde uyum iyiliği değerlerinin kabul edilebilir düzeyleri sağlamaması ve regresyon ağırlıkları itibarıyla anlamlılık düzeyinde olmayan ölçüm sonuçları elde edilmesi sebebiyle Tutum boyutuna ait TUT1 maddesi ile Davranış boyutuna ait DVR1 ve DVR2 maddeleri modelden çıkarılmıştır. İlgili yapı oluşturulup model yeniden çözümlendiğinde ise, kabul edilebilir uyum iyiliği değerleri (Tablo 7.4) ve regresyon katsayıları (Tablo 7.5) sağlanmıştır.

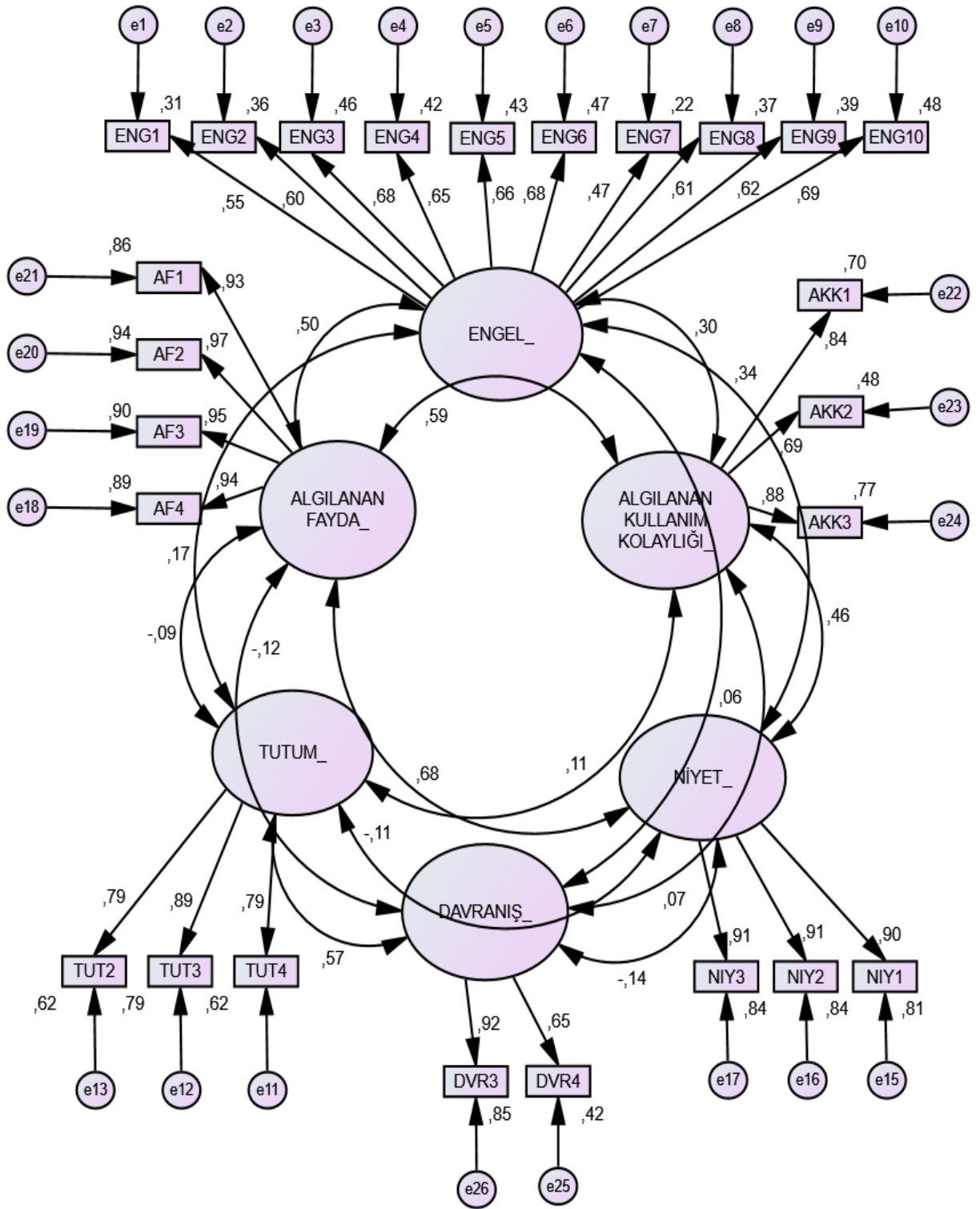
**Tablo 7.4:** TKM Doğrulayıcı Faktör Analizi Uyum İyiliği Değerleri.

| Uyum İyiliği Değerleri           | CMIN/DF | CFI    | NFI    | TLI    | GFI    | AGFI   | RMSEA  | SRMR   |
|----------------------------------|---------|--------|--------|--------|--------|--------|--------|--------|
| Kabul Edilebilir Sınır           | ≤ 5     | ≥ 0.90 | ≥ 0.90 | ≥ 0.90 | ≥ 0.85 | ≥ 0.85 | ≤ 0.08 | ≤ 0.08 |
| Teknoloji Kabul Modeli Değerleri | 2.313   | 0.949  | 0.914  | 0.941  | 0.891  | 0.864  | 0.057  | 0,0633 |

Tablo 7.4’te özetlendiği üzere, ölçüm modeline ait uyum iyiliği değerleri Ki kare (CMIN) 601.41; serbestlik derecesi (df) 260; CMIN/df (2.313) 5’ten küçük; CFI (0.949), NFI (0.914) ve TLI (0.941) 0.90’dan büyük; GFI (0.891) ve AGFI (0.864) 0.85’ten büyük, RMSEA (0.057) ve SRMR (0.0633) 0.08’den küçük olarak elde edilmiştir. Bununla birlikte ölçüm modeline ait tüm yol katsayılarının istatistiksel olarak anlamlı olduğu tespit edilmiş olup Tablo 7.5’te hem standartlaştırılmış ( $\beta_1$ ) hem de standartlaştırılmamış ( $\beta_2$ ) olmak üzere beta değerleri ile standart hata (S.E.), kritik oran ( $C.R = \beta_2/S.E.$ ) ve p değerleri itibarıyla analiz sonuçları sunulmuştur. Ardından da Şekil 7.2’de Teknoloji Kabul Modeli Doğrulayıcı Faktör Analizi Diyagramı verilmiştir.

**Tablo 7.5:** TKM Doğrulamalı Faktör Analizi Regresyon Ağırlıkları.

| ÖLÇÜM MODELİ                    |      |                              | $\beta_1$                               | $\beta_2$ | S.E.  | C.R.   | P      |
|---------------------------------|------|------------------------------|-----------------------------------------|-----------|-------|--------|--------|
| ENG1                            | <--- | ENGEL                        | 0.554                                   | 1         |       |        |        |
| ENG2                            | <--- | ENGEL                        | 0.596                                   | 1.019     | 0.110 | 9.266  | <0.001 |
| ENG3                            | <--- | ENGEL                        | 0.681                                   | 1.033     | 0.102 | 10.096 | <0.001 |
| ENG4                            | <--- | ENGEL                        | 0.649                                   | 0.993     | 0.101 | 9.793  | <0.001 |
| ENG5                            | <--- | ENGEL                        | 0.658                                   | 0.94      | 0.095 | 9.882  | <0.001 |
| ENG6                            | <--- | ENGEL                        | 0.684                                   | 1.004     | 0.099 | 10.122 | <0.001 |
| ENG7                            | <--- | ENGEL                        | 0.467                                   | 0.789     | 0.102 | 7.757  | <0.001 |
| ENG8                            | <--- | ENGEL                        | 0.612                                   | 0.953     | 0.101 | 9.427  | <0.001 |
| ENG9                            | <--- | ENGEL                        | 0.621                                   | 0.903     | 0.095 | 9.522  | <0.001 |
| ENG10                           | <--- | ENGEL                        | 0.693                                   | 1.074     | 0.105 | 10.204 | <0.001 |
| TUT4                            | <--- | TUTUM                        | 0.789                                   | 1         |       |        |        |
| TUT3                            | <--- | TUTUM                        | 0.890                                   | 1.055     | 0.059 | 17.942 | <0.001 |
| TUT2                            | <--- | TUTUM                        | 0.788                                   | 0.943     | 0.057 | 16.485 | <0.001 |
| NIY1                            | <--- | NİYET                        | 0.901                                   | 1         |       |        | <0.001 |
| NIY2                            | <--- | NİYET                        | 0.914                                   | 1.008     | 0.035 | 28.51  | <0.001 |
| NIY3                            | <--- | NİYET                        | 0.914                                   | 1.023     | 0.036 | 28.489 | <0.001 |
| AF4                             | <--- | ALGILANAN FAYDA              | 0.943                                   | 1         |       |        |        |
| AF3                             | <--- | ALGILANAN FAYDA              | 0.949                                   | 1.025     | 0.025 | 40.625 | <0.001 |
| AF2                             | <--- | ALGILANAN FAYDA              | 0.968                                   | 1.049     | 0.024 | 44.634 | <0.001 |
| AF1                             | <--- | ALGILANAN FAYDA              | 0.926                                   | 0.994     | 0.027 | 36.639 | <0.001 |
| AKK1                            | <--- | ALGILANAN KULLANIM KOLAYLIĞI | 0.836                                   | 1         |       |        |        |
| AKK2                            | <--- | ALGILANAN KULLANIM KOLAYLIĞI | 0.691                                   | 0.858     | 0.059 | 14.656 | <0.001 |
| AKK3                            | <--- | ALGILANAN KULLANIM KOLAYLIĞI | 0.876                                   | 1.001     | 0.055 | 18.318 | <0.001 |
| DVR4                            | <--- | DAVRANIŞ                     | 0.648                                   | 1         |       |        |        |
| DVR3                            | <--- | DAVRANIŞ                     | 0.921                                   | 1.34      | 0.152 | 8.837  | <0.001 |
| $\beta_1$ : Standart katsayılar |      |                              | $\beta_2$ : Standart olmayan katsayılar |           |       |        |        |



CMIN=601,407; DF=260; CMIN/DF=2,313; RMSEA=,057; CFI=,949; GFI=,891; AGFI=,864; NFI=,914; TLI=,941

Şekil 7.1: Teknoloji Kabul Modelinin Doğrulayıcı Faktör Analizi Diyagramı.

Uygulanan “Doğrulamalı Faktör Analizi” sonuçlarına göre; “Teknoloji Kabul Modeli” ölçeği altı boyutlu olarak doğrulanmıştır. İlgili ölçeğe ilişkin Şekil 7.1’de verilen DFA diyagramında da görüldüğü üzere; faktör yüklerinin, “Engel” boyutu için 0.47 ile 0.69 arasında; “Algılanan Fayda” boyutu için 0.93 ile 0.97 arasında; “Algılanan Kullanım Kolaylığı” boyutu için 0.69 ile 0.88 arasında; “Tutum” boyutu için 0.79 ile 0.89 arasında; “Niyet” boyutu için 0.90 ile 0.91 arasında ve “Davranış” boyutu için ise, 0.65 ile 0.92 arasında olduğu tespit edilmiştir. Dış değişken Engel boyutunun etkilediği Algılanan Kullanım Kolaylığı ile Algılanan Fayda boyutlarının Tutumu ve Niyeti dolayısıyla da Davranışı etkilediği doğrulanmış ve modelin geçerliliği desteklenmiştir.

Doğrulamalı faktör analizi sonrasında ise Teknoloji Kabul Modeli ölçek maddelerine, ilgili boyutları itibarıyla güvenilirlik analizleri uygulanmış ve analiz sonuçları her bir boyuta ilişkin alfa değerleri itibarıyla Tablo 7.6’da özetlenmiştir. Güvenilirlik analizi sonuçlarına göre; tüm boyutlara ait alfa değerleri 0.70 alt sınırı aştığından boyutların ölçek iç tutarlılıkları sağlanmıştır. Dolayısıyla ölçek boyutları güvenilirdir. Bununla birlikte, en düşük güvenilirliğe sahip boyut Davranış boyutu olurken; en yüksek güvenilirliğe sahip boyut ise, Algılanan Fayda boyutu olarak gerçekleşmiştir.

**Tablo 7.6:** Ölçek Boyutları İtibarıyla Güvenilirlik Analizi Sonuçları.

| Ölçek Boyutu                 | Cronbach Alfa Değeri | Madde Sayısı |
|------------------------------|----------------------|--------------|
| Engel                        | 0.861                | 10           |
| Algılanan Fayda              | 0.972                | 4            |
| Algılanan Kullanım Kolaylığı | 0.840                | 3            |
| Tutum                        | 0.858                | 3            |
| Niyet                        | 0.935                | 3            |
| Davranış                     | 0.746                | 2            |
| <b>Toplam</b>                |                      | <b>25</b>    |

#### 7.3.4 Korelasyon Analizine Ait Bulgular

Doğrulanmış Teknoloji Kabul Modeli değişkenlerine yönelik hipotezlerin test edilmesinden önce değişkenler arasındaki ilişkinin yönünün ve gücünün ortaya konulabilmesi için korelasyon analizi uygulanmıştır. Analizde, değişkenlerin tamamı aralıklı ölçek olduğundan Pearson katsayısı kullanılmış ve çift kuyruk testi yapılmıştır. İlgili analize ait bulgular Tablo

7.7’de verilmiş ve ardından değişkenler arasındaki ilişki aşağıda maddeler halinde istatistiki olarak açıklanmıştır.

**Tablo 7.7:** TKM Ölçeği Korelasyon Analizi.

| DEĞİŞKENLER                  | Engel   | Algılanan Fayda | Algılanan Kullanım Kolaylığı | Tutum   | Niyet  | Davranış |
|------------------------------|---------|-----------------|------------------------------|---------|--------|----------|
| Engel                        | 1       |                 |                              |         |        |          |
| Algılanan Fayda              | 0.430** | 1               |                              |         |        |          |
| Algılanan Kullanım Kolaylığı | 0.270** | 0.530**         | 1                            |         |        |          |
| Tutum                        | 0.169** | -0.095          | 0.118*                       | 1       |        |          |
| Niyet                        | 0.289** | 0.649**         | 0.387**                      | -0.110* | 1      |          |
| Davranış                     | 0.109*  | -0.054          | 0.110*                       | 0.482** | -0.095 | 1        |

\*  $p < 0.05$     \*\*  $p < 0.01$

Korelasyon analizi sonuçlarına göre;

- Engel ile Algılanan Fayda arasında ( $r = 0.430$ ,  $p < 0.01$ ); % 99 güven seviyesinde, pozitif yönlü orta dereceli bir ilişki bulunduğu,
- Engel ile Algılanan Kullanım Kolaylığı arasında ( $r = 0.270$ ,  $p < 0.01$ ); % 99 güven seviyesinde, pozitif yönlü zayıf bir ilişki bulunduğu,
- Engel ile Tutum arasında ( $r = 0.169$ ,  $p < 0.01$ ); % 99 güven seviyesinde, pozitif yönlü çok zayıf bir ilişki bulunduğu,
- Engel ile Niyet arasında ( $r = 0.289$ ,  $p < 0.01$ ); % 99 güven seviyesinde, pozitif yönlü zayıf bir ilişki bulunduğu,
- Engel ile Davranış arasında ( $r = 0.109$ ,  $p < 0.05$ ); % 95 güven seviyesinde, pozitif yönlü çok zayıf bir ilişki bulunduğu,
- Algılanan Fayda ile Algılanan Kullanım Kolaylığı arasında ( $r = 0.530$ ,  $p < 0.01$ ); % 99 güven seviyesinde, pozitif yönlü orta dereceli bir ilişki bulunduğu,
- Algılanan Fayda ile Tutum arasında ( $r = -0.095$ ); negatif yönlü zayıf bir ilişki bulunduğu,
- Algılanan Fayda ile Niyet arasında ( $r = 0.649$ ,  $p < 0.01$ ); % 99 güven seviyesinde, pozitif yönlü güçlü bir ilişki bulunduğu,

- i. Algılanan Fayda ile Davranış arasında ( $r = -0.054$ ); negatif yönlü zayıf bir ilişki bulunduğu,
- j. Algılanan Kullanım Kolaylığı ile Tutum arasında ( $r = 0.118$ ,  $p < 0.05$ ); % 95 güven seviyesinde, pozitif yönlü çok zayıf bir ilişki bulunduğu,
- k. Algılanan Kullanım Kolaylığı ile Niyet arasında ( $r = 0.387$ ,  $p < 0.01$ ); % 99 güven seviyesinde, pozitif yönlü zayıf bir ilişki bulunduğu,
- l. Algılanan Kullanım Kolaylığı ile Davranış arasında ( $r = 0.110$ ,  $p < 0.05$ ); % 95 güven seviyesinde, pozitif yönlü çok zayıf bir ilişki bulunduğu,
- m. Tutum ile Niyet arasında ( $r = -0.110$ ,  $p < 0.05$ ); % 95 güven seviyesinde, negatif yönlü çok zayıf bir ilişki bulunduğu,
- n. Tutum ile Davranış arasında ( $r = -0.482$ ,  $p < 0.01$ ); % 99 güven seviyesinde, pozitif yönlü orta dereceli bir ilişki bulunduğu,
- o. Niyet ile Davranış arasında ( $r = -0.095$ ); negatif yönlü zayıf bir ilişki bulunduğu tespit edilmiştir.

### 7.3.5 Teknoloji Kabul Modeli Hipotezlerinin Test Edilmesi ve Sonuçları

Teknoloji Kabul Modeli Ölçeği verilerinin güvenilirliği, yapılan testler sonucunda değerlendirilmiş ve normallik dağılımı kontrol edilmiştir. Ön veri analizi bulgularına göre; güvenilirlik koşullarının sağlandığı ve veri setinin, normal dağılım gösterdiği tespit edilmiştir. Bu nedenle; TKM hipotezleri, parametrik analiz yöntemleri ile test edilmiştir.

TKM Ölçeği ile İstanbul'da faaliyet gösteren mali müşavir meslek mensuplarının blokzincir teknolojisi kabullerini açıklamak amacıyla engel, algılanan fayda, algılanan kullanım kolaylığı, tutum, niyet ve davranış değişkenlerinin birbirlerine etkisinin ortaya konulması için ilişki analizleri uygulanmıştır. TKM modeline göre; engel, algılanan fayda ve algılanan kullanım kolaylığı bağımsız değişkenler iken; tutum, niyet ve davranış bağımlı değişkenlerdir. Model ile ayrıca bağımlı değişkenler tutum ve niyetin hem birbirlerine etkisi hem de teknoloji kabulünü belirleyen davranış üzerine etkisi de ölçülmektedir. Bu kapsamda çalışmada, her bir bağımlı değişken için ayrı ayrı olmak üzere standart çoklu regresyon



analizi ile ölçüm gerçekleştirilmiştir. İlgili bağımlı değişkenler itibarıyla test edilen hipotezler aşağıda açıklanmıştır:

- a. “Tutum” bağımlı değişkeni ile engel, algılanan fayda ve algılanan kullanım kolaylığı bağımsız değişkenleri arasındaki ilişki, sırasıyla H1 hipotezi (engel ile tutum arasında negatif bir ilişki vardır), H2 hipotezi (algılanan fayda ile tutum arasında pozitif bir ilişki vardır) ve H3 hipotezi (algılanan kullanım kolaylığı ile tutum arasında pozitif bir ilişki vardır) ile ifade edilmektedir.
- b. “Niyet” bağımlı değişkeni ile engel, algılanan fayda, algılanan kullanım kolaylığı ve tutum bağımsız değişkenleri arasındaki ilişki, sırasıyla H4 hipotezi (engel ile niyet arasında negatif bir ilişki vardır), H5 hipotezi (algılanan fayda ile niyet arasında pozitif bir ilişki vardır), H6 hipotezi (algılanan kullanım kolaylığı ile niyet arasında pozitif bir ilişki vardır) ve H7 hipotezi (tutum ile niyet arasında pozitif bir ilişki vardır) ile ifade edilmektedir.
- c. “Davranış” bağımlı değişkeni ile engel, algılanan fayda, algılanan kullanım kolaylığı ve niyet bağımsız değişkenleri arasındaki ilişki, sırasıyla H8 hipotezi (engel ile davranış arasında negatif bir ilişki vardır), H9 hipotezi (algılanan fayda ile davranış arasında pozitif bir ilişki vardır), H10 hipotezi (algılanan kullanım kolaylığı ile davranış arasında pozitif bir ilişki vardır) ve H11 hipotezi (niyet ile davranış arasında pozitif bir ilişki vardır) ile ifade edilmektedir.

Buradan hareketle izleyen alt bölümde; bağımlı değişkenler bazında ilgili hipotezlere ait bulguların özeti birlikte sunulmuştur. Ardından da her bir hipoteze yönelik açıklamalar detaylandırılarak sonuçların istatistiksel anlamlılıkları tartışılmış ve elde edilen bulgular yorumlanmıştır.

#### **7.3.5.1 Standart çoklu regresyon analizine ait bulgular**

Bu çalışmada, mali müşavir meslek mensuplarının blokzincir teknolojisi kabul düzeylerine ilişkin H1'den H12'ye kadar olan hipotezler, bağımsız değişkenler grubu ile bağımlı değişkenin tahmin edilme düzeyinin tespit edilmesi üzerine olduğundan standart çoklu regresyon analizi kullanılarak test edilmiştir. İlgili hipotezlerin istatistiksel sonuçları tutum, niyet ve davranış bağımlı değişkenleri itibarıyla sınıflandırılarak aşağıda sırasıyla sunulmaktadır:

**a. Tutum bağımlı değişkenine ilişkin hipotezler**

Engel, algılanan fayda ve algılanan kullanım kolaylığı bağımsız değişkenlerinin “tutum” bağımlı değişkenini tahmine etme düzeylerine yönelik hipotezler sırasıyla H1, H2 ve H3 hipotezleridir. Söz konusu hipotezlerin test edilmesi amacıyla standart çoklu regresyon analizi yapılmış ve analiz bulguları Tablo 7.8’de özetlenmiştir. İlgili bulgular tek tek hipotezler ele alınarak istatistiki olarak yorumlanmıştır.

**Tablo 7.8:** TKM Standart Çoklu Regresyon Analizi (Tutum).

**Bağımlı Değişken : Tutum**

| Bağımsız Değişkenler                                                              | Standart Olmayan Katsayılar |            | Standart Katsayılar | t      | Sig.  | Korelasyon |                     | Doğrusallık İstatistikleri |       |
|-----------------------------------------------------------------------------------|-----------------------------|------------|---------------------|--------|-------|------------|---------------------|----------------------------|-------|
|                                                                                   | $\beta$                     | Std. Sapma | Std. $\beta$        |        |       | Part       | (Part) <sub>2</sub> | Tolerans                   | VIF   |
| (Sabit)                                                                           | 1.959                       | 0.239      |                     | 8.194  | 0.000 |            |                     |                            |       |
| Engel                                                                             | 0.310                       | 0.066      | 0.246               | 4.695  | 0.000 | 0.222      | 0.049               | 0.812                      | 1.231 |
| Algılanan Fayda                                                                   | -0.316                      | 0.059      | -0.317              | -5.327 | 0.000 | -0.252     | 0.063               | 0.630                      | 1.587 |
| Algılanan Kullanım Kolaylığı                                                      | 0.238                       | 0.060      | 0.220               | 3.940  | 0.000 | 0.186      | 0.035               | 0.717                      | 1.395 |
| <b>R = 0.312      Adj. R<sup>2</sup> = 0.091      F = 14.574      p &lt; 0.01</b> |                             |            |                     |        |       |            |                     |                            |       |

Tablo 7.8’de özetlenen bulgulara göre; tutum bağımlı değişkenine yönelik modelin ( $F = 14.574$ ;  $p < 0.01$ ) istatistiki olarak anlamlı olduğu ve modeldeki bağımsız değişkenlerin birlikte, tutumdaki değişimin %9.1’ini açıkladığı görülmektedir. Yeni bir teknolojiye dair tutumun açıklanmasında, modelde alınan değişkenlerden başka birçok faktörün etkili olabileceği göz önünde bulundurulduğunda; 0.091’lik  $R^2$  değeri, oldukça yeterli bir değeri ifade etmektedir. Bununla birlikte tutum varyansının; %4.9’unu engel değişkeni, %6.3’ünü algılanan fayda değişkeni ve %3.5’ini algılanan kullanım kolaylığı değişkeni tek başına açıklamaktadır. T değerleri itibarıyla değerlendirdiğimizde ise tutuma en yüksek katkının engel değişkeni olduğu görülmektedir. Diğer yandan tolerans değerleri 0.10’dan yüksek ve VIF değerleri ise 3’den düşüktür. Dolayısıyla bağımsız değişkenler arasında çoklu ilişki bulunmamaktadır.

Hipotezler itibarıyla bağımsız değişkenlerin tutuma etkisini incelendiğimizde;

### ***Hipotez 1***

**H<sub>0</sub>** : Dış değişkenler (engeller), mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumunu pozitif yönde etkilemektedir veya hiç etkilememektedir.

**H<sub>1</sub>**: Dış değişkenler (engeller), mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumunu negatif yönde etkilemektedir.

Tablo 7.8’de görüldüğü üzere; “Engel” bağımsız değişkenine ait p değeri (0.000) 0.05’den küçük; Std.β değeri (0.246) ise pozitif olarak hesaplanmıştır. Bu bulgular doğrultusunda; engeller ile mali müşavirlerin blokzincir kullanımına yönelik tutumları arasında istatistiksel olarak anlamlı bir ilişki tespit edilmiş olmasına rağmen etki yönü pozitif olmasından dolayı Hipotez 1 reddedilmiştir.

### ***Hipotez 2***

**H<sub>0</sub>** : Algılanan fayda, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumunu negatif yönde etkilemektedir veya hiç etkilememektedir.

**H<sub>1</sub>**: Algılanan fayda, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumunu pozitif yönde etkilemektedir.

Tablo 7.8’de görüldüğü üzere; “Algılanan Fayda” bağımsız değişkenine ait p değeri (0.000) 0.05’den küçük; Std.β değeri (-0.317) ise negatif olarak hesaplanmıştır. Bu bulgular doğrultusunda; algılanan fayda ile mali müşavirlerin blokzincir kullanımına yönelik tutumları arasında istatistiksel olarak anlamlı bir ilişki tespit edilememiş olup Hipotez 2 reddedilmiştir.

### ***Hipotez 3***

**H<sub>0</sub>** : Algılanan kullanım kolaylığı, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumunu negatif yönde etkilemektedir veya hiç etkilememektedir.

**H<sub>1</sub>**: Algılanan kullanım kolaylığı, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumunu pozitif yönde etkilemektedir.

Tablo 7.8’de görüldüğü üzere; “Algılanan kullanım kolaylığı” bağımsız değişkenine ait p değeri (0.000) 0.05’den küçük; Std.β değeri (0.220) ise pozitif olarak hesaplanmıştır. Bu

bulgular doğrultusunda; algılanan kullanım kolaylığı ile mali müşavirlerin blokzincir kullanımına yönelik tutumları arasında istatistiksel olarak anlamlı bir ilişki tespit edilmiş olup Hipotez 3 kabul edilmiştir.

**b. Niyet bağımlı değişkenine ilişkin hipotezler**

Engel, algılanan fayda, algılanan kullanım kolaylığı ve tutum bağımsız değişkenlerinin “niyet” bağımlı değişkenini tahmine etme düzeylerine yönelik hipotezler sırasıyla H4, H5, H6 ve H7 hipotezleridir. Söz konusu hipotezlerin test edilmesi amacıyla standart çoklu regresyon analizi yapılmış ve analiz bulguları Tablo 7.9’de özetlenmiştir. İlgili bulgular tek tek hipotezler ele alınarak istatistiki olarak yorumlanmıştır.

**Tablo 7.9: TKM Standart Çoklu Regresyon Analizi (Niyet).**

**Bağımlı Değişken : Niyet**

| Bağımsız Değişkenler                                                              | Standart Olmayan Katsayılar |            | Standart Katsayılar | t      | Sig.  | Korelasyon |                     | Doğrusallık İstatistikleri |       |
|-----------------------------------------------------------------------------------|-----------------------------|------------|---------------------|--------|-------|------------|---------------------|----------------------------|-------|
|                                                                                   | $\beta$                     | Std. Sapma | Std. $\beta$        |        |       | Part       | (Part) <sup>2</sup> | Tolerans                   | VIF   |
| (Sabit)                                                                           | 1.160                       | 0.205      |                     | 5.666  | 0.000 |            |                     |                            |       |
| Engel                                                                             | 0.032                       | 0.054      | 0.025               | 0.586  | 0.558 | 0.022      | 0.000               | 0.770                      | 1.298 |
| Algılanan Fayda                                                                   | 0.586                       | 0.049      | 0.592               | 12.054 | 0.000 | 0.454      | 0.206               | 0.589                      | 1.699 |
| Algılanan Kullanım Kolaylığı                                                      | 0.080                       | 0.049      | 0.074               | 1.637  | 0.102 | 0.062      | 0.004               | 0.690                      | 1.449 |
| Tutum                                                                             | -0.067                      | 0.039      | -0.067              | -1.691 | 0.092 | -0.064     | 0.004               | 0.902                      | 1.108 |
| <b>R = 0.654      Adj. R<sup>2</sup> = 0.422      F = 75.229      p &lt; 0.01</b> |                             |            |                     |        |       |            |                     |                            |       |

Tablo 7.9’da özetlenen bulgulara göre; niyet bağımlı değişkenine yönelik modelin ( $F = 75.229$ ;  $p < 0.01$ ) istatistiki olarak anlamlı olduğu ve modeldeki bağımsız değişkenlerin birlikte, niyetteki değişimin %42.2’sini açıkladığı görülmektedir. Yeni bir teknoloji kullanımına yönelik niyetin açıklanmasında, 0.422’lik  $R^2$  değeri, oldukça yüksek bir değeri ifade etmektedir. Bununla birlikte niyet varyansının; %0,05’ini engel değişkeni, %20.6’sını algılanan fayda değişkeni; %0.4’ünü algılanan kullanım kolaylığı değişkeni ve %0.4’ünü tutum değişkeni tek başına açıklamaktadır. T değerleri itibarıyla değerlendirdiğimizde ise niyete en yüksek katkının algılanan fayda değişkeni olduğu görülmektedir. Diğer yandan tolerans değerleri 0.10’dan yüksek ve VIF değerleri ise 3’ten düşüktür. Dolayısıyla bağımsız değişkenler arasında çoklu ilişki bulunmamaktadır.

Hipotezler itibarıyla bağımsız değişkenlerin tutuma etkisini incelendiğimizde;

#### **Hipotez 4**

**H<sub>0</sub>** : Dış değişkenler, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik niyetini pozitif yönde etkilemektedir veya hiç etkilememektedir.

**H<sub>1</sub>**: Dış değişkenler, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik niyetini negatif yönde etkilemektedir.

Tablo 7.9’da görüldüğü üzere; “Engel” bağımsız değişkenine ait p değeri (0.558) 0.05’ten büyük; Std.β değeri (0.025) ise pozitif olarak hesaplanmıştır. Bu bulgular doğrultusunda; engeller ile mali müşavirlerin blokzincir kullanımına yönelik niyetleri arasında istatistiksel olarak anlamlı bir ilişki tespit edilememiş olup Hipotez 4 reddedilmiştir.

#### **Hipotez 5**

**H<sub>0</sub>** : Algılanan fayda, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik niyetini negatif yönde etkilemektedir veya hiç etkilememektedir.

**H<sub>1</sub>**: Algılanan fayda, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik niyetini pozitif yönde etkilemektedir.

Tablo 7.9’da görüldüğü üzere; “Algılanan Fayda” bağımsız değişkenine ait p değeri (0.000) 0.05’ten küçük; Std.β değeri (0.592) ise pozitif olarak hesaplanmıştır. Bu bulgular doğrultusunda; algılanan fayda ile mali müşavirlerin blokzincir kullanımına yönelik niyetleri arasında istatistiksel olarak anlamlı bir ilişki tespit edilmiş olup Hipotez 5 kabul edilmiştir.

#### **Hipotez 6**

**H<sub>0</sub>** : Algılanan kullanım kolaylığı, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik niyetini negatif yönde etkilemektedir veya hiç etkilememektedir.

**H<sub>1</sub>**: Algılanan kullanım kolaylığı, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik niyetini pozitif yönde etkilemektedir.

Tablo 7.9’da görüldüğü üzere; “Algılanan Kullanım Kolaylığı” bağımsız değişkenine ait p değeri (0.102) 0.05’ten büyük; Std.β değeri (0.074) ise pozitif olarak hesaplanmıştır. Bu bulgular doğrultusunda; algılanan kullanım kolaylığı ile mali müşavirlerin blokzincir

kullanımına yönelik niyetleri arasında istatistiksel olarak anlamlı bir ilişki tespit edilememiş olup Hipotez 6 reddedilmiştir.

### **Hipotez 7**

**H<sub>0</sub>** : Mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumları, niyetlerini negatif yönde etkilemektedir veya hiç etkilememektedir.

**H<sub>1</sub>**: Mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumları, niyetlerini pozitif yönde etkilemektedir.

Tablo 7.9’da görüldüğü üzere; “Tutum” bağımsız değişkenine ait p değeri (0.092) 0.05’ten büyük; Std.β değeri (0.039) ise pozitif olarak hesaplanmıştır. Bu bulgular doğrultusunda; tutum ile mali müşavirlerin blokzincir kullanımına yönelik niyetleri arasında istatistiksel olarak anlamlı bir ilişki tespit edilememiş olup Hipotez 7 reddedilmiştir.

### **c. Davranış bağımlı değişkenine ilişkin hipotezler**

Engel, algılanan fayda, algılanan kullanım kolaylığı, tutum ve niyet bağımsız değişkenlerinin “davranış” bağımlı değişkenini tahmine etme düzeylerine yönelik hipotezler sırasıyla H8, H9, H10, H11 ve H12 hipotezleridir. Söz konusu hipotezlerin test edilmesi amacıyla standart çoklu regresyon analizi yapılmış ve analiz bulguları Tablo 7.10’da özetlenmiştir. İlgili bulgular tek tek hipotezler ele alınarak istatistiki olarak yorumlanmıştır.

**Tablo 7.10:** TKM Standart Çoklu Regresyon Analizi (Davranış).

#### **BAĞIMLI DEĞİŞKEN : DAVRANIŞ**

| Bağımsız Değişkenler                                                              | Standart Olmayan Katsayılar |            | Standart Katsayılar | t      | Sig.  | Korelasyon |                     | Doğrusallık İstatistikleri |       |
|-----------------------------------------------------------------------------------|-----------------------------|------------|---------------------|--------|-------|------------|---------------------|----------------------------|-------|
|                                                                                   | β                           | Std. Sapma | Std. β              |        |       | Part       | (Part) <sup>2</sup> | Tolerans                   | VIF   |
| (Sabit)                                                                           | 1.114                       | 0.263      |                     | 4.227  | 0.000 |            |                     |                            |       |
| Engel                                                                             | 0.056                       | 0.067      | 0.041               | 0.835  | 0.404 | 0.036      | 0.001               | 0.770                      | 1.299 |
| Algılanan Fayda                                                                   | -0.031                      | 0.070      | -0.029              | -0.442 | 0.659 | -0.019     | 0.000               | 0.433                      | 2.311 |
| Algılanan Kullanım Kolaylığı                                                      | 0.103                       | 0.061      | 0.089               | 1.702  | 0.090 | 0.074      | 0.005               | 0.686                      | 1.458 |
| Tutum                                                                             | 0.485                       | 0.049      | 0.454               | 9.885  | 0.000 | 0.429      | 0.184               | 0.896                      | 1.116 |
| Niyet                                                                             | -0.078                      | 0.062      | -0.073              | -1.272 | 0.204 | -0.055     | 0.003               | 0.573                      | 1.747 |
| <b>R = 0.491      Adj. R<sup>2</sup> = 0.232      F = 25.598      p &lt; 0.01</b> |                             |            |                     |        |       |            |                     |                            |       |

Tablo 7.10’da özetlenen bulgulara göre; davranış bağımlı değişkenine yönelik modelin ( $F = 25.598$ ;  $p < 0.01$ ) istatistiki olarak anlamlı olduğu ve modeldeki bağımsız değişkenlerin birlikte, niyetteki değişimin %23.2’sini açıkladığı görülmektedir. Yeni bir teknoloji kullanımına yönelik niyetin açıklanmasında, 0.232’lik  $R^2$  değeri, oldukça yüksek bir değeri ifade etmektedir. Bununla birlikte niyet varyansının; %0,1’ini engel değişkeni, %0.04’ünü algılanan fayda değişkeni; %0.5’ini algılanan kullanım kolaylığı değişkeni; %18.4’ünü tutum değişkeni ve %0.3’ünü niyet değişkeni tek başına açıklamaktadır. T değerleri itibarıyla değerlendirdiğimizde ise davranışa en yüksek katkının tutum değişkeni olduğu görülmektedir. Diğer yandan tolerans değerleri 0.10’dan yüksek ve VIF değerleri ise 3’ten düşüktür. Dolayısıyla bağımsız değişkenler arasında çoklu ilişki bulunmamaktadır.

Hipotezler itibarıyla bağımsız değişkenlerin tutuma etkisini incelediğimizde;

#### ***Hipotez 8***

**H<sub>0</sub>** : Dış değişkenler (engeller), mali müşavirlerin blokzincir teknolojisi kullanım davranışını pozitif yönde etkilemektedir veya hiç etkilememektedir.

**H<sub>1</sub>**: Dış değişkenler (engeller), mali müşavirlerin blokzincir teknolojisi kullanım davranışını negatif yönde etkilemektedir.

Tablo 7.10’da görüldüğü üzere; “Engel” bağımsız değişkenine ait p değeri (0.404) 0.05’ten büyük; Std.β değeri (0.041) ise pozitif olarak hesaplanmıştır. Bu bulgular doğrultusunda; engel ile mali müşavirlerin blokzincir kullanımına yönelik davranışları arasında istatistiksel olarak anlamlı bir ilişki tespit edilmiş olmasına rağmen etki yönü pozitif olmasından dolayı Hipotez 8 reddedilmiştir.

#### ***Hipotez 9***

**H<sub>0</sub>** : Algılanan fayda, mali müşavirlerin blokzincir teknolojisi kullanım davranışını negatif yönde etkilemektedir veya hiç etkilememektedir.

**H<sub>1</sub>**: Algılanan fayda, mali müşavirlerin blokzincir teknolojisi kullanım davranışını pozitif yönde etkilemektedir.

Tablo 7.10’da görüldüğü üzere; “Algılanan Fayda” bağımsız değişkenine ait p değeri (0.659) 0.05’ten büyük; Std.β değeri (-0.029) ise negatif olarak hesaplanmıştır. Bu bulgular

doğrultusunda; algılanan fayda ile mali müşavirlerin blokzincir kullanımına yönelik davranışları arasında istatistiksel olarak anlamlı bir ilişki tespit edilememiş olup Hipotez 9 reddedilmiştir.

#### ***Hipotez 10***

**H<sub>0</sub>** : Algılanan kullanım kolaylığı, mali müşavirlerin blokzincir teknolojisi kullanım davranışını negatif yönde etkilemektedir veya hiç etkilememektedir.

**H<sub>1</sub>**: Algılanan kullanım kolaylığı, mali müşavirlerin blokzincir teknolojisi kullanım davranışını pozitif yönde etkilemektedir.

Tablo 7.10’da görüldüğü üzere; “Algılanan Kullanım Kolaylığı” bağımsız değişkenine ait p değeri (0.090) 0.05’ten büyük; Std.β değeri (0.089) ise pozitif olarak hesaplanmıştır. Bu bulgular doğrultusunda; algılanan kullanım kolaylığı ile mali müşavirlerin blokzincir kullanımına yönelik davranışları arasında istatistiksel olarak anlamlı bir ilişki tespit edilememiş olup Hipotez 10 reddedilmiştir.

#### ***Hipotez 11***

**H<sub>0</sub>** : Mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumları, kullanım davranışını negatif yönde etkilemektedir veya hiç etkilememektedir.

**H<sub>1</sub>**: Mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumları, kullanım davranışını pozitif yönde etkilemektedir.

Tablo 7.10’da görüldüğü üzere; “Tutum” bağımsız değişkenine ait p değeri (0.000) 0.05’ten küçük; Std.β değeri (0.454) ise pozitif olarak hesaplanmıştır. Bu bulgular doğrultusunda; tutum ile mali müşavirlerin blokzincir kullanımına yönelik davranışları arasında istatistiksel olarak anlamlı bir ilişki tespit edilmiş olup Hipotez 11 kabul edilmiştir.

#### ***Hipotez 12***

**H<sub>0</sub>** : Mali müşavirlerin blokzincir teknolojisi kullanımına yönelik niyetleri, kullanım davranışını negatif yönde etkilemektedir veya hiç etkilememektedir.

**H<sub>1</sub>**: Mali müşavirlerin blokzincir teknolojisi kullanımına yönelik niyetleri, kullanım davranışını pozitif yönde etkilemektedir.



Tablo 7.10’da görüldüğü üzere; “Niyet” bağımsız değişkenine ait p değeri (0.204) 0.05’ten büyük; Std.β değeri (-0.073) ise negatif olarak hesaplanmıştır. Bu bulgular doğrultusunda; niyet ile mali müşavirlerin blokzincir kullanımına yönelik davranışları arasında istatistiksel olarak anlamlı bir ilişki tespit edilememiş olup Hipotez 12 reddedilmiştir.

### 7.3.5.2 TKM hipotezlerinin sonuçları

Teknoloji Kabul Modeli kapsamında gerçekleştirilen ve önceki bölümde bulguları açıklanan çoklu regresyon analizi ile test edilen hipotezlere ilişkin sonuçlar aşağıda Tablo 7.11’de özetlenmiştir.

**Tablo 7.11:** TKM Hipotez Sonuç Tablosu.

| HİPOTEZLER |                                                                                                                                   | SONUÇ |
|------------|-----------------------------------------------------------------------------------------------------------------------------------|-------|
| H1         | Dış değişkenler (engeller), mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumunu negatif yönde etkilemektedir.   | RED   |
| H2         | Algılanan fayda, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumunu pozitif yönde etkilemektedir.              | RED   |
| H3         | Algılanan kullanım kolaylığı, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumunu pozitif yönde etkilemektedir. | KABUL |
| H4         | Dış değişkenler, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik niyetini negatif yönde etkilemektedir.              | RED   |
| H5         | Algılanan fayda, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik niyetini pozitif yönde etkilemektedir.              | KABUL |
| H6         | Algılanan kullanım kolaylığı, mali müşavirlerin blokzincir teknolojisi kullanımına yönelik niyetini pozitif yönde etkilemektedir. | RED   |
| H7         | Mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumları, niyetlerini pozitif yönde etkilemektedir.                 | RED   |
| H8         | Dış değişkenler (engeller), mali müşavirlerin blokzincir teknolojisi kullanım davranışını negatif yönde etkilemektedir.           | RED   |
| H9         | Algılanan fayda, mali müşavirlerin blokzincir teknolojisi kullanım davranışını pozitif yönde etkilemektedir.                      | RED   |
| H10        | Algılanan kullanım kolaylığı, mali müşavirlerin blokzincir teknolojisi kullanım davranışını pozitif yönde etkilemektedir.         | RED   |
| H11        | Mali müşavirlerin blokzincir teknolojisi kullanımına yönelik tutumları, kullanım davranışını pozitif yönde etkilemektedir.        | KABUL |
| H12        | Mali müşavirlerin blokzincir teknolojisi kullanımına yönelik niyetleri, kullanım davranışını pozitif yönde etkilemektedir.        | RED   |

TKM Hipotez Sonuç Tablosu'nda görüldüğü üzere; hipotezlerin 9'u reddedilirken, 3'ü kabul edilmiştir. Bu sonuçlara göre TKM boyutları açısından; “Engel” dış değişkeninin, blokzincir teknolojisi kabulüne yönelik tutum, niyet ve davranışın üzerinde herhangi bir anlamlı etkisinin olmadığı görülmektedir. Diğer yandan modelde yer alan “Algılanan Fayda” değişkeninin, blokzincir teknolojisi kullanımına yönelik tutum ve davranışa anlamlı bir etkisi bulunmazken; niyet üzerinde pozitif yönde bir etkisi bulunmakta ve mali müşavirlerin algıladıkları fayda düzeyindeki 1 birimlik standart sapmadaki artış, blokzincir teknolojisini kullanma niyetlerinin 0.049'luk standart sapma kadar artmasını sağlamaktadır. “Algılanan Kullanım Kolaylığı” değişkeni ise, blokzincir teknolojisi kullanımına yönelik niyet ve davranışa anlamlı bir etkide bulunmazken; tutum üzerinde pozitif yönde anlamlı bir etki yaratmaktadır. Bu etki, mali müşavirlerin algıladıkları kullanım kolaylığına ilişkin 1 birimlik standart sapma artışının, blokzincir teknolojisini kullanma tutumlarını 0.060'lık standart sapma kadar artırması düzeyinde gerçekleşmektedir. Ayrıca mali müşavirlerin blokzincir teknolojisini kullanma niyetleri, tutum değişkeninden etkilenmediği gibi, davranış değişkeni üzerinde de herhangi bir anlamlı etkiye sahip değildir. Buna rağmen tutum değişkeninin, blokzincir teknolojisi kullanımına yönelik davranış üzerinde doğrudan pozitif yönde anlamlı bir etkisi bulunmaktadır.

Özetle, araştırma bulgularına göre; tutum değişkeni üzerinde algılanan kullanım kolaylığı değişkeninin etkileri gözlemlenebiliyorken; algılanan fayda değişkeninin tutum üzerindeki etkisi gözlemlenememektedir. Buna rağmen niyeti doğrudan etkilemekte ancak niyetin ise davranış üzerinde etkisi bulunmamaktadır. Dolayısıyla yalnızca algılanan kullanım kolaylığı ile tutum değişkenlerinin blokzincir kullanım davranışı üzerindeki toplam etkisi istatistiksel olarak anlamlı bulunmaktadır. Sonuç olarak; Teknoloji Kabul Modeli değişkenlerinin, blokzincir teknolojisi kullanım davranışı üzerindeki etkileri açığa çıkmamıştır. Bu durum, değişkenler arasındaki düzenleyici ve aracı etkilerin varlığına ilişkin bir işaret olarak yorumlanabilir.

### **7.3.6 Demografik Özelliklere Göre TKM Boyutlarına Yönelik Farklılıkların Test Edilmesi ve Sonuçları**

Teknoloji Kabul Modeli Ölçeği verilerinin güvenilirliği, yapılan testler sonucunda değerlendirilmiş ve normallik dağılımı kontrol edilmiştir. Ön veri analizi bulgularına göre; güvenilirlik koşullarının sağlandığı ve veri setinin, normal dağılım gösterdiği tespit

edilmiştir. Bu nedenle; TKM farklılık hipotezleri, parametrik analiz yöntemleri ile test edilmiştir.

TKM Ölçeği ile İstanbul’da faaliyet gösteren mali müşavir meslek mensuplarının blokzincir teknolojisi kabulleri cinsiyet ve mesleki ünvan değişkenleri açısından farklılık analizleri ile ölçülmüştür. Bu bağlamda, her bir değişken için ayrı ayrı olmak üzere grup sayısına bağlı olarak T testi uygulanarak mali müşavirlerin blokzincir teknolojisini kabulleri arasında anlamlı bir fark olup olmadığı tespit edilmiştir.

Blokzincir teknolojisi kabulüne ilişkin demografik ve mesleki farklılıklar ise sırasıyla H13 hipotezi (cinsiyet ile engeller arasında fark vardır), H14 hipotezi (cinsiyet ile algılanan fayda arasında fark vardır), H15 hipotezi (cinsiyet ile algılanan kullanım kolaylığı arasında fark vardır), H16 hipotezi (cinsiyet ile tutum arasında fark vardır), H17 hipotezi (cinsiyet ile niyet arasında fark vardır), H18 hipotezi (cinsiyet ile davranış arasında fark vardır), H19 hipotezi (mesleki ünvan ile engeller arasında fark vardır), H20 hipotezi (mesleki ünvan ile algılanan fayda arasında fark vardır), H21 hipotezi (mesleki ünvan ile algılanan kullanım kolaylığı arasında fark vardır), H22 hipotezi (mesleki ünvan ile tutum arasında fark vardır), H23 hipotezi (mesleki ünvan ile niyet arasında fark vardır), H24 hipotezi (mesleki ünvan ile davranış arasında fark vardır) ile ifade edilmektedir.

Buradan hareketle izleyen alt bölümde; bağımsız değişkenler bazında ilgili hipotezlere ait bulguların özeti birlikte sunulmuştur. Ardından da her bir hipoteze yönelik açıklamalar detaylandırılarak sonuçların istatistiksel anlamlılıkları tartışılmış ve elde edilen bulgular yorumlanmıştır.

#### **7.3.6.1 T testine ait bulgular**

Bu çalışmada, blokzincir teknolojisi kabulüne yönelik farklılık hipotezlerinden H13’ten H24’e kadar olan hipotezler, iki grup sayısına sahip olmaları nedeniyle t testi ile analiz edilmiştir. İlgili hipotezlerin istatistiksel sonuçları cinsiyet ve mesleki ünvan bağımsız değişkenleri itibarıyla sınıflandırılarak aşağıda sırasıyla sunulmaktadır:

#### a. Cinsiyet bağımsız değişkenine ilişkin hipotezler

Mali müşavirlerin blokzincir teknolojisi kullanımına yönelik engel, algılanan fayda, algılanan kullanım kolaylığı, tutum, niyet ve davranışları ile “Cinsiyet” bağımsız değişkenine ait gruplar arasındaki farklılıkların tespit edilmesine yönelik hipotezler sırasıyla H13, H14, H15, H16, H17 ve H18 hipotezleridir. Söz konusu hipotezlerin test edilmesi amacıyla t testi yapılmış ve analiz bulguları Tablo 7.12’de özetlenmiştir. İlgili bulgular tek tek hipotezler ele alınarak istatistiki olarak yorumlanmıştır.

**Tablo 7.12:** Katılımcıların TKM Boyutları Açısından Cinsiyetlerine Göre Farklılıkları.

#### Bağımsız Değişken : Cinsiyet

|     | TKM Boyutları<br>İtibariyle Blokzincir<br>Teknoloji Kabulü | Cinsiyet | N   | Ortalama | Levene Testi |       | P değeri (çift kuyruk) |                      |
|-----|------------------------------------------------------------|----------|-----|----------|--------------|-------|------------------------|----------------------|
|     |                                                            |          |     |          | F            | Sig.  | Eşit varyans           | Eşit olmayan varyans |
| H13 | Engel                                                      | Kadın    | 125 | 3.404    | 3.673        | 0.056 | 0.679                  | 0.655                |
|     |                                                            | Erkek    | 283 | 3.372    |              |       |                        |                      |
| H14 | Algılanan Fayda                                            | Kadın    | 125 | 3.851    | 4.075        | 0.044 | 0.223                  | 0.204                |
|     |                                                            | Erkek    | 283 | 3.735    |              |       |                        |                      |
| H15 | Algılanan Kullanım Kolaylığı                               | Kadın    | 125 | 3.185    | 0.373        | 0.542 | 0.181                  | 0.160                |
|     |                                                            | Erkek    | 283 | 3.068    |              |       |                        |                      |
| H16 | Tutum                                                      | Kadın    | 125 | 2.483    | 0.898        | 0.344 | 0.258                  | 0.242                |
|     |                                                            | Erkek    | 283 | 2.590    |              |       |                        |                      |
| H17 | Niyet                                                      | Kadın    | 125 | 3.613    | 1.734        | 0.189 | 0.361                  | 0.348                |
|     |                                                            | Erkek    | 283 | 3.526    |              |       |                        |                      |
| H18 | Davranış                                                   | Kadın    | 125 | 2.310    | 0.188        | 0.665 | 0.026                  | 0.024                |
|     |                                                            | Erkek    | 283 | 2.535    |              |       |                        |                      |

#### Hipotez 13

**H<sub>0</sub>** : Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik algıladıkları engeller arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik algıladıkları engeller arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul’da faaliyet gösteren meslek mensuplarının cinsiyetlerine göre blokzincir teknolojisinin kabulünde algıladıkları engellere yönelik farklılıkları Tablo 7.12’de verilmiştir. T testi sonuçlarına göre; Levene p değeri (0.056), 0.05’ten büyük olduğundan her iki grup için anakütle varyansları eşit dağılmıştır. Bununla birlikte eşit

varyans p değerinin (0.679) 0.05'ten büyük olduğu görülmektedir. Bu bulgular doğrultusunda; mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik algıladıkları engellere arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup Hipotez 13 reddedilmiştir.

#### **Hipotez 14**

**H<sub>0</sub>** : Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik algılanan fayda arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik algılanan fayda arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul'da faaliyet gösteren meslek mensuplarının cinsiyetlerine göre blokzincir teknolojisinin kabulünde algıladıkları faydalara yönelik farklılıkları Tablo 7.12'de verilmiştir. T testi sonuçlarına göre; Levene p değeri (0.044), 0.05'ten küçük olduğundan her iki grup için anakütle varyanslar eşit dağılmamıştır. Bununla birlikte eşit olmayan varyans p değerinin (0.204) 0.05'ten büyük olduğu görülmektedir. Bu bulgular doğrultusunda; mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik algılanan fayda arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup Hipotez 14 reddedilmiştir.

#### **Hipotez 15**

**H<sub>0</sub>** : Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik algılanan kullanım kolaylığı arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik algılanan kullanım kolaylığı arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul'da faaliyet gösteren meslek mensuplarının cinsiyetlerine göre blokzincir teknolojisinin kabulünde algıladıkları kullanım kolaylığına yönelik farklılıkları Tablo 7.12'de verilmiştir. T testi sonuçlarına göre; Levene p değeri (0.542), 0.05'ten büyük olduğundan her iki grup için anakütle varyansları eşit dağılmıştır. Bununla birlikte eşit varyans p değerinin (0.181) 0.05'ten büyük olduğu görülmektedir. Bu bulgular doğrultusunda; mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik

algılanan kullanım kolaylığı arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup Hipotez 15 reddedilmiştir.

#### ***Hipotez 16***

**H<sub>0</sub>** : Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik tutumları arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik tutumları arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul'da faaliyet gösteren meslek mensuplarının cinsiyetlerine göre blokzincir teknolojisinin kabulüne ilişkin tutumlarına yönelik farklılıkları Tablo 7.12'de verilmiştir. T testi sonuçlarına göre; Levene p değeri (0.344), 0.05'ten büyük olduğundan her iki grup için anakütle varyansları eşit dağılmıştır. Bununla birlikte eşit varyans p değerinin (0.258) 0.05'ten büyük olduğu görülmektedir. Bu bulgular doğrultusunda; mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik tutumları arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup Hipotez 16 reddedilmiştir.

#### ***Hipotez 17***

**H<sub>0</sub>** : Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik niyetleri arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik niyetleri arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul'da faaliyet gösteren meslek mensuplarının cinsiyetlerine göre blokzincir teknolojisinin kabulüne ilişkin niyetlerine yönelik farklılıkları Tablo 7.12'de verilmiştir. T testi sonuçlarına göre; Levene p değeri (0.189), 0.05'ten büyük olduğundan her iki grup için anakütle varyansları eşit dağılmıştır. Bununla birlikte eşit varyans p değerinin (0.361) 0.05'ten büyük olduğu görülmektedir. Bu bulgular doğrultusunda; mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik niyetleri arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup Hipotez 17 reddedilmiştir.

### ***Hipotez 18***

**H<sub>0</sub>** : Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik davranışları arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik davranışları arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul’da faaliyet gösteren meslek mensuplarının cinsiyetlerine göre blokzincir teknolojisinin kabulüne ilişkin davranışlarına yönelik farklılıkları Tablo 7.12’de verilmiştir. T testi sonuçlarına göre; Levene p değeri (0.665), 0.05’ten büyük olduğundan her iki grup için anakütle varyansları eşit dağılmıştır. Bununla birlikte eşit varyans p değerinin (0.026) 0.05’ten küçük olduğu görülmektedir. Ayrıca grup ortalamaları değerlendirildiğinde “erkek”ler 2.54 ortalama ile daha yüksek ortalamaya sahip bulunmaktadır. Bu bulgular doğrultusunda; mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik davranışları arasında istatistiksel olarak anlamlı bir farklılık tespit edilmiş olup Hipotez 18 kabul edilmiştir.

#### ***b. Mesleki ünvan bağımsız değişkenine ilişkin hipotezler***

Mali müşavirlerin blokzincir teknolojisi kullanımına yönelik engel, algılanan fayda, algılanan kullanım kolaylığı, tutum, niyet ve davranışları ile “Mesleki Ünvan” bağımsız değişkenine ait gruplar arasındaki farklılıkların tespit edilmesine yönelik hipotezler sırasıyla H19, H20, H21, H22, H23 ve H24 hipotezleridir. Söz konusu hipotezlerin test edilmesi amacıyla t testi yapılmış ve analiz bulguları Tablo 7.13’te özetlenmiştir. İlgili bulgular tek tek hipotezler ele alınarak istatistiki olarak yorumlanmıştır.

**Tablo 7.13:** Katılımcıların TKM Boyutları Açısından Mesleki Ünvanlarına Göre Farklılıkları.

**Bağımsız Değişken : Mesleki Ünvan**

|     | TKM Boyutları<br>İtibariyle Blokzincir<br>Teknoloji Kabulü | Cinsiyet | N   | Ortalama | Levene Testi |       | P değeri (çift kuyruk) |                                 |
|-----|------------------------------------------------------------|----------|-----|----------|--------------|-------|------------------------|---------------------------------|
|     |                                                            |          |     |          | F            | Sig.  | Eşit varyans<br>(p1)   | Eşit varyans<br>olmayan<br>(p2) |
| H19 | Engel                                                      | SMMM     | 374 | 3.371    | 1.158        | 0.282 | 0.306                  | 0.232                           |
|     |                                                            | YMM      | 34  | 3.500    |              |       |                        |                                 |
| H20 | Algılanan Fayda                                            | SMMM     | 374 | 3.752    | 1.614        | 0.205 | 0.170                  | 0.095                           |
|     |                                                            | YMM      | 34  | 3.971    |              |       |                        |                                 |
| H21 | Algılanan Kullanım<br>Kolaylığı                            | SMMM     | 374 | 3.103    | 0.576        | 0.448 | 0.918                  | 0.913                           |
|     |                                                            | YMM      | 34  | 3.118    |              |       |                        |                                 |
| H22 | Tutum                                                      | SMMM     | 374 | 2.581    | 0.763        | 0.383 | 0.070                  | 0.060                           |
|     |                                                            | YMM      | 34  | 2.294    |              |       |                        |                                 |
| H23 | Niyet                                                      | SMMM     | 374 | 3.543    | 0.208        | 0.649 | 0.472                  | 0.436                           |
|     |                                                            | YMM      | 34  | 3.657    |              |       |                        |                                 |
| H24 | Davranış                                                   | SMMM     | 374 | 2.464    | 1.514        | 0.219 | 0.901                  | 0.894                           |
|     |                                                            | YMM      | 34  | 2.485    |              |       |                        |                                 |

**Hipotez 19**

**H<sub>0</sub>** : Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımında algılanan dış etkenler (engeller) arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımında algılanan dış etkenler (engeller) arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul'da faaliyet gösteren meslek mensuplarının ünvanlarına göre blokzincir teknolojisinin kabulünde algıladıkları engellere yönelik farklılıkları Tablo 7.13'te verilmiştir. T testi sonuçlarına göre; Levene p değeri (0.282), 0.05'ten büyük olduğundan her iki grup için anakütle varyansları eşit dağılmıştır. Bununla birlikte eşit varyans p değerinin (0.306) 0.05'ten büyük olduğu görülmektedir. Bu bulgular doğrultusunda; mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımında algılanan engeller arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup Hipotez 19 reddedilmiştir.



### ***Hipotez 20***

**H<sub>0</sub>** : Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımında algılanan dış etkenler (engeller) arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımında algılanan dış etkenler (engeller) arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul'da faaliyet gösteren meslek mensuplarının ünvanlarına göre blokzincir teknolojisinin kabulünde algılanan faydaya yönelik farklılıkları Tablo 7.13'te verilmiştir. T testi sonuçlarına göre; Levene p değeri (0.205), 0.05'ten büyük olduğundan her iki grup için anakütle varyansları eşit dağılmıştır. Bununla birlikte eşit varyans p değerinin (0.170) 0.05'ten büyük olduğu görülmektedir. Bu bulgular doğrultusunda; mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımında algılanan fayda arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup Hipotez 20 reddedilmiştir.

### ***Hipotez 21***

**H<sub>0</sub>** : Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımında algılanan kullanım kolaylığı arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımında algılanan kullanım kolaylığı arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul'da faaliyet gösteren meslek mensuplarının ünvanlarına göre blokzincir teknolojisinin kabulünde algılanan kullanım kolaylığına yönelik farklılıkları Tablo 7.13'te verilmiştir. T testi sonuçlarına göre; Levene p değeri (0.448), 0.05'ten büyük olduğundan her iki grup için anakütle varyansları eşit dağılmıştır. Bununla birlikte eşit varyans p değerinin (0.918) 0.05'ten büyük olduğu görülmektedir. Bu bulgular doğrultusunda; mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımında algılanan kullanım kolaylığı arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup Hipotez 21 reddedilmiştir.

### ***Hipotez 22***

**H<sub>0</sub>** : Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımına yönelik tutumları arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımına yönelik tutumları arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul'da faaliyet gösteren meslek mensuplarının ünvanlarına göre blokzincir teknolojisinin kabulüne ilişkin tutumlarına yönelik farklılıkları Tablo 7.13'te verilmiştir. T testi sonuçlarına göre; Levene p değeri (0.383), 0.05'ten büyük olduğundan her iki grup için anakütle varyansları eşit dağılmıştır. Bununla birlikte eşit varyans p değerinin (0.070) 0.05'ten büyük olduğu görülmektedir. Bu bulgular doğrultusunda; mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımına yönelik tutumları arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup Hipotez 22 reddedilmiştir.

### ***Hipotez 23***

**H<sub>0</sub>** : Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımına yönelik niyetleri arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımına yönelik niyetleri arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul'da faaliyet gösteren meslek mensuplarının ünvanlarına göre blokzincir teknolojisinin kabulüne ilişkin niyetlerine yönelik farklılıkları Tablo 7.13'te verilmiştir. T testi sonuçlarına göre; Levene p değeri (0.649), 0.05'ten büyük olduğundan her iki grup için anakütle varyansları eşit dağılmıştır. Bununla birlikte eşit varyans p değerinin (0.472) 0.05'ten büyük olduğu görülmektedir. Bu bulgular doğrultusunda; mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımına yönelik niyetleri arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup Hipotez 23 reddedilmiştir.

#### **Hipotez 24**

**H<sub>0</sub>** : Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımına yönelik davranışları arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımına yönelik davranışları arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul’da faaliyet gösteren meslek mensuplarının ünvanlarına göre blokzincir teknolojisinin kabulüne ilişkin davranışlarına yönelik farklılıkları Tablo 7.13’te verilmiştir. T testi sonuçlarına göre; Levene p değeri (0.219), 0.05’ten büyük olduğundan her iki grup için anakütle varyansları eşit dağılmıştır. Bununla birlikte eşit varyans p değerinin (0.901) 0.05’ten büyük olduğu görülmektedir. Bu bulgular doğrultusunda; mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımına yönelik davranışları arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup Hipotez 24 reddedilmiştir.

#### **7.3.6.2 TKM farklılık hipotezlerinin sonuçları**

Teknoloji Kabul Modeli kapsamında gerçekleştirilen ve önceki bölümlerde bulguları açıklanan t testi ile test edilen hipotezlere ilişkin sonuçlar aşağıda Tablo 7.14’te özetlenmiştir.

**Tablo 7.14:** TKM Farklılık Hipotezlerinin Sonuçları.

| <b>HİPOTEZLER</b> |                                                                                                                                         | <b>SONUÇ</b> |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <b>H13</b>        | Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımında algılanan dış etkenler (engeller) arasında anlamlı bir fark vardır. | RED          |
| <b>H14</b>        | Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımında algılanan fayda arasında anlamlı bir fark vardır.                   | RED          |
| <b>H15</b>        | Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımında algılanan kullanım kolaylığı arasında anlamlı bir fark vardır.      | RED          |
| <b>H16</b>        | Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik tutumları arasında anlamlı bir fark vardır.                  | RED          |
| <b>H17</b>        | Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik niyetleri arasında anlamlı bir fark vardır.                  | RED          |

**Tablo 7.14:** TKM Farklılık Hipotezlerinin Sonuçları (Devam).

|            |                                                                                                                                      |       |
|------------|--------------------------------------------------------------------------------------------------------------------------------------|-------|
| <b>H18</b> | Mali müşavirlerin cinsiyeti ile blokzincir teknolojisi kullanımına yönelik davranışları arasında anlamlı bir fark vardır.            | KABUL |
| <b>H19</b> | Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımında algılanan dış etkenler (engeller) arasında anlamlı bir fark vardır. | RED   |
| <b>H20</b> | Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımında algılanan fayda arasında anlamlı bir fark vardır.                   | RED   |
| <b>H21</b> | Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımında algılanan kullanım kolaylığı arasında anlamlı bir fark vardır.      | RED   |
| <b>H22</b> | Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımına yönelik tutumları arasında anlamlı bir fark vardır.                  | RED   |
| <b>H23</b> | Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımına yönelik niyetleri arasında anlamlı bir fark vardır.                  | RED   |
| <b>H24</b> | Mali müşavirlerin ünvanı ile blokzincir teknolojisi kullanımına yönelik davranışları arasında anlamlı bir fark vardır.               | RED   |

TKM Hipotez Sonuç Tablosu'nda görüldüğü üzere; hipotezlerin 10'u reddedilirken, 1'i kabul edilmiştir. Bu sonuçlara göre; mali müşavirlerin mesleki ünvan özellikleri yani SMMM veya YMM olmaları, TKM ölçeği boyutları üzerinden meslek mensuplarının blokzincir teknolojisi kabullerinde herhangi bir farklılık yaratmamaktadır. Diğer yandan cinsiyet özelliği de davranış boyutu hariç diğer boyutlar üzerinde yine herhangi bir farklılık ortaya çıkarmamaktadır. Cinsiyete ilişkin blokzincir teknolojisi kabul davranışındaki farklılıklar incelendiğinde ise grup ortalamalarına göre erkeklerin (2.54), blokzincir teknolojisini kullanma eğilimlerinin kadınlara (2.31) kıyasla görece daha fazla olmasıyla birlikte aradaki farkın çok yüksek olmadığı görülmektedir.

#### **7.4 HİLE ARAŞTIRMALARI ÖLÇEĞİNE AİT BULGULAR**

Çalışmanın bu bölümünde, hile araştırmaları ölçeğine uygulanan çeşitli analiz yöntemlerine ait bulgular açıklanmıştır. Bu bağlamda öncelikle güvenilirlik ve normal dağılım kontrolü gibi ön analizler yapılmış ve bu ön analizlerin sonucuna göre uygulanacak analiz yöntemleri belirlenmiştir. Daha sonra hile araştırmaları ölçeği çerçevesinde muhasebe hileleri ile karşılaşma sıklıkları ve blokzincir teknolojisinin muhasebe hilelerini önlemedeki rolüne ilişkin mali müşavirlerin görüşlerinin test edilmesine yönelik katılımcıların demografik ve

mesleki özelliklerine göre farklılıkları araştırılmıştır. Bu kapsamda da Mann-Whitney U ve Kruskal-Wallis testleri uygulanarak bulgular özetlenmiş ve yorumlanmıştır.

#### 7.4.1 Güvenilirlik Analizine Ait Bulgular

TKM ölçeğinde olduğu gibi hile araştırmaları ölçeği kapsamında da güvenilirlik analizi<sup>59</sup>, Cronbach alfa katsayısı referans alınarak gerçekleştirilmiştir. Buna göre; hile araştırmaları ölçeğine ilişkin alfa değeri 0.920 olarak hesaplanmış olup 0.70 alt sınırı aştığından ölçek iç tutarlılığı sağlanmıştır. Dolayısıyla hile araştırmaları ölçeği güvenilirlerdir.

#### 7.4.2 Normallik Testi ve Tanımlayıcı İstatistik Bulguları

Çalışmanın bu bölümünde, hile araştırmaları kapsamında tanımlayıcı istatistiksel bulgulara yer verilmiş ve verinin normal dağılım kontrolü<sup>60</sup> yapılmıştır. Normallik testi, gözlem sayısının 408 olması yani 29’dan büyük olması nedeniyle Kolmogorov-Smirnov testi ile yapılmıştır. Söz konusu istatistiki bulgular ile normallik testi sonuçları Tablo 7.15’te verilmiştir.

**Tablo 7.15:** Hile Araştırmaları Ölçeğine İlişkin Normallik Testi ve Tanımlayıcı İstatistik Bulguları.

| Ölçekler                                                      | N   | Min. | Max. | Ortalama | Standart Sapma | Çarpıklık | Basıklık | K-S Sig. |
|---------------------------------------------------------------|-----|------|------|----------|----------------|-----------|----------|----------|
| Muhasebe Hileleri ile Karşılaşma Sıklığı                      | 408 | 1    | 5    | 2.3110   | 0.90594        | 0.521     | -2.121   | < 0.001  |
| Muhasebe Hilelerinin Önlenmesine Yönelik Faaliyetler          | 408 | 1    | 5    | 3.7648   | 0.72351        | -1.195    | 3.009    | < 0.001  |
| Blokzincir Teknolojisinin Muhasebe Hilelerini Önlemedeki Rolü | 408 | 1    | 5    | 3.5139   | 0.65105        | -0.519    | 2.267    | < 0.001  |

Kolmogorov-Smirnov testi sonucu p değeri 0.05’in altında bulunmuştur. Bununla birlikte ölçek verilerine ilişkin çarpıklık ve basıklık değerleri de kabul edilebilir aralık olan  $\pm 2$  arasında gerçekleşmemiştir. Bu nedenle normal dağılım uygunluk koşulları

<sup>59</sup> “Güvenilirlik analizi” hakkında detaylı bilgi için bkz. s.258.

<sup>60</sup> “Normal dağılım” hakkında detaylı bilgi için bkz. s.258.

sağlanamamıştır. Dolayısıyla hile araştırmaları ölçek verilerine ait dağılım, normal dağılım göstermemektedir.

#### **7.4.3 Demografik ve Mesleki Özelliklere Göre Hile Belirtileri ile Karşılaşma Sıklıklarına Yönelik Farklılıkların Test Edilmesi ve Sonuçları**

Hile Araştırmaları Ölçeği verilerinin güvenilirliği, yapılan testler sonucunda değerlendirilmiş ve normallik dağılımı kontrol edilmiştir. Ön veri analizi bulgularına göre; güvenilirlik koşulları sağlanırken, veri setinin, normal dağılım göstermediği tespit edilmiştir. Bu nedenle hile belirtileri ile karşılaşma sıklıklarına yönelik hipotezler, parametrik olmayan analiz yöntemleri ile test edilmiştir.

Hile Araştırmaları Ölçeği ile İstanbul'da faaliyet gösteren meslek mensuplarının demografik ve mesleki özelliklerine göre hile belirtileri ile karşılaşma sıklıkları, cinsiyet, eğitim düzeyi, mesleki ünvan, çalışma şekli, mesleki tecrübe ve mükellef sayısı gibi değişkenler açısından farklılık analizleri ile ölçülmüştür. Bu bağlamda her bir değişken için ayrı ayrı olmak üzere grup sayısına bağlı olarak Mann-Whitney U ve Kruskal-Wallis testleri uygulanarak hile belirtileri görülen işlemlerle karşılaşma sıklığı arasında anlamlı bir fark olup olmadığı tespit edilmiştir.

Finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığına ilişkin demografik ve mesleki farklılıklar ise sırasıyla H25 hipotezi (cinsiyet ile arasında fark vardır), H26 hipotezi (eğitim düzeyi ile arasında fark vardır), H27 hipotezi (mesleki ünvan ile arasında fark vardır), H28 hipotezi (çalışma şekli ile arasında fark vardır), H29 hipotezi (mesleki tecrübe ile arasında fark vardır) ve H30 hipotezi (mükellef sayısı ile arasında fark vardır) ile ifade edilmektedir.

Buradan hareketle; analiz bulguları, uygulanan analiz yöntemleri itibarıyla sınıflandırılarak ilgili hipotezlere yönelik sonuçların istatistiksel anlamlılıkları tartışılmıştır. İzleyen alt bölümde ise hipotez sonuçlarının özeti sunularak elde edilen bulgular yorumlanmıştır.

##### **7.4.3.1 Mann-Whitney U testine ait bulgular**

Bu çalışmada, hile belirtileri ile karşılaşma sıklıklarına yönelik hipotezlerden H25, H27 ve H28 hipotezleri, iki grup sayısına sahip olmaları nedeniyle Mann-Whitney U testi ile analiz edilmiştir. İlgili hipotezlere dair istatistiksel açıklamalar aşağıda sırasıyla sunulmuştur:

### Hipotez 25

**H<sub>0</sub>** : Mali müşavirlerin cinsiyeti ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin cinsiyeti ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır.

**Tablo 7.16** Katılımcıların Hile Belirtileri ile Karşılaşma Sıklıkları Açısından Cinsiyetlerine Göre Farklılıkları.

|    | Hile Belirtileri Görülen İşlemler ve Hile Belirtileri ile Karşılaşma Sıklığı | Cinsiyet | N   | Ortalama | M-W P değeri |
|----|------------------------------------------------------------------------------|----------|-----|----------|--------------|
| 1  | Çek düzenleme işlemlerinde hile belirtileri                                  | Kadın    | 121 | 192.42   | 0.334        |
|    |                                                                              | Erkek    | 279 | 204.00   |              |
| 2  | Fatura düzenleme işlemlerinde hile belirtileri                               | Kadın    | 123 | 189.83   | 0.132        |
|    |                                                                              | Erkek    | 281 | 208.04   |              |
| 3  | Satışlar ve satış iadeleri işlemlerinde hile belirtileri                     | Kadın    | 120 | 185.27   | 0.065        |
|    |                                                                              | Erkek    | 281 | 207.72   |              |
| 4  | Bordro düzenleme işlemlerinde hile belirtileri                               | Kadın    | 119 | 180.89   | 0.028*       |
|    |                                                                              | Erkek    | 279 | 207.44   |              |
| 5  | Çeşitli gider ödemeleri işlemlerinde hile belirtileri                        | Kadın    | 119 | 181.49   | 0.031*       |
|    |                                                                              | Erkek    | 280 | 207.87   |              |
| 6  | Stoklar ve duran varlıklar işlemlerinde hile belirtileri                     | Kadın    | 118 | 175.01   | 0.005*       |
|    |                                                                              | Erkek    | 279 | 209.15   |              |
| 7  | Banka havaaleleri işlemlerinde hile belirtileri                              | Kadın    | 120 | 188.57   | 0.188        |
|    |                                                                              | Erkek    | 278 | 204.22   |              |
| 8  | Nakit ödemeler/tahsilatlar işlemlerinde hile belirtileri                     | Kadın    | 119 | 180.34   | 0.018*       |
|    |                                                                              | Erkek    | 281 | 209.04   |              |
| 9  | Envanter ve satın alma işlemlerinde hile belirtileri                         | Kadın    | 120 | 177.83   | 0.008*       |
|    |                                                                              | Erkek    | 280 | 210.21   |              |
| 10 | Borç ve ödeme işlemlerinde hile belirtileri                                  | Kadın    | 119 | 179.09   | 0.016*       |
|    |                                                                              | Erkek    | 279 | 208.21   |              |
| 11 | Alacak ve tahsilat işlemlerinde hile belirtileri                             | Kadın    | 121 | 180.67   | 0.014*       |
|    |                                                                              | Erkek    | 281 | 210.47   |              |
| 12 | Belge ve kayıt düzeninde hile belirtileri                                    | Kadın    | 122 | 188.56   | 0.126        |
|    |                                                                              | Erkek    | 280 | 207.14   |              |

Araştırmaya katılan İstanbul’da faaliyet gösteren meslek mensuplarının cinsiyetlerine göre hile belirtileri ile karşılaşma sıklıkları açısından farklılıkları Tablo 7.16’da verilmiştir. Mann-Whitney U testi sonuçlarına göre; “4-bordro düzenleme”, “5-çeşitli gider ödemeleri işlemlerinde”, “6-stoklar ve duran varlık işlemlerinde”, “8-nakit ödeme işlemlerinde”, “9-envanter işlemlerinde”, “10-borç ve ödeme işlemlerinde” ve “11-alacak işlemlerinde” görülen hile belirtilerine ilişkin ifadelerle ait p değerleri 0.05’ten küçük iken; kalan beş adet ifadeye ilişkin p değerleri 0.05’ten büyüktür. Diğer yandan gruplara ait ortalamalar da p değeri sonuçlarını desteklemekte; 0.5’ten büyük olan değerlerde ortalamalar arası fark düşük iken, 0.5’ten küçük olan değerlerde ortalamalar arası fark yüksektir. Ayrıca grup ortalamaları genel olarak değerlendirildiğinde, tüm ifadelerde “erkek”lerin daha yüksek ortalamaya sahip oldukları görülmektedir. Bununla birlikte tüm hile belirtisi maddeleri birlikte değerlendirildiğinde; ortalama p değeri (0.009), 0.05’ten küçük hesaplanmaktadır. Bu bulgular doğrultusunda; mali müşavirlerin cinsiyeti ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklıkları arasında istatistiksel olarak anlamlı bir farklılık tespit edilmiş olup Hipotez 25 kabul edilmiştir.

#### ***Hipotez 27***

**H<sub>0</sub>** : Mali müşavirlerin ünvanı ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin ünvanı ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul’da faaliyet gösteren meslek mensuplarının mesleki ünvanlarına göre hile belirtileri ile karşılaşma sıklıkları açısından farklılıkları Tablo 7.17’de verilmiştir. Mann-Whitney U testi sonuçlarına göre; çek düzenleme, fatura düzenleme ve banka havale işlemlerinde görülen hile belirtileri dışındaki tüm hile belirtilerinin görülmesine ilişkin ifadelerle ait p değerleri 0.05’ten küçüktür. Diğer yandan gruplara ait ortalamalar da p değerini desteklemekte ve bu üç hile belirtisi dışındaki belirtilere ait grup ortalamalarında “YMM”lerin daha yüksek ortalamaya sahip oldukları görülmektedir. Tüm hile belirtisi maddeleri birlikte değerlendirildiğinde ise ortalama p değeri (0.001) yine 0.05’ten küçük hesaplanmaktadır. Bu bulgular doğrultusunda; mali müşavirlerin ünvanı ile finansal bilgi



manipölasyonu göstergeleriyle karşılaşma sıklıkları arasında istatistiksel olarak anlamlı bir farklılık tespit edilmiş olup, Hipotez 27 kabul edilmiştir.

**Tablo 7.17:** Katılımcıların Hile Belirtileri ile Karşılaşma Sıklıkları Açısından Mesleki Ünvanlarına Göre Farklılıkları.

|    | Hile Belirtileri Görülen İşlemler ve Hile Belirtileri ile Karşılaşma Sıklığı | Mesleki Ünvan | N   | Ortalama | M-W P değeri |
|----|------------------------------------------------------------------------------|---------------|-----|----------|--------------|
| 1  | Çek düzenleme işlemlerinde hile belirtileri                                  | SMMM          | 366 | 198.82   | 0.316*       |
|    |                                                                              | YMM           | 34  | 218.62   |              |
| 2  | Fatura düzenleme işlemlerinde hile belirtileri                               | SMMM          | 370 | 199.26   | 0.055*       |
|    |                                                                              | YMM           | 34  | 237.71   |              |
| 3  | Satışlar ve satış iadeleri işlemlerinde hile belirtileri                     | SMMM          | 367 | 197.05   | 0.020        |
|    |                                                                              | YMM           | 34  | 243.59   |              |
| 4  | Bordro düzenleme işlemlerinde hile belirtileri                               | SMMM          | 364 | 194.06   | 0.001        |
|    |                                                                              | YMM           | 34  | 257.74   |              |
| 5  | Çeşitli gider ödemeleri işlemlerinde hile belirtileri                        | SMMM          | 365 | 193.32   | 0.000        |
|    |                                                                              | YMM           | 34  | 271.69   |              |
| 6  | Stoklar ve duran varlıklar işlemlerinde hile belirtileri                     | SMMM          | 363 | 193.82   | 0.002        |
|    |                                                                              | YMM           | 34  | 254.34   |              |
| 7  | Banka havaleleri işlemlerinde hile belirtileri                               | SMMM          | 364 | 196.96   | 0.128*       |
|    |                                                                              | YMM           | 34  | 226.68   |              |
| 8  | Nakit ödemeler/tahsilatlar işlemlerinde hile belirtileri                     | SMMM          | 366 | 196.77   | 0.027        |
|    |                                                                              | YMM           | 34  | 240.71   |              |
| 9  | Envanter ve satın alma işlemlerinde hile belirtileri                         | SMMM          | 366 | 194.49   | 0.000        |
|    |                                                                              | YMM           | 34  | 265.21   |              |
| 10 | Borç ve ödeme işlemlerinde hile belirtileri                                  | SMMM          | 364 | 194.86   | 0.006        |
|    |                                                                              | YMM           | 34  | 249.21   |              |
| 11 | Alacak ve tahsilat işlemlerinde hile belirtileri                             | SMMM          | 368 | 195.74   | 0.001        |
|    |                                                                              | YMM           | 34  | 263.85   |              |
| 12 | Belge ve kayıt düzeninde hile belirtileri                                    | SMMM          | 368 | 196.55   | 0.004        |
|    |                                                                              | YMM           | 34  | 255.07   |              |

### Hipotez 28

**H<sub>0</sub>** : Mali müşavirlerin çalışma şekli (bağımlı – bağımsız) ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin çalışma şekli (bağımlı – bağımsız) ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır.

**Tablo 7.18:** Katılımcıların Hile Belirtileri ile Karşılaşma Sıklıkları Açısından Çalışma Şekillerine Göre Farklılıkları.

|    | Hile Belirtileri Görülen İşlemler ve Hile Belirtileri ile Karşılaşma Sıklığı | Çalışma Şekli | N   | Ortalama | M-W P değeri |
|----|------------------------------------------------------------------------------|---------------|-----|----------|--------------|
| 1  | Çek düzenleme işlemlerinde hile belirtileri                                  | Bağımlı       | 113 | 191.33   | 0.296        |
|    |                                                                              | Bağımsız      | 287 | 204.11   |              |
| 2  | Fatura düzenleme işlemlerinde hile belirtileri                               | Bağımlı       | 115 | 183.25   | 0.029*       |
|    |                                                                              | Bağımsız      | 289 | 210.16   |              |
| 3  | Satışlar ve satış iadeleri işlemlerinde hile belirtileri                     | Bağımlı       | 111 | 190.65   | 0.251        |
|    |                                                                              | Bağımsız      | 290 | 204.96   |              |
| 4  | Bordro düzenleme işlemlerinde hile belirtileri                               | Bağımlı       | 112 | 188.61   | 0.218        |
|    |                                                                              | Bağımsız      | 286 | 203.76   |              |
| 5  | Çeşitli gider ödemeleri işlemlerinde hile belirtileri                        | Bağımlı       | 112 | 186.21   | 0.123        |
|    |                                                                              | Bağımsız      | 287 | 205.38   |              |
| 6  | Stoklar ve duran varlıklar işlemlerinde hile belirtileri                     | Bağımlı       | 112 | 185.45   | 0.128        |
|    |                                                                              | Bağımsız      | 285 | 204.32   |              |
| 7  | Banka havaleleri işlemlerinde hile belirtileri                               | Bağımlı       | 109 | 179.88   | 0.027*       |
|    |                                                                              | Bağımsız      | 289 | 206.90   |              |
| 8  | Nakit ödemeler/tahsilatlar işlemlerinde hile belirtileri                     | Bağımlı       | 112 | 188.01   | 0.161        |
|    |                                                                              | Bağımsız      | 288 | 205.36   |              |
| 9  | Envanter ve satın alma işlemlerinde hile belirtileri                         | Bağımlı       | 112 | 188.49   | 0.179        |
|    |                                                                              | Bağımsız      | 288 | 205.17   |              |
| 10 | Borç ve ödeme işlemlerinde hile belirtileri                                  | Bağımlı       | 110 | 183.07   | 0.067        |
|    |                                                                              | Bağımsız      | 288 | 205.78   |              |
| 11 | Alacak ve tahsilat işlemlerinde hile belirtileri                             | Bağımlı       | 112 | 184.70   | 0.061        |
|    |                                                                              | Bağımsız      | 290 | 207.99   |              |
| 12 | Belge ve kayıt düzeninde hile belirtileri                                    | Bağımlı       | 113 | 189.56   | 0.182        |
|    |                                                                              | Bağımsız      | 289 | 206.17   |              |

Araştırmaya katılan İstanbul’da faaliyet gösteren meslek mensuplarının çalışma şekillerine göre hile belirtileri ile karşılaşma sıklıkları açısından farklılıkları Tablo 7.18’de verilmiştir. Mann-Whitney U testi sonuçlarına göre; fatura düzenleme ve banka havale işlemlerinde görülen hile belirtileri dışındaki tüm hile belirtilerinin görülmesine ilişkin ifadelerle ait p

değerleri 0.05'ten büyüktür. Diğer yandan gruplara ait ortalamalar da p değerini desteklemekte ve bu iki hile belirtisi dışındaki belirtilere ait grup ortalamalarında “Bağımsız”lar daha yüksek ortalamaya sahip olmakla birlikte aradaki farkın çok düşük olduğu görülmektedir. Tüm hile belirtisi maddeleri birlikte değerlendirildiğinde ise ortalama p değeri (0.051) yine 0.05'ten büyük hesaplanmaktadır. Bu bulgular doğrultusunda; mali müşavirlerin çalışma şekli ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklıkları arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup, Hipotez 28 reddedilmiştir.

#### **7.4.3.2 Kruskal-Wallis testine ait bulgular**

Bu çalışmada, hile belirtileri ile karşılaşma sıklıklarına yönelik hipotezlerden H26, H29 ve H30 hipotezleri, iki grup sayısından fazla grup sayısına sahip olmaları nedeniyle Kruskal-Wallis testi ile analiz edilmiştir. İlgili hipotezlere dair istatistiksel açıklamalar aşağıda sırasıyla sunulmuştur:

##### ***Hipotez 26***

**H<sub>0</sub>** : Mali müşavirlerin eğitim düzeyi ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin eğitim düzeyi ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul'da faaliyet gösteren meslek mensuplarının eğitim düzeylerine göre hile belirtileri ile karşılaşma sıklıkları açısından farklılıkları Tablo 7.19'da verilmiştir. Kruskal-Wallis testi sonuçlarına göre; çek düzenleme, “2-fatura düzenleme” ve “6-stoklar ve duran varlıklar işlemlerinde görülen hile belirtileri dışındaki tüm hile belirtilerinin görülmesine ilişkin ifadelerle ait p değerleri 0.05'ten küçüktür. Diğer yandan gruplara ait ortalamalar da p değerini desteklemekte ve bu iki hile belirtisi dışındaki belirtilere ait grup ortalamaları arasındaki farklar da daha yüksektir. Ayrıca grup ortalamaları genel olarak değerlendirildiğinde tüm ifadelerde “doktora” mezunlarının daha yüksek ortalamaya sahip oldukları görülmektedir. Bununla birlikte hile belirtisi maddeleri birlikte değerlendirildiğinde ise ortalama p değeri (0.011) yine 0.05'ten küçük hesaplanmaktadır. Bu bulgular doğrultusunda; mali müşavirlerin eğitim düzeyi ile finansal bilgi manipülasyonu

göstergeleriyle karşılaşma sıklıkları arasında istatistiksel olarak anlamlı bir farklılık tespit edilmiş olup, Hipotez 26 kabul edilmiştir.

**Tablo 7.19:** Katılımcıların Hile Belirtileri ile Karşılaşma Sıklıkları Açısından Eğitim Düzeylerine Göre Farklılıkları.

|   | Hile Belirtileri Görülen İşlemler ve Hile Belirtileri ile Karşılaşma Sıklığı | Eğitim Düzeyi | N   | Ortalama | K-W P değeri |
|---|------------------------------------------------------------------------------|---------------|-----|----------|--------------|
| 1 | Çek düzenleme işlemlerinde hile belirtileri                                  | Lise          | 8   | 179.06   | 0.045        |
|   |                                                                              | Lisans        | 281 | 194.28   |              |
|   |                                                                              | Yüksek Lisans | 100 | 210.75   |              |
|   |                                                                              | Doktora       | 11  | 281.77   |              |
| 2 | Fatura düzenleme işlemlerinde hile belirtileri                               | Lise          | 8   | 153.25   | 0.072*       |
|   |                                                                              | Lisans        | 284 | 196.93   |              |
|   |                                                                              | Yüksek Lisans | 101 | 215.24   |              |
|   |                                                                              | Doktora       | 11  | 265.05   |              |
| 3 | Satışlar ve satış iadeleri işlemlerinde hile belirtileri                     | Lise          | 8   | 142.75   | 0.036        |
|   |                                                                              | Lisans        | 281 | 196.60   |              |
|   |                                                                              | Yüksek Lisans | 101 | 209.36   |              |
|   |                                                                              | Doktora       | 11  | 279.05   |              |
| 4 | Bordro düzenleme işlemlerinde hile belirtileri                               | Lise          | 8   | 212.56   | 0.010        |
|   |                                                                              | Lisans        | 278 | 194.38   |              |
|   |                                                                              | Yüksek Lisans | 101 | 200.79   |              |
|   |                                                                              | Doktora       | 11  | 307.64   |              |
| 5 | Çeşitli gider ödemeleri işlemlerinde hile belirtileri                        | Lise          | 8   | 202.56   | 0.043        |
|   |                                                                              | Lisans        | 280 | 193.48   |              |
|   |                                                                              | Yüksek Lisans | 100 | 208.55   |              |
|   |                                                                              | Doktora       | 11  | 286.36   |              |
| 6 | Stoklar ve duran varlıklar işlemlerinde hile belirtileri                     | Lise          | 7   | 211.07   | 0.227*       |
|   |                                                                              | Lisans        | 278 | 194.56   |              |
|   |                                                                              | Yüksek Lisans | 101 | 203.40   |              |
|   |                                                                              | Doktora       | 11  | 263.09   |              |
| 7 | Banka havaleleri işlemlerinde hile belirtileri                               | Lise          | 6   | 186.83   | 0.010        |
|   |                                                                              | Lisans        | 282 | 194.75   |              |
|   |                                                                              | Yüksek Lisans | 99  | 201.92   |              |
|   |                                                                              | Doktora       | 11  | 306.32   |              |

**Tablo 7.19 : Katılımcıların Hile Belirtileri ile Karşılaşma Sıklıkları Açısından Eğitim Düzeylerine Göre Farklılıkları (Devam).**

|    | Hile Belirtileri Görülen İşlemler ve Hile Belirtileri ile Karşılaşma Sıklığı | Eğitim Düzeyi | N   | Ortalama | K-W P değeri |
|----|------------------------------------------------------------------------------|---------------|-----|----------|--------------|
| 8  | Nakit ödemeler/tahsilatlar işlemlerinde hile belirtileri                     | Lise          | 8   | 207.94   | 0.027        |
|    |                                                                              | Lisans        | 279 | 199.06   |              |
|    |                                                                              | Yüksek Lisans | 102 | 193.20   |              |
|    |                                                                              | Doktora       | 11  | 299.27   |              |
| 9  | Envanter ve satın alma işlemlerinde hile belirtileri                         | Lise          | 7   | 195.21   | 0.008        |
|    |                                                                              | Lisans        | 281 | 195.79   |              |
|    |                                                                              | Yüksek Lisans | 101 | 201.66   |              |
|    |                                                                              | Doktora       | 11  | 313.41   |              |
| 10 | Borç ve ödeme işlemlerinde hile belirtileri                                  | Lise          | 7   | 201.50   | 0.007        |
|    |                                                                              | Lisans        | 279 | 195.35   |              |
|    |                                                                              | Yüksek Lisans | 101 | 198.37   |              |
|    |                                                                              | Doktora       | 11  | 314.00   |              |
| 11 | Alacak ve tahsilat işlemlerinde hile belirtileri                             | Lise          | 8   | 170.00   | 0.006        |
|    |                                                                              | Lisans        | 281 | 196.22   |              |
|    |                                                                              | Yüksek Lisans | 102 | 206.47   |              |
|    |                                                                              | Doktora       | 11  | 313.14   |              |
| 12 | Belge ve kayıt düzeninde hile belirtileri                                    | Lise          | 8   | 179.25   | 0.003        |
|    |                                                                              | Lisans        | 281 | 195.11   |              |
|    |                                                                              | Yüksek Lisans | 102 | 208.08   |              |
|    |                                                                              | Doktora       | 11  | 319.82   |              |

### Hipotez 29

**H<sub>0</sub> :** Mali müşavirlerin mesleki tecrübesi (çalışma süresi) ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark yoktur.

**H<sub>1</sub>:** Mali müşavirlerin mesleki tecrübesi (çalışma süresi) ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul’da faaliyet gösteren meslek mensuplarının mesleki tecrübelerine göre hile belirtileri ile karşılaşma sıklıkları açısından farklılıkları Tablo 7.20’de verilmiştir. Kruskal-Wallis testi sonuçlarına göre; tüm hile belirtilerinin görülmesine ilişkin ifadelerle ait p değerleri 0.05’ten büyüktür. Diğer yandan gruplara ait ortalamaların birbirine

çok yakın olması da bu sonuçları desteklemektedir. Bu bulgular doğrultusunda; mali müşavirlerin çalışma şekli ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklıkları arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup, Hipotez 29 reddedilmiştir.

**Tablo 7.20:** Katılımcıların Hile Belirtileri ile Karşılaşma Sıklıkları Açısından Mesleki Tecrübelerine Göre Farklılıkları.

|   | Hile Belirtileri Görülen İşlemler ve Hile Belirtileri ile Karşılaşma Sıklığı | Mesleki Tecrübe | N   | Ortalama | K-W P değeri |
|---|------------------------------------------------------------------------------|-----------------|-----|----------|--------------|
| 1 | Çek düzenleme işlemlerinde hile belirtileri                                  | 1-5 yıl         | 17  | 243.88   | 0.492        |
|   |                                                                              | 6-10 yıl        | 32  | 204.02   |              |
|   |                                                                              | 11-15 yıl       | 71  | 196.37   |              |
|   |                                                                              | 16-20 yıl       | 95  | 191.75   |              |
|   |                                                                              | 21 yıl ve üzeri | 185 | 201.98   |              |
| 2 | Fatura düzenleme işlemlerinde hile belirtileri                               | 1-5 yıl         | 17  | 225.03   | 0.929        |
|   |                                                                              | 6-10 yıl        | 32  | 204.25   |              |
|   |                                                                              | 11-15 yıl       | 71  | 201.16   |              |
|   |                                                                              | 16-20 yıl       | 95  | 197.89   |              |
|   |                                                                              | 21 yıl ve üzeri | 189 | 203.00   |              |
| 3 | Satışlar ve satış iadeleri işlemlerinde hile belirtileri                     | 1-5 yıl         | 17  | 220.94   | 0.934        |
|   |                                                                              | 6-10 yıl        | 32  | 193.20   |              |
|   |                                                                              | 11-15 yıl       | 71  | 204.89   |              |
|   |                                                                              | 16-20 yıl       | 93  | 198.54   |              |
|   |                                                                              | 22 yıl ve üzeri | 188 | 200.27   |              |
| 4 | Bordro düzenleme işlemlerinde hile belirtileri                               | 1-5 yıl         | 17  | 184.91   | 0.471        |
|   |                                                                              | 6-10 yıl        | 32  | 178.44   |              |
|   |                                                                              | 11-15 yıl       | 70  | 195.87   |              |
|   |                                                                              | 16-20 yıl       | 93  | 191.91   |              |
|   |                                                                              | 23 yıl ve üzeri | 186 | 209.62   |              |
| 5 | Çeşitli gider ödemeleri işlemlerinde hile belirtileri                        | 1-5 yıl         | 17  | 202.97   | 0.674        |
|   |                                                                              | 6-10 yıl        | 32  | 205.63   |              |
|   |                                                                              | 11-15 yıl       | 71  | 198.99   |              |
|   |                                                                              | 16-20 yıl       | 92  | 185.22   |              |
|   |                                                                              | 24 yıl ve üzeri | 187 | 206.42   |              |
| 6 | Stoklar ve duran varlıklar işlemlerinde hile belirtileri                     | 1-5 yıl         | 16  | 201.75   | 0.187        |
|   |                                                                              | 6-10 yıl        | 32  | 202.80   |              |
|   |                                                                              | 11-15 yıl       | 71  | 188.30   |              |
|   |                                                                              | 16-20 yıl       | 95  | 179.70   |              |
|   |                                                                              | 25 yıl ve üzeri | 183 | 212.27   |              |

**Tablo 7.20:** Katılımcıların Hile Belirtileri ile Karşılaşma Sıklıkları Açısından Mesleki Tecrübelerine Göre Farklılıkları (Devam).

|    | Hile Belirtileri Görülen İşlemler ve Hile Belirtileri ile Karşılaşma Sıklığı | Mesleki Tecrübe | N   | Ortalama | K-W P değeri |
|----|------------------------------------------------------------------------------|-----------------|-----|----------|--------------|
| 7  | Banka havaleleri işlemlerinde hile belirtileri                               | 1-5 yıl         | 17  | 190.74   | 0.967        |
|    |                                                                              | 6-10 yıl        | 32  | 201.63   |              |
|    |                                                                              | 11-15 yıl       | 70  | 202.11   |              |
|    |                                                                              | 16-20 yıl       | 93  | 193.30   |              |
|    |                                                                              | 26 yıl ve üzeri | 186 | 202.05   |              |
| 8  | Nakit ödemeler/tahsilatlar işlemlerinde hile belirtileri                     | 1-5 yıl         | 17  | 172.03   | 0.496        |
|    |                                                                              | 6-10 yıl        | 32  | 208.16   |              |
|    |                                                                              | 11-15 yıl       | 70  | 192.01   |              |
|    |                                                                              | 16-20 yıl       | 93  | 191.90   |              |
|    |                                                                              | 27 yıl ve üzeri | 188 | 209.19   |              |
| 9  | Envanter ve satın alma işlemlerinde hile belirtileri                         | 1-5 yıl         | 17  | 188.21   | 0.278        |
|    |                                                                              | 6-10 yıl        | 32  | 194.08   |              |
|    |                                                                              | 11-15 yıl       | 71  | 190.25   |              |
|    |                                                                              | 16-20 yıl       | 95  | 186.44   |              |
|    |                                                                              | 28 yıl ve üzeri | 185 | 213.89   |              |
| 10 | Borç ve ödeme işlemlerinde hile belirtileri                                  | 1-5 yıl         | 17  | 198.26   | 0.894        |
|    |                                                                              | 6-10 yıl        | 32  | 202.66   |              |
|    |                                                                              | 11-15 yıl       | 71  | 189.02   |              |
|    |                                                                              | 16-20 yıl       | 93  | 196.75   |              |
|    |                                                                              | 29 yıl ve üzeri | 185 | 204.47   |              |
| 11 | Alacak ve tahsilat işlemlerinde hile belirtileri                             | 1-5 yıl         | 17  | 201.26   | 0.909        |
|    |                                                                              | 6-10 yıl        | 32  | 209.56   |              |
|    |                                                                              | 11-15 yıl       | 71  | 194.56   |              |
|    |                                                                              | 16-20 yıl       | 95  | 195.45   |              |
|    |                                                                              | 30 yıl ve üzeri | 187 | 205.85   |              |
| 12 | Belge ve kayıt düzeninde hile belirtileri                                    | 1-5 yıl         | 17  | 200.03   | 0.916        |
|    |                                                                              | 6-10 yıl        | 32  | 197.00   |              |
|    |                                                                              | 11-15 yıl       | 71  | 195.32   |              |
|    |                                                                              | 16-20 yıl       | 95  | 196.49   |              |
|    |                                                                              | 31 yıl ve üzeri | 187 | 207.29   |              |

### Hipotez 30

**H<sub>0</sub>** : Mali müşavirlerin mükellef sayısı ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin mükellef sayısı ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul'da faaliyet gösteren meslek mensuplarının mükellef sayılarına göre hile belirtileri ile karşılaşma sıklıkları açısından farklılıkları Tablo 7.21'de verilmiştir.

Kruskal-Wallis testi sonuçlarına göre; bordro düzenleme işlemlerinde görülen hile belirtileri dışındaki tüm hile belirtilerinin görülmesine ilişkin ifadelere ait p değerleri 0.05'ten büyüktür. Diğer yandan gruplara ait ortalamalar da p değerini desteklemekte ve bu hile belirtisi dışındaki belirtilere ait grup ortalamaları arasındaki farkların daha düşük olduğu görülmektedir. Tüm hile belirtisi maddeleri birlikte değerlendirildiğinde ise ortalama p değeri (0.058) yine 0.05'ten büyük hesaplanmaktadır. Bu bulgular doğrultusunda; mali müşavirlerin mükellef sayıları ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklıkları arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup, Hipotez 30 reddedilmiştir.

**Tablo 7.21:** Katılımcıların Hile Belirtileri ile Karşılaşma Sıklıkları Açısından Mükellef Sayılarına Göre Farklılıkları.

|   | Hile Belirtileri Görülen İşlemler ve Hile Belirtileri ile Karşılaşma Sıklığı | Mükellef Sayısı | N   | Ortalama | K-W P değeri |
|---|------------------------------------------------------------------------------|-----------------|-----|----------|--------------|
| 1 | Çek düzenleme işlemlerinde hile belirtileri                                  | 1-5             | 94  | 191.21   | 0.591        |
|   |                                                                              | 6-10            | 20  | 199.45   |              |
|   |                                                                              | 11-20           | 45  | 205.02   |              |
|   |                                                                              | 21-30           | 59  | 186.23   |              |
|   |                                                                              | 31 ve üzeri     | 182 | 208.92   |              |
| 2 | Fatura düzenleme işlemlerinde hile belirtileri                               | 1-5             | 96  | 175.63   | 0.052        |
|   |                                                                              | 6-10            | 21  | 233.93   |              |
|   |                                                                              | 11-20           | 45  | 221.21   |              |
|   |                                                                              | 21-30           | 59  | 197.60   |              |
|   |                                                                              | 31 ve üzeri     | 183 | 209.97   |              |
| 3 | Satışlar ve satış iadeleri işlemlerinde hile belirtileri                     | 1-5             | 92  | 185.38   | 0.093        |
|   |                                                                              | 6-10            | 21  | 236.74   |              |
|   |                                                                              | 11-20           | 46  | 229.10   |              |
|   |                                                                              | 21-30           | 59  | 185.87   |              |
|   |                                                                              | 31 ve üzeri     | 183 | 202.57   |              |
| 4 | Bordro düzenleme işlemlerinde hile belirtileri                               | 1-5             | 93  | 175.00   | 0.008*       |
|   |                                                                              | 6-10            | 21  | 256.71   |              |
|   |                                                                              | 11-20           | 45  | 218.38   |              |
|   |                                                                              | 21-30           | 57  | 181.21   |              |
|   |                                                                              | 31 ve üzeri     | 182 | 206.48   |              |
| 5 | Çeşitli gider ödemeleri işlemlerinde hile belirtileri                        | 1-5             | 93  | 188.17   | 0.169        |
|   |                                                                              | 6-10            | 20  | 243.25   |              |
|   |                                                                              | 11-20           | 45  | 208.67   |              |
|   |                                                                              | 21-30           | 59  | 181.07   |              |
|   |                                                                              | 31 ve üzeri     | 182 | 205.29   |              |
| 6 | Stoklar ve duran varlıklar işlemlerinde hile belirtileri                     | 1-5             | 93  | 180.30   | 0.409        |
|   |                                                                              | 6-10            | 21  | 219.52   |              |
|   |                                                                              | 11-20           | 44  | 206.32   |              |
|   |                                                                              | 21-30           | 58  | 198.86   |              |
|   |                                                                              | 31 ve üzeri     | 181 | 204.49   |              |



**Tablo 7.21:** Katılımcıların Hile Belirtileri ile Karşılaşma Sıklıkları Açısından Mükellef Sayılarına Göre Farklılıkları (Devam).

|    | Hile Belirtileri Görülen İşlemler ve Hile Belirtileri ile Karşılaşma Sıklığı | Mükellef Sayısı | N   | Ortalama | K-W P değeri |
|----|------------------------------------------------------------------------------|-----------------|-----|----------|--------------|
| 7  | Banka havaleleri işlemlerinde hile belirtileri                               | 1-5             | 91  | 177.42   | 0.061        |
|    |                                                                              | 6-10            | 21  | 238.50   |              |
|    |                                                                              | 11-20           | 45  | 186.74   |              |
|    |                                                                              | 21-30           | 59  | 195.53   |              |
|    |                                                                              | 31 ve üzeri     | 182 | 210.48   |              |
| 8  | Nakit ödemeler/tahsilatlar işlemlerinde hile belirtileri                     | 1-5             | 93  | 187.32   | 0.544        |
|    |                                                                              | 6-10            | 21  | 221.48   |              |
|    |                                                                              | 11-20           | 46  | 207.86   |              |
|    |                                                                              | 21-30           | 58  | 191.29   |              |
|    |                                                                              | 31 ve üzeri     | 182 | 205.89   |              |
| 9  | Envanter ve satın alma işlemlerinde hile belirtileri                         | 1-5             | 93  | 188.41   | 0.462        |
|    |                                                                              | 6-10            | 21  | 225.88   |              |
|    |                                                                              | 11-20           | 45  | 205.87   |              |
|    |                                                                              | 21-30           | 59  | 187.67   |              |
|    |                                                                              | 31 ve üzeri     | 182 | 206.58   |              |
| 10 | Borç ve ödeme işlemlerinde hile belirtileri                                  | 1-5             | 92  | 182.46   | 0.183        |
|    |                                                                              | 6-10            | 21  | 237.95   |              |
|    |                                                                              | 11-20           | 45  | 201.43   |              |
|    |                                                                              | 21-30           | 59  | 187.90   |              |
|    |                                                                              | 31 ve üzeri     | 181 | 207.00   |              |
| 11 | Alacak ve tahsilat işlemlerinde hile belirtileri                             | 1-5             | 93  | 180.59   | 0.101        |
|    |                                                                              | 6-10            | 21  | 241.69   |              |
|    |                                                                              | 11-20           | 46  | 205.30   |              |
|    |                                                                              | 21-30           | 59  | 190.25   |              |
|    |                                                                              | 31 ve üzeri     | 183 | 210.19   |              |
| 12 | Belge ve kayıt düzeninde hile belirtileri                                    | 1-5             | 94  | 184.95   | 0.077        |
|    |                                                                              | 6-10            | 21  | 248.86   |              |
|    |                                                                              | 11-20           | 46  | 207.25   |              |
|    |                                                                              | 21-30           | 59  | 182.78   |              |
|    |                                                                              | 31 ve üzeri     | 182 | 209.20   |              |

#### 7.4.3.3 Hile araştırmaları hipotezlerinin sonuçları-1

Hile araştırmaları kapsamında gerçekleştirilen ve önceki iki bölümde bulguları açıklanan Mann-Whitney ve Kruskal-Wallis testleri ile test edilen hipotezlere ilişkin sonuçlar aşağıda Tablo 7.22’de özetlenmiştir.

**Tablo 7.22:** Hile Araştırmaları Hipotezleri Sonuç Tablosu-1.

| HİPOTEZLER |                                                                                                                                                            | SONUÇ |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| H25        | Mali müşavirlerin cinsiyeti ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır.                          | KABUL |
| H26        | Mali müşavirlerin eğitim düzeyi ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır.                      | KABUL |
| H27        | Mali müşavirlerin ünvanı ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır.                             | KABUL |
| H28        | Mali müşavirlerin çalışma şekli (bağımlı – bağımsız) ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır. | RED   |
| H29        | Mali müşavirlerin mesleki tecrübesi (çalışma süresi) ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır. | RED   |
| H30        | Mali müşavirlerin mükellef sayısı ile finansal bilgi manipülasyonu göstergeleriyle karşılaşma sıklığı arasında anlamlı bir fark vardır.                    | RED   |

Hipotez Sonuç Tablosu -1’de görüldüğü üzere; hipotezlerin 3’ü reddedilirken, 3’ü kabul edilmiştir. Bu sonuçlara göre; mali müşavirlerin çalışma şekli, mesleki tecrübesi ve mükellef sayısı, finansal bilgi manipülasyonu göstergeleri ile karşılaşma sıklıklarına ilişkin ifadelerinde farklılık yaratmıyor iken; cinsiyet, eğitim düzeyi ve mesleki ünvan özellikleri, ifadelerinde farklılıklar ortaya çıkarmaktadır. Bu değişkenler Tablo 7.23’te verilen grup ortalamaları itibarıyla incelendiğinde ise:

**Tablo 7.23:** Cinsiyet, Ünvan ve Eğitim Düzeyi Gruplarına Göre Farklılık Analizi Sonuçları.

| Hile Belirtileri ile Karşılaşma Sıklığı |               | N   | Grup ortalaması | P değeri |
|-----------------------------------------|---------------|-----|-----------------|----------|
| CİNSİYET                                | Kadın         | 124 | 180.46          | 0.009    |
|                                         | Erkek         | 282 | 213.63          |          |
| ÜNVAN                                   | SMMM          | 372 | 197.88          | 0.001    |
|                                         | YMM           | 34  | 264.97          |          |
| EĞİTİM DÜZEYİ                           | Lise          | 8   | 189.13          | 0.011    |
|                                         | Lisans        | 285 | 197.76          |          |
|                                         | Yüksek lisans | 102 | 208.52          |          |
|                                         | Doktora       | 11  | 316.18          |          |

- a. Cinsiyet özelliğinin grup ortalamalarına göre; erkeklerin (213.63), finansal bilgi manipülasyonlarıyla karşılaşma sıklıklarının kadınlara (180.46) kıyasla daha fazla olduğu görülmektedir. Bu durumun, erkek (282 kişi) mali müşavir meslek mensupları

sayısının kadınlara (124 kişi) göre daha fazla olmasından kaynaklandığı düşünülmektedir.

- b. Eğitim düzeyine göre grup ortalamaları; lise düzeyinde 189.13, lisans düzeyinde 197.76, yüksek lisans düzeyinde 208.52 ve doktora düzeyinde ise 316.18 olarak belirlenmiştir. Bu sonuçlar; finansal bilgi manipülasyonlarıyla en sık karşılaşanların doktora ve yüksek lisans seviyesinde eğitim görenler olduğunu görülmektedir. Bu durumun, eğitim seviyesinin artmasıyla finansal bilgi manipülasyonlarının daha fazla fark edilmesinden kaynaklandığı düşünülmektedir.
- c. Mesleki ünvan özelliğinin grup ortalamalarına göre; YMM'lerin (264.97), finansal bilgi manipülasyonlarıyla karşılaşma sıklıklarının SMMM'lere (197.88) kıyasla daha fazla olduğu görülmektedir. Katılımcı sayıları açısından YMM'lerin (34 kişi), SMMM'lerden (372) daha az olmasına rağmen bu farklılığın YMM ünvanı alabilmek için gerekli olan üst mesleki eğitim ve yetkinliklerden kaynaklandığı düşünülmektedir.

Özetle, araştırma sonucuna göre; finansal bilgi manipülasyonlarının, hileli işlemlerin özel beceri ve eğitim gerektirmesi nedeniyle, akademik ve mesleki eğitim düzeylerinin artmasıyla daha fazla tespit edilebilir olduğuna ilişkin yaygın görüş desteklenmektedir.

#### **7.4.4 Demografik ve Mesleki Özelliklere Göre Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonlarını Önlemedeki Rolüne İlişkin Mali Müşavirlerin Görüşlerine Yönelik Farklılıkların Test Edilmesi ve Sonuçları**

Hile Araştırmaları Ölçeği verilerinin güvenilirliği, yapılan testler sonucunda değerlendirilmiş ve normallik dağılımı kontrol edilmiştir. Ön veri analizi bulgularına göre güvenilirlik koşulları sağlanırken; veri setinin, normal dağılım göstermediği tespit edilmiştir. Bu nedenle blokzincir teknolojisinin finansal bilgi manipülasyonlarını önlemedeki rolüne ilişkin mali müşavirlerin görüşlerine yönelik hipotezler, parametrik olmayan analiz yöntemleri ile test edilmiştir.

Hile Araştırmaları Ölçeği ile İstanbul'da faaliyet gösteren meslek mensuplarının demografik ve mesleki özelliklerine göre blokzincir teknolojisinin finansal bilgi manipülasyonlarını önlemedeki rolüne ilişkin ifadeleri, cinsiyet, eğitim düzeyi, mesleki ünvan, çalışma şekli, mesleki tecrübe, mükellef sayısı ve blokzincir bilgi düzeyi gibi değişkenler açısından

farklılık analizleri ile ölçülmüştür. Bu bağlamda her bir değişken için ayrı ayrı olmak üzere grup sayısına bağlı olarak Mann-Whitney U ve Kruskal-Wallis testleri uygulanarak blokzincir teknolojisinin finansal bilgi manipülasyonlarını önlemedeki rolüne ilişkin görüşler arasında anlamlı bir fark olup olmadığı tespit edilmiştir.

Blokszincir teknolojisinin finansal bilgi manipülasyonlarını önlemedeki rolüne ilişkin görüşlere yönelik demografik ve mesleki farklılıklar ise sırasıyla H31 hipotezi (cinsiyet ile arasında fark vardır), H32 hipotezi (eğitim düzeyi ile arasında fark vardır), H33 hipotezi (mesleki ünvan ile arasında fark vardır), H34 hipotezi (çalışma şekli ile arasında fark vardır), H35 hipotezi (mesleki tecrübe ile arasında fark vardır), H36 hipotezi (mükellef sayısı ile arasında fark vardır) ve H37 hipotezi (blokszincir bilgi düzeyi ile arasında fark vardır) ile ifade edilmektedir.

Buradan hareketle; analiz bulguları, uygulanan analiz yöntemleri itibarıyla sınıflandırılarak ilgili hipotezlere yönelik sonuçların istatistiksel anlamlılıkları tartışılmıştır. İzleyen alt bölümde ise hipotez sonuçlarının özeti sunularak elde edilen bulgular yorumlanmıştır.

#### **7.4.4.1 Mann-Whitney U testine ait bulgular**

Bu çalışmada, blokzincir teknolojisinin finansal bilgi manipülasyonlarını önlemedeki rolüne ilişkin mali müşavirlerin görüşlerine yönelik hipotezlerden H31, H33 ve H34 hipotezleri, iki grup sayısına sahip olmaları nedeniyle Mann-Whitney U testi ile analiz edilmiştir. İlgili hipotezlere dair istatistiksel açıklamalar aşağıda sırasıyla sunulmuştur:

##### ***Hipotez 31***

**H<sub>0</sub> :** Mali müşavirlerin cinsiyeti ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark yoktur.

**H<sub>1</sub> :** Mali müşavirlerin cinsiyeti ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul’da faaliyet gösteren meslek mensuplarının mesleki ünvanlarına göre blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri açısından farklılıkları Tablo 7.24’te verilmiştir. Mann-Whitney U testi sonuçlarına göre; “1-muhasebe bilgilerinin güvenilirliğini olumlu etkiler”, “6-ekonomik sistemi olumlu etkiler” ve “7-kontrol ve denetimi kolaylaştırır” ifadeleri dışındaki tüm ifadelere ait p

değerleri 0.05'ten büyüktür. Diğer yandan gruplara ait ortalamalar da p değerini desteklemekte ve bu üç ifade dışındaki ifadelerle ait grup ortalamaları arasındaki farkların daha düşük olduğu görülmektedir. Tüm hile belirtisi maddeleri birlikte değerlendirildiğinde ise ortalama p değeri (0.174) yine 0.05'ten büyük hesaplanmaktadır. Bu bulgular doğrultusunda; mali müşavirlerin cinsiyeti ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup, Hipotez 31 reddedilmiştir.

**Tablo 7.24:** Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Cinsiyetlerine Göre Farklılıkları.

|    | Blokzincir Teknolojisinin Muhasebe Hilelerini Önlemedeki Rolü                                             | Cinsiyet | N   | Ortalama | M-W P değeri |
|----|-----------------------------------------------------------------------------------------------------------|----------|-----|----------|--------------|
| 1  | Muhasebe bilgi sisteminin blokzincir tabanlı olması muhasebe bilgilerinin güvenilirliğini olumlu etkiler. | Kadın    | 124 | 221.36   | 0.028*       |
|    |                                                                                                           | Erkek    | 282 | 195.65   |              |
| 2  | Blokzincir tabanlı mali denetim vergi mükelleflerinin hileli finansal raporlama eğilimini engeller.       | Kadın    | 124 | 217.89   | 0.068        |
|    |                                                                                                           | Erkek    | 281 | 196.43   |              |
| 3  | Blokzincir tabanlı mali denetim devletin vergi gelirlerini artırır.                                       | Kadın    | 125 | 200.16   | 0.774        |
|    |                                                                                                           | Erkek    | 279 | 203.55   |              |
| 4  | Blokzincir tabanlı mali raporlama finansal sistemin şeffaflığını olumlu etkiler.                          | Kadın    | 125 | 213.32   | 0.247        |
|    |                                                                                                           | Erkek    | 282 | 199.87   |              |
| 5  | Muhasebe bilgi sisteminin blokzincir tabanlı olması finansal bilgilerin mahremiyetini zedeler.            | Kadın    | 124 | 203.00   | 0.905        |
|    |                                                                                                           | Erkek    | 283 | 204.44   |              |
| 6  | Finansal bilgilerin blokzincir üzerinden denetlenmesi ekonomik sistemi olumlu etkiler.                    | Kadın    | 123 | 218.82   | 0.038*       |
|    |                                                                                                           | Erkek    | 280 | 194.61   |              |
| 7  | Blokzincir teknolojisi işlemlerin kontrol ve denetimini yapmayı kolaylaştırır.                            | Kadın    | 124 | 219.19   | 0.044*       |
|    |                                                                                                           | Erkek    | 281 | 195.86   |              |
| 8  | Blokzincir teknolojisi elektronik beyannameleri kolay bir şekilde hazırlama imkânı sunar.                 | Kadın    | 124 | 209.71   | 0.375        |
|    |                                                                                                           | Erkek    | 280 | 199.31   |              |
| 9  | Muhasebe verilerinin güvenliği, kayıt ve dosyalama sisteminin güvencesine bağlıdır.                       | Kadın    | 122 | 215.22   | 0.117        |
|    |                                                                                                           | Erkek    | 282 | 197.00   |              |
| 10 | Muhasebe yazılımlarında geriye dönük işlem yapılmasında sakınca yoktur.                                   | Kadın    | 122 | 190.14   | 0.164        |
|    |                                                                                                           | Erkek    | 281 | 207.15   |              |
| 11 | Blokzincir teknolojisi hileli işlemleri ortaya çıkarabilir.                                               | Kadın    | 124 | 203.28   | 0.978        |
|    |                                                                                                           | Erkek    | 282 | 203.60   |              |

### Hipotez 33

**H<sub>0</sub>** : Mali müşavirlerin ünvanı ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin ünvanı ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.

**Tablo 7.25:** Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Mesleki Ünvanlarına Göre Farklılıkları.

|    | Blokzincir Teknolojisinin Muhasebe Hilelerini Önlemedeki Rolü                                             | Mesleki Ünvan | N   | Ortalama | M-W P değeri |
|----|-----------------------------------------------------------------------------------------------------------|---------------|-----|----------|--------------|
| 1  | Muhasebe bilgi sisteminin blokzincir tabanlı olması muhasebe bilgilerinin güvenilirliğini olumlu etkiler. | SMMM          | 372 | 199.35   | 0.011*       |
|    |                                                                                                           | YMM           | 34  | 248.96   |              |
| 2  | Blokzincir tabanlı mali denetim vergi mükelleflerinin hileli finansal raporlama eğilimini engeller.       | SMMM          | 371 | 201.91   | 0.507        |
|    |                                                                                                           | YMM           | 34  | 214.90   |              |
| 3  | Blokzincir tabanlı mali denetim devletin vergi gelirlerini artırır.                                       | SMMM          | 370 | 199.19   | 0.046*       |
|    |                                                                                                           | YMM           | 34  | 238.50   |              |
| 4  | Blokzincir tabanlı mali raporlama finansal sistemin şeffaflığını olumlu etkiler.                          | SMMM          | 373 | 200.77   | 0.045*       |
|    |                                                                                                           | YMM           | 34  | 239.49   |              |
| 5  | Muhasebe bilgi sisteminin blokzincir tabanlı olması finansal bilgilerin mahremiyetini zedeler.            | SMMM          | 373 | 206.38   | 0.153        |
|    |                                                                                                           | YMM           | 34  | 177.84   |              |
| 6  | Finansal bilgilerin blokzincir üzerinden denetlenmesi ekonomik sistemi olumlu etkiler.                    | SMMM          | 369 | 199.76   | 0.170        |
|    |                                                                                                           | YMM           | 34  | 226.32   |              |
| 7  | Blokzincir teknolojisi işlemlerin kontrol ve denetimini yapmayı kolaylaştırır.                            | SMMM          | 371 | 199.21   | 0.019*       |
|    |                                                                                                           | YMM           | 34  | 244.34   |              |
| 8  | Blokzincir teknolojisi elektronik beyannameleri kolay bir şekilde hazırlama imkânı sunar.                 | SMMM          | 370 | 200.02   | 0.130        |
|    |                                                                                                           | YMM           | 34  | 229.47   |              |
| 9  | Muhasebe verilerinin güvenliği, kayıt ve dosyalama sisteminin güvencesine bağlıdır.                       | SMMM          | 370 | 200.14   | 0.144        |
|    |                                                                                                           | YMM           | 34  | 228.18   |              |
| 10 | Muhasebe yazılımlarında geriye dönük işlem yapılmasında sakınca yoktur.                                   | SMMM          | 369 | 209.20   | 0.000*       |
|    |                                                                                                           | YMM           | 34  | 123.81   |              |
| 11 | Blokzincir teknolojisi hileli işlemleri ortaya çıkarabilir.                                               | SMMM          | 372 | 200.49   | 0.064        |
|    |                                                                                                           | YMM           | 34  | 236.40   |              |

Araştırmaya katılan İstanbul’da faaliyet gösteren meslek mensuplarının mesleki ünvanlarına göre blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri açısından farklılıkları Tablo 7.25’te verilmiştir. Mann-Whitney U testi sonuçlarına göre; “1-muhasebe bilgilerinin güvenilirliğini olumlu etkiler”, “3-devletin vergi gelirlerini artırır”, “4-finance sistemin şeffaflığını olumlu etkiler”, “7-kontrol ve denetimi kolaylaştırır” ve “10-geriye dönük işlem yapılmasında sakınca yoktur” ifadeleri dışındaki tüm ifadelere ait p değerleri 0.05’ten büyüktür. Diğer yandan gruplara ait ortalamalar da p değerini desteklemekte ve bu beş ifade dışındaki ifadelere ait grup ortalamaları arasındaki farkların daha düşük olduğu görülmektedir. Tüm hile belirtisi maddeleri birlikte değerlendirildiğinde ise ortalama p değeri (0.534) yine 0.05’ten büyük hesaplanmaktadır. Bu bulgular doğrultusunda; mali müşavirlerin ünvanı ile blokzincir teknolojisinin finansal

bilgi manipölasyonunu önlemedeki rolüne ilişkin görüşleri arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup, Hipotez 33 reddedilmiştir.

#### **Hipotez 34**

**H<sub>0</sub>** : Mali müşavirlerin çalışma şekli (bağımlı – bağımsız) ile blokzincir teknolojisinin finansal bilgi manipölasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin çalışma şekli (bağımlı – bağımsız) ile blokzincir teknolojisinin finansal bilgi manipölasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.

**Tablo 7.26:** Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipölasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Çalışma Şekillerine Göre Farklılıkları.

|    | <b>Blokzincir Teknolojisinin Muhasebe Hilelerini Önlemedeki Rolü</b>                                      | <b>Çalışma Şekli</b> | <b>N</b> | <b>Ortalama</b> | <b>M-W P değeri</b> |
|----|-----------------------------------------------------------------------------------------------------------|----------------------|----------|-----------------|---------------------|
| 1  | Muhasebe bilgi sisteminin blokzincir tabanlı olması muhasebe bilgilerinin güvenilirliğini olumlu etkiler. | Bağımlı              | 117      | 212.94          | 0.264               |
|    |                                                                                                           | Bağımsız             | 289      | 199.68          |                     |
| 2  | Blokzincir tabanlı mali denetim vergi mükelleflerinin hileli finansal raporlama eğilimini engeller.       | Bağımlı              | 116      | 207.07          | 0.634               |
|    |                                                                                                           | Bağımsız             | 289      | 201.37          |                     |
| 3  | Blokzincir tabanlı mali denetim devletin vergi gelirlerini artırır.                                       | Bağımlı              | 116      | 198.16          | 0.614               |
|    |                                                                                                           | Bağımsız             | 288      | 204.25          |                     |
| 4  | Blokzincir tabanlı mali raporlama finansal sistemin şeffaflığını olumlu etkiler.                          | Bağımlı              | 116      | 209.74          | 0.498               |
|    |                                                                                                           | Bağımsız             | 291      | 201.71          |                     |
| 5  | Muhasebe bilgi sisteminin blokzincir tabanlı olması finansal bilgilerin mahremiyetini zedeler.            | Bağımlı              | 116      | 194.35          | 0.271               |
|    |                                                                                                           | Bağımsız             | 291      | 207.85          |                     |
| 6  | Finansal bilgilerin blokzincir üzerinden denetlenmesi ekonomik sistemi olumlu etkiler.                    | Bağımlı              | 116      | 196.57          | 0.521               |
|    |                                                                                                           | Bağımsız             | 287      | 204.19          |                     |
| 7  | Blokzincir teknolojisi işlemlerin kontrol ve denetimini yapmayı kolaylaştırır.                            | Bağımlı              | 116      | 202.56          | 0.958               |
|    |                                                                                                           | Bağımsız             | 289      | 203.18          |                     |
| 8  | Blokzincir teknolojisi elektronik beyannameleri kolay bir şekilde hazırlama imkânı sunar.                 | Bağımlı              | 115      | 202.03          | 0.956               |
|    |                                                                                                           | Bağımsız             | 289      | 202.69          |                     |
| 9  | Muhasebe verilerinin güvenliği, kayıt ve dosyalama sisteminin güvencesine bağlıdır.                       | Bağımlı              | 115      | 200.27          | 0.792               |
|    |                                                                                                           | Bağımsız             | 289      | 203.39          |                     |
| 10 | Muhasebe yazılımlarında geriye dönük işlem yapılmasında sakınca yoktur.                                   | Bağımlı              | 115      | 190.10          | 0.181               |
|    |                                                                                                           | Bağımsız             | 288      | 206.75          |                     |
| 11 | Blokzincir teknolojisi hileli işlemleri ortaya çıkarabilir.                                               | Bağımlı              | 116      | 196.69          | 0.423               |
|    |                                                                                                           | Bağımsız             | 290      | 206.22          |                     |

Araştırmaya katılan İstanbul’da faaliyet gösteren meslek mensuplarının çalışma şekillerine göre blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri açısından farklılıkları Tablo 7.26’da verilmiştir. Mann-Whitney U testi sonuçlarına göre; tüm ifadeler için p değerleri 0.05’ten büyüktür. Diğer yandan gruplara ait ortalamaların birbirine çok yakın olması da bu sonuçları desteklemektedir. Bu bulgular doğrultusunda; mali müşavirlerin çalışma şekli ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup, Hipotez 34 reddedilmiştir.

#### 7.4.4.2 Kruskal-Wallis testine ait bulgular

Bu çalışmada, blokzincir teknolojisinin finansal bilgi manipülasyonlarını önlemedeki rolüne ilişkin mali müşavirlerin görüşlerine yönelik hipotezlerden H32, H35, H36 ve H37 hipotezleri, iki grup sayısından fazla grup sayısına sahip olmaları nedeniyle Kruskal-Wallis testi ile analiz edilmiştir. İlgili hipotezlere dair istatistiksel açıklamalar aşağıda sırasıyla sunulmuştur:

##### **Hipotez 32**

**H<sub>0</sub>** : Mali müşavirlerin eğitim düzeyi ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin eğitim düzeyi ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır

**Tablo 7.27:** Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Eğitim Düzeylerine Göre Farklılıkları.

|   | Blokzincir Teknolojisinin Muhasebe Hilelerini Önlemedeki Rolü                                             | Eğitim        | N   | Ortalama | K-W P değeri |
|---|-----------------------------------------------------------------------------------------------------------|---------------|-----|----------|--------------|
| 1 | Muhasebe bilgi sisteminin blokzincir tabanlı olması muhasebe bilgilerinin güvenilirliğini olumlu etkiler. | Lise          | 8   | 164.81   | 0.086        |
|   |                                                                                                           | Lisans        | 286 | 199.46   |              |
|   |                                                                                                           | Yüksek Lisans | 101 | 210.20   |              |
|   |                                                                                                           | Doktora       | 11  | 275.09   |              |
| 2 | Blokzincir tabanlı mali denetim vergi mükelleflerinin hileli finansal raporlama eğilimini engeller.       | Lise          | 8   | 169.69   | 0.090        |
|   |                                                                                                           | Lisans        | 285 | 200.75   |              |
|   |                                                                                                           | Yüksek Lisans | 101 | 203.49   |              |
|   |                                                                                                           | Doktora       | 11  | 281.09   |              |
| 3 | Blokzincir tabanlı mali denetim devletin vergi gelirlerini artırır.                                       | Lise          | 8   | 166.50   | 0.026*       |
|   |                                                                                                           | Lisans        | 284 | 200.56   |              |



|   |                                                                                  |               |     |        |        |
|---|----------------------------------------------------------------------------------|---------------|-----|--------|--------|
| 4 | Blokzincir tabanlı mali raporlama finansal sistemin şeffaflığını olumlu etkiler. | Yüksek Lisans | 101 | 200.45 | 0.011* |
|   |                                                                                  | Doktora       | 11  | 297.55 |        |
|   |                                                                                  | Lise          | 7   | 178.36 |        |
|   |                                                                                  | Lisans        | 287 | 195.63 |        |
|   |                                                                                  | Yüksek Lisans | 102 | 220.11 |        |
|   |                                                                                  | Doktora       | 11  | 289.18 |        |

**Tablo 7.27:** Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Eğitim Düzeylerine Göre Farklılıkları (Devam).

|    |                                                                                                |               |     |        |        |
|----|------------------------------------------------------------------------------------------------|---------------|-----|--------|--------|
| 5  | Muhasebe bilgi sisteminin blokzincir tabanlı olması finansal bilgilerin mahremiyetini zedeler. | Lise          | 8   | 240.00 | 0.827  |
|    |                                                                                                | Lisans        | 287 | 202.59 |        |
|    |                                                                                                | Yüksek Lisans | 101 | 205.28 |        |
|    |                                                                                                | Doktora       | 11  | 202.86 |        |
| 6  | Finansal bilgilerin blokzincir üzerinden denetlenmesi ekonomik sistemi olumlu etkiler.         | Lise          | 8   | 173.06 | 0.090  |
|    |                                                                                                | Lisans        | 283 | 196.08 |        |
|    |                                                                                                | Yüksek Lisans | 101 | 213.94 |        |
|    |                                                                                                | Doktora       | 11  | 265.77 |        |
| 7  | Blokzincir teknolojisi işlemlerin kontrol ve denetimini yapmayı kolaylaştırır.                 | Lise          | 8   | 188.25 | 0.009* |
|    |                                                                                                | Lisans        | 284 | 196.32 |        |
|    |                                                                                                | Yüksek Lisans | 102 | 212.00 |        |
|    |                                                                                                | Doktora       | 11  | 302.82 |        |
| 8  | Blokzincir teknolojisi elektronik beyannameleri kolay bir şekilde hazırlama imkânı sunar.      | Lise          | 8   | 142.25 | 0.023* |
|    |                                                                                                | Lisans        | 284 | 196.70 |        |
|    |                                                                                                | Yüksek Lisans | 101 | 215.85 |        |
|    |                                                                                                | Doktora       | 11  | 273.64 |        |
| 9  | Muhasebe verilerinin güvenliği, kayıt ve dosyalama sisteminin güvencesine bağlıdır.            | Lise          | 8   | 178.00 | 0.142  |
|    |                                                                                                | Lisans        | 284 | 198.47 |        |
|    |                                                                                                | Yüksek Lisans | 101 | 208.47 |        |
|    |                                                                                                | Doktora       | 11  | 269.59 |        |
| 10 | Muhasebe yazılımlarında geriye dönük işlem yapılmasında sakınca yoktur.                        | Lise          | 8   | 259.50 | 0.380  |
|    |                                                                                                | Lisans        | 283 | 198.21 |        |
|    |                                                                                                | Yüksek Lisans | 101 | 209.73 |        |
|    |                                                                                                | Doktora       | 11  | 186.77 |        |
| 11 | Blokzincir teknolojisi hileli işlemleri ortaya çıkarabilir.                                    | Lise          | 8   | 239.19 | 0.023* |
|    |                                                                                                | Lisans        | 286 | 194.15 |        |
|    |                                                                                                | Yüksek Lisans | 101 | 219.82 |        |
|    |                                                                                                | Doktora       | 11  | 270.95 |        |

Araştırmaya katılan İstanbul’da faaliyet gösteren meslek mensuplarının eğitim düzeylerine göre blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri açısından farklılıkları Tablo 7.27’de verilmiştir. Kruskal-Wallis testi sonuçlarına göre; ”3-devletin vergi gelirlerini artırır”, “4-finansal sistemin şeffaflığını olumlu etkiler”, “7-denetim yapmayı kolaylaştırır”, “8-elektronik beyannameleri kolay bir şekilde hazırlama

imkânı sunar” ve “11-hileli işlemleri ortaya çıkarabilir” ifadeleri dışındaki tüm ifadelere ait p değerleri 0.05’ten büyüktür. Diğer yandan gruplara ait ortalamalar da p değerini desteklemekte ve bu ifade dışındaki ifadelere ait grup ortalamaları arasındaki farkların daha düşük olduğu görülmektedir. Tüm hile belirtisi maddeleri birlikte değerlendirildiğinde ise ortalama p değeri (0.082) yine 0.05’ten büyük hesaplanmaktadır. Bu bulgular doğrultusunda; mali müşavirlerin eğitim düzeyi ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup, Hipotez 32 reddedilmiştir.

### **Hipotez 35**

**H<sub>0</sub>** : Mali müşavirlerin mesleki tecrübesi (çalışma süresi) ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin mesleki tecrübesi (çalışma süresi) ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.

**Tablo 7.28:** Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Mesleki Tecrübelerine Göre Farklılıkları.

|   | <b>Blokzincir Teknolojisinin Muhasebe Hilelerini Önlemedeki Rolü</b>                                      | <b>Mesleki Tecrübe</b>                                           | <b>N</b>                    | <b>Ortalama</b>                                | <b>K-W P değeri</b> |
|---|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|-----------------------------|------------------------------------------------|---------------------|
| 1 | Muhasebe bilgi sisteminin blokzincir tabanlı olması muhasebe bilgilerinin güvenilirliğini olumlu etkiler. | 1-5 yıl<br>6-10 yıl<br>11-15 yıl<br>16-20 yıl<br>21 yıl ve üzeri | 17<br>32<br>71<br>96<br>190 | 176.88<br>196.13<br>215.41<br>193.61<br>207.67 | 0.540               |
| 2 | Blokzincir tabanlı mali denetim vergi mükelleflerinin hileli finansal raporlama eğilimini engeller.       | 1-5 yıl<br>6-10 yıl<br>11-15 yıl<br>16-20 yıl<br>21 yıl ve üzeri | 17<br>32<br>71<br>96<br>189 | 211.35<br>207.38<br>208.47<br>195.39<br>203.32 | 0.939               |
| 3 | Blokzincir tabanlı mali denetim devletin vergi gelirlerini artırır.                                       | 1-5 yıl<br>6-10 yıl<br>11-15 yıl<br>16-20 yıl<br>22 yıl ve üzeri | 17<br>32<br>71<br>94<br>190 | 231.53<br>223.08<br>184.61<br>187.61<br>210.49 | 0.140               |
| 4 | Blokzincir tabanlı mali raporlama finansal sistemin şeffaflığını olumlu etkiler.                          | 1-5 yıl<br>6-10 yıl<br>11-15 yıl<br>16-20 yıl                    | 17<br>32<br>71<br>96        | 244.65<br>181.02<br>203.42<br>191.14           | 0.199               |

|   |                                                                                                |                 |     |        |       |
|---|------------------------------------------------------------------------------------------------|-----------------|-----|--------|-------|
|   |                                                                                                | 23 yıl ve üzeri | 191 | 210.92 |       |
| 5 | Muhasebe bilgi sisteminin blokzincir tabanlı olması finansal bilgilerin mahremiyetini zedeler. | 1-5 yıl         | 17  | 248.09 | 0.190 |
|   |                                                                                                | 6-10 yıl        | 32  | 228.00 |       |
|   |                                                                                                | 11-15 yıl       | 71  | 185.40 |       |
|   |                                                                                                | 16-20 yıl       | 96  | 204.38 |       |
|   |                                                                                                | 24 yıl ve üzeri | 191 | 202.78 |       |

**Tablo 7.28:** Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Mesleki Tecrübelerine Göre Farklılıkları (Devam).

|    |                                                                                           |                 |     |        |        |
|----|-------------------------------------------------------------------------------------------|-----------------|-----|--------|--------|
| 6  | Finansal bilgilerin blokzincir üzerinden denetlenmesi ekonomik sistemi olumlu etkiler.    | 1-5 yıl         | 17  | 239.26 | 0.311  |
|    |                                                                                           | 6-10 yıl        | 32  | 193.06 |        |
|    |                                                                                           | 11-15 yıl       | 69  | 206.04 |        |
|    |                                                                                           | 16-20 yıl       | 96  | 186.17 |        |
|    |                                                                                           | 25 yıl ve üzeri | 189 | 206.73 |        |
| 7  | Blokzincir teknolojisi işlemlerin kontrol ve denetimini yapmayı kolaylaştırır.            | 1-5 yıl         | 17  | 223.03 | 0.604  |
|    |                                                                                           | 6-10 yıl        | 30  | 197.23 |        |
|    |                                                                                           | 11-15 yıl       | 71  | 212.80 |        |
|    |                                                                                           | 16-20 yıl       | 96  | 190.10 |        |
|    |                                                                                           | 26 yıl ve üzeri | 191 | 204.97 |        |
| 8  | Blokzincir teknolojisi elektronik beyannameleri kolay bir şekilde hazırlama imkânı sunar. | 1-5 yıl         | 17  | 236.00 | 0.126  |
|    |                                                                                           | 6-10 yıl        | 31  | 209.65 |        |
|    |                                                                                           | 11-15 yıl       | 71  | 212.27 |        |
|    |                                                                                           | 16-20 yıl       | 94  | 178.48 |        |
|    |                                                                                           | 27 yıl ve üzeri | 191 | 206.54 |        |
| 9  | Muhasebe verilerinin güvenliği, kayıt ve dosyalama sisteminin güvencesine bağlıdır.       | 1-5 yıl         | 17  | 216.59 | 0.832  |
|    |                                                                                           | 6-10 yıl        | 30  | 216.40 |        |
|    |                                                                                           | 11-15 yıl       | 71  | 200.70 |        |
|    |                                                                                           | 16-20 yıl       | 94  | 193.85 |        |
|    |                                                                                           | 28 yıl ve üzeri | 192 | 203.98 |        |
| 10 | Muhasebe yazılımlarında geriye dönük işlem yapılmasında sakınca yoktur.                   | 1-5 yıl         | 17  | 272.79 | 0.011* |
|    |                                                                                           | 6-10 yıl        | 30  | 247.55 |        |
|    |                                                                                           | 11-15 yıl       | 71  | 196.55 |        |
|    |                                                                                           | 16-20 yıl       | 95  | 194.04 |        |
|    |                                                                                           | 29 yıl ve üzeri | 190 | 194.49 |        |
| 11 | Blokzincir teknolojisi hileli işlemleri ortaya çıkarabilir.                               | 1-5 yıl         | 17  | 244.65 | 0.199  |
|    |                                                                                           | 6-10 yıl        | 31  | 224.85 |        |
|    |                                                                                           | 11-15 yıl       | 71  | 203.41 |        |
|    |                                                                                           | 16-20 yıl       | 95  | 186.57 |        |
|    |                                                                                           | 30 yıl ve üzeri | 192 | 204.82 |        |

Araştırmaya katılan İstanbul’da faaliyet gösteren meslek mensuplarının mesleki tecrübelerine göre blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri açısından farklılıkları Tablo 7.28’de verilmiştir. Kruskal-Wallis testi sonuçlarına göre; ”10-geriye dönük işlem yapılmasında sakınca yoktur” ifadesi dışındaki tüm ifadelerle ait p değerleri 0.05’ten büyüktür. Diğer yandan gruplara ait ortalamalar da p

değerini desteklemekte ve bu ifade dışındaki ifadelere ait grup ortalamaları arasındaki farkların daha düşük olduğu görülmektedir. Tüm hile belirtisi maddeleri birlikte değerlendirildiğinde ise ortalama p değeri (0.438) yine 0.05'ten büyük hesaplanmaktadır. Bu bulgular doğrultusunda; mali müşavirlerin çalışma şekli ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup, Hipotez 35 reddedilmiştir.

### **Hipotez 36**

**H<sub>0</sub>** : Mali müşavirlerin mükellef sayısı ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin mükellef sayısı ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul'da faaliyet gösteren meslek mensuplarının mükellef sayılarına göre blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri açısından farklılıkları Tablo 7.29'da verilmiştir. Kruskal-Wallis testi sonuçlarına göre; tüm ifadelere ait p değerleri 0.05'ten büyüktür. Diğer yandan gruplara ait ortalamalar da p değerini desteklemekte ve grup ortalamaları arasındaki farkların düşük olduğu görülmektedir. Bu bulgular doğrultusunda; mali müşavirlerin mükellef sayıları ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında istatistiksel olarak anlamlı bir farklılık tespit edilememiş olup, Hipotez 36 reddedilmiştir.

**Tablo 7.29:** Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Mükellef Sayılarına Göre Farklılıkları.

|          | <b>Blokzincir Teknolojisinin Muhasebe Hilelerini Önlemedeki Rolü</b>                                      | <b>Mükellef Sayısı</b> | <b>N</b> | <b>Ortalama</b> | <b>K-W P değeri</b> |
|----------|-----------------------------------------------------------------------------------------------------------|------------------------|----------|-----------------|---------------------|
| <b>1</b> | Muhasebe bilgi sisteminin blokzincir tabanlı olması muhasebe bilgilerinin güvenilirliğini olumlu etkiler. | 1-5                    | 98       | 214.31          | 0.522               |
|          |                                                                                                           | 6-10                   | 21       | 200.81          |                     |
|          |                                                                                                           | 11-20                  | 45       | 213.96          |                     |
|          |                                                                                                           | 21-30                  | 59       | 184.86          |                     |
|          |                                                                                                           | 31 ve üzeri            | 183      | 201.46          |                     |
| <b>2</b> | Blokzincir tabanlı mali denetim vergi mükelleflerinin hileli finansal raporlama eğilimini engeller.       | 1-5                    | 98       | 208.91          | 0.969               |
|          |                                                                                                           | 6-10                   | 21       | 199.81          |                     |
|          |                                                                                                           | 11-20                  | 46       | 202.95          |                     |
|          |                                                                                                           | 21-30                  | 58       | 205.74          |                     |
|          |                                                                                                           | 31 ve üzeri            | 182      | 199.33          |                     |
| <b>3</b> | Blokzincir tabanlı mali denetim devletin vergi gelirlerini artırır.                                       | 1-5                    | 97       | 200.43          | 0.998               |
|          |                                                                                                           | 6-10                   | 21       | 202.50          |                     |
|          |                                                                                                           | 11-20                  | 46       | 207.29          |                     |
|          |                                                                                                           | 21-30                  | 59       | 203.67          |                     |

|                                                                                  |             |     |        |       |
|----------------------------------------------------------------------------------|-------------|-----|--------|-------|
|                                                                                  | 31 ve üzeri | 181 | 202.01 |       |
| Blokzincir tabanlı mali raporlama finansal sistemin şeffaflığını olumlu etkiler. | 1-5         | 98  | 208.04 | 0.971 |
|                                                                                  | 6-10        | 21  | 212.00 |       |
|                                                                                  | 11-20       | 46  | 199.93 |       |
|                                                                                  | 21-30       | 59  | 197.56 |       |
|                                                                                  | 31 ve üzeri | 183 | 204.02 |       |

**Tablo 7.29:** Katılımcıların Blokszincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Mükellef Sayılarına Göre Farklılıkları (Devam).

|    | Blokszincir Teknolojisinin Muhasebe Hilelerini Önlemedeki Rolü                                  | Mükellef Sayısı | N   | Ortalama | K-W P değeri |
|----|-------------------------------------------------------------------------------------------------|-----------------|-----|----------|--------------|
| 5  | Muhasebe bilgi sisteminin blokszincir tabanlı olması finansal bilgilerin mahremiyetini zedeler. | 1-5             | 97  | 196.92   | 0.436        |
|    |                                                                                                 | 6-10            | 21  | 219.90   |              |
|    |                                                                                                 | 11-20           | 46  | 183.75   |              |
|    |                                                                                                 | 21-30           | 59  | 197.25   |              |
|    |                                                                                                 | 31 ve üzeri     | 184 | 213.14   |              |
| 6  | Finansal bilgilerin blokszincir üzerinden denetlenmesi ekonomik sistemi olumlu etkiler.         | 1-5             | 97  | 194.56   | 0.915        |
|    |                                                                                                 | 6-10            | 21  | 213.21   |              |
|    |                                                                                                 | 11-20           | 46  | 209.42   |              |
|    |                                                                                                 | 21-30           | 59  | 199.82   |              |
|    |                                                                                                 | 31 ve üzeri     | 180 | 203.52   |              |
| 7  | Blokszincir teknolojisi işlemlerin kontrol ve denetimini yapmayı kolaylaştırır.                 | 1-5             | 97  | 197.62   | 0.949        |
|    |                                                                                                 | 6-10            | 21  | 205.90   |              |
|    |                                                                                                 | 11-20           | 46  | 213.50   |              |
|    |                                                                                                 | 21-30           | 59  | 204.63   |              |
|    |                                                                                                 | 31 ve üzeri     | 182 | 202.35   |              |
| 8  | Blokszincir teknolojisi elektronik beyannameleri kolay bir şekilde hazırlama imkânı sunar.      | 1-5             | 96  | 205.58   | 0.722        |
|    |                                                                                                 | 6-10            | 21  | 195.71   |              |
|    |                                                                                                 | 11-20           | 45  | 183.36   |              |
|    |                                                                                                 | 21-30           | 59  | 198.21   |              |
|    |                                                                                                 | 31 ve üzeri     | 183 | 207.75   |              |
| 9  | Muhasebe verilerinin güvenliği, kayıt ve dosyalama sisteminin güvencesine bağlıdır.             | 1-5             | 96  | 195.56   | 0.392        |
|    |                                                                                                 | 6-10            | 21  | 219.90   |              |
|    |                                                                                                 | 11-20           | 45  | 198.61   |              |
|    |                                                                                                 | 21-30           | 59  | 183.42   |              |
|    |                                                                                                 | 31 ve üzeri     | 183 | 211.25   |              |
| 10 | Muhasebe yazılımlarında geriye dönük işlem yapılmasında sakınca yoktur.                         | 1-5             | 96  | 185.74   | 0.439        |
|    |                                                                                                 | 6-10            | 21  | 210.86   |              |
|    |                                                                                                 | 11-20           | 45  | 192.06   |              |
|    |                                                                                                 | 21-30           | 59  | 203.87   |              |
|    |                                                                                                 | 31 ve üzeri     | 182 | 211.41   |              |
| 11 | Blokszincir teknolojisi hileli işlemleri ortaya çıkarabilir.                                    | 1-5             | 97  | 193.59   | 0.784        |
|    |                                                                                                 | 6-10            | 21  | 223.40   |              |
|    |                                                                                                 | 11-20           | 45  | 209.22   |              |
|    |                                                                                                 | 21-30           | 59  | 207.77   |              |
|    |                                                                                                 | 31 ve üzeri     | 184 | 203.68   |              |

### Hipotez 37

**H<sub>0</sub>** : Mali müşavirlerin blokzincir bilgi düzeyi ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark yoktur.

**H<sub>1</sub>**: Mali müşavirlerin blokzincir bilgi düzeyi ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.

Araştırmaya katılan İstanbul’da faaliyet gösteren meslek mensuplarının blokzincir bilgi düzeylerine göre blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri açısından farklılıkları Tablo 7.30’da verilmiştir. Kruskal-Wallis testi sonuçlarına göre; “5-finance bilgilerin mahremiyetini zedeler” ve “10-geriye dönük işlem yapılmasında sakınca yoktur” ifadeleri dışındaki tüm ifadeler için p değerleri 0.05’ten küçüktür. Diğer yandan gruplara ait ortalamalar da p değerini desteklemekte ve grup ortalamaları arasındaki farkların büyük olduğu görülmektedir. Tüm ifadeler birlikte değerlendirildiğinde ise ortalama p değeri (0.044), yine 0.05’ten küçük hesaplanmaktadır. Bu bulgular doğrultusunda; mali müşavirlerin blokzincir bilgi düzeyi ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında istatistiksel olarak anlamlı bir farklılık tespit edilmiş olup, Hipotez 37 kabul edilmiştir.

**Tablo 7.30:** Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Blokzincir Bilgi Düzeylerine Göre Farklılıkları.

|   | Blokzincir Teknolojisinin Muhasebe Hilelerini Önlemedeki Rolü                                             | Blokzincir Bilgi Düzeyi | N   | Ortalama | K-W P değeri |
|---|-----------------------------------------------------------------------------------------------------------|-------------------------|-----|----------|--------------|
| 1 | Muhasebe bilgi sisteminin blokzincir tabanlı olması muhasebe bilgilerinin güvenilirliğini olumlu etkiler. | Bilgim yok              | 117 | 170.95   | 0.000        |
|   |                                                                                                           | Çok az                  | 102 | 200.80   |              |
|   |                                                                                                           | Orta                    | 131 | 220.65   |              |
|   |                                                                                                           | İyi                     | 49  | 229.43   |              |
|   |                                                                                                           | İleri                   | 7   | 284.50   |              |
| 2 | Blokzincir tabanlı mali denetim vergi mükelleflerinin hileli finansal raporlama eğilimini engeller.       | Bilgim yok              | 117 | 186.65   | 0.012        |
|   |                                                                                                           | Çok az                  | 100 | 186.27   |              |
|   |                                                                                                           | Orta                    | 132 | 218.99   |              |
|   |                                                                                                           | İyi                     | 49  | 222.09   |              |
|   |                                                                                                           | İleri                   | 7   | 280.07   |              |
| 3 | Blokzincir tabanlı mali denetim devletin vergi gelirlerini artırır.                                       | Bilgim yok              | 116 | 171.34   | 0.000        |
|   |                                                                                                           | Çok az                  | 101 | 201.40   |              |
|   |                                                                                                           | Orta                    | 132 | 217.28   |              |
|   |                                                                                                           | İyi                     | 48  | 223.47   |              |
|   |                                                                                                           | İleri                   | 7   | 312.21   |              |
| 4 | Blokzincir tabanlı mali raporlama finansal sistemin şeffaflığını olumlu etkiler.                          | Bilgim yok              | 116 | 176.51   | 0.001        |
|   |                                                                                                           | Çok az                  | 103 | 203.06   |              |
|   |                                                                                                           | Orta                    | 132 | 215.02   |              |
|   |                                                                                                           | İyi                     | 49  | 224.88   |              |
|   |                                                                                                           | İleri                   | 7   | 319.36   |              |

|   |                                                                                                |            |     |        |        |
|---|------------------------------------------------------------------------------------------------|------------|-----|--------|--------|
| 5 | Muhasebe bilgi sisteminin blokzincir tabanlı olması finansal bilgilerin mahremiyetini zedeler. | Bilgim yok | 116 | 221.10 | 0.279* |
|   |                                                                                                | Çok az     | 103 | 203.71 |        |
|   |                                                                                                | Orta       | 132 | 189.72 |        |
|   |                                                                                                | İyi        | 49  | 205.23 |        |
|   |                                                                                                | İleri      | 7   | 185.43 |        |
| 6 | Finansal bilgilerin blokzincir üzerinden denetlenmesi ekonomik sistemi olumlu etkiler.         | Bilgim yok | 116 | 177.39 | 0.048  |
|   |                                                                                                | Çok az     | 101 | 203.01 |        |
|   |                                                                                                | Orta       | 130 | 216.61 |        |
|   |                                                                                                | İyi        | 49  | 216.42 |        |
|   |                                                                                                | İleri      | 7   | 223.00 |        |

**Tablo 7.30:** Katılımcıların Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu Önlemedeki Rolüne İlişkin İfadeleri Açısından Blokzincir Bilgi Düzeylerine Göre Farklılıkları (Devam).

|    | Blokzincir Teknolojisinin Muhasebe Hilelerini Önlemedeki Rolü                             | Blokzincir Bilgi Düzeyi | N   | Ortalama | K-W P değeri |
|----|-------------------------------------------------------------------------------------------|-------------------------|-----|----------|--------------|
| 7  | Blokzincir teknolojisi işlemlerin kontrol ve denetimini yapmayı kolaylaştırır.            | Bilgim yok              | 117 | 177.91   | 0.005        |
|    |                                                                                           | Çok az                  | 101 | 197.84   |              |
|    |                                                                                           | Orta                    | 131 | 216.14   |              |
|    |                                                                                           | İyi                     | 49  | 240.91   |              |
|    |                                                                                           | İleri                   | 7   | 185.50   |              |
| 8  | Blokzincir teknolojisi elektronik beyannameleri kolay bir şekilde hazırlama imkânı sunar. | Bilgim yok              | 117 | 177.41   | 0.027        |
|    |                                                                                           | Çok az                  | 102 | 203.18   |              |
|    |                                                                                           | Orta                    | 129 | 213.30   |              |
|    |                                                                                           | İyi                     | 49  | 230.74   |              |
|    |                                                                                           | İleri                   | 7   | 215.14   |              |
| 9  | Muhasebe verilerinin güvenliği, kayıt ve dosyalama sisteminin güvencesine bağlıdır.       | Bilgim yok              | 116 | 175.24   | 0.010        |
|    |                                                                                           | Çok az                  | 102 | 203.34   |              |
|    |                                                                                           | Orta                    | 130 | 213.08   |              |
|    |                                                                                           | İyi                     | 49  | 231.56   |              |
|    |                                                                                           | İleri                   | 7   | 242.00   |              |
| 10 | Muhasebe yazılımlarında geriye dönük işlem yapılmasında sakınca yoktur.                   | Bilgim yok              | 117 | 215.93   | 0.498*       |
|    |                                                                                           | Çok az                  | 101 | 188.14   |              |
|    |                                                                                           | Orta                    | 129 | 201.52   |              |
|    |                                                                                           | İyi                     | 49  | 199.73   |              |
|    |                                                                                           | İleri                   | 7   | 193.86   |              |
| 11 | Blokzincir teknolojisi hileli işlemleri ortaya çıkarabilir.                               | Bilgim yok              | 117 | 177.65   | 0.007        |
|    |                                                                                           | Çok az                  | 103 | 196.45   |              |
|    |                                                                                           | Orta                    | 130 | 220.51   |              |
|    |                                                                                           | İyi                     | 49  | 229.93   |              |
|    |                                                                                           | İleri                   | 7   | 238.50   |              |

#### 7.4.4.3 Hile araştırmaları hipotezlerinin sonuçları-2

Hile araştırmaları kapsamında gerçekleştirilen ve önceki iki bölümde bulguları açıklanan Mann-Whitney ve Kruskal-Wallis testleri ile test edilen hipotezlere ilişkin sonuçlar Tablo 7.31’de özetlenmiştir.

Hipotez Sonuç Tablosu-2’de görüldüğü üzere; hipotezlerin 6’sı reddedilirken, 1’i kabul edilmiştir. Bu sonuçlara göre; meslek mensuplarının herhangi bir demografik ve mesleki özellikleri blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşlerine ilişkin ifadelerinde farklılık yaratmıyor iken; blokzincir teknolojisi hakkındaki bilgi düzeyleri, ifadelerinde farklılıklar ortaya çıkarmaktadır. Bilgi düzeylerine ilişkin farklılıklar incelendiğinde ise blokzincir teknolojisi hakkında bilgi düzeyi arttıkça, bu teknolojinin finansal bilgi manipülasyonlarını önlemede bir araç olarak kullanılabileceğine ilişkin görüşün hâkim olduğu görülmektedir.

**Tablo 7.31:** Hile Araştırmaları Hipotezleri Sonuç Tablosu-2.

| HİPOTEZLER |                                                                                                                                                                                         | SONUÇ        |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <b>H31</b> | Mali müşavirlerin cinsiyeti ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.                          | <b>RED</b>   |
| <b>H32</b> | Mali müşavirlerin eğitim düzeyi ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.                      | <b>RED</b>   |
| <b>H33</b> | Mali müşavirlerin ünvanı ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.                             | <b>RED</b>   |
| <b>H34</b> | Mali müşavirlerin çalışma şekli (bağımlı – bağımsız) ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır. | <b>RED</b>   |
| <b>H35</b> | Mali müşavirlerin mesleki tecrübesi (çalışma süresi) ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır. | <b>RED</b>   |
| <b>H36</b> | Mali müşavirlerin mükellef sayısı ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.                    | <b>RED</b>   |
| <b>H37</b> | Mali müşavirlerin blokzincir bilgi düzeyi ile blokzincir teknolojisinin finansal bilgi manipülasyonunu önlemedeki rolüne ilişkin görüşleri arasında anlamlı bir fark vardır.            | <b>KABUL</b> |



## 8. SONUÇ VE ÖNERİLER

Blokzincir teknolojisinin sunduğu merkeziyetsiz, güvenilir ve kendi kendine yeten otonom sistem, nesnelerin/endüstriyel interneti (IoT/IIoT), yapay zekâ (AI) gibi Endüstri 4.0 bileşenleri ve Web 3.0 teknolojilerinin birleşimiyle akıllı toplum yaratılmasına yönelik çözümler vadetmektedir. Bu yenilikçi ekosistem, sadece teknoloji dünyasında değil, iş dünyasında dolayısıyla muhasebe ve denetim süreçlerinde de devrim niteliğinde bir dönüşümü tetiklemektedir.

Blokzincir teknolojisinin merkeziyetsiz yapısı sayesinde, muhasebe verileri tek bir noktada değil, dağıtık bir ağda saklanmakta ve kriptografi teknikleri ile şifrelenmiş zincir yapısı ve mutabakat mekanizmaları sayesinde ise finansal işlemler, kurcalamaya dayanıklı ve değiştirilemez bir şekilde kaydedilmektedir. Bu durum; muhasebe bilgi kalitesini artırmakla birlikte, aynı zamanda mutabakat ihtiyacını da ortadan kaldırarak, muhasebe kayıt sisteminin, yüzyıllardır uygulanan “Çift Taraflı Kayıt Sistemi”nden, “Üç Taraflı Kayıt Sistemi”ne geliştirilmesi şeklinde bir dönüşüm potansiyeli de yaratmaktadır.

Ayrıca verilerin zaman damgalı ve dijital imzalı olarak hash fonksiyonları ile birbirine bağlanarak zincire kaydedilmesi sayesinde de her bir işlem kaydının geçmişi ile izlenebilmesi sağlanmaktadır. Böylece tüm işlemlerin denetlenebilirliğini, otomatik doğrulanabilir kanıt üretilmesini, gerçek zamanlı sürekli denetim yapılabilmesini, denetim risklerinin azaltılmasını, tasdik hizmetlerinin kolaylaştırılmasını ve otomatik vergi denetimini mümkün kılarak denetim sürecinde etkinlik ve verimlilik artışı ile zaman ve maliyet tasarrufu elde edilmesine olanak yaratmaktadır.

Diğer yandan akıllı sözleşmeler ile birlikte muhasebe kayıt süreci ve finansal tablo sunumu otomatikleştirilmekte, bu sayede insan hataları ve manipülasyon fırsatları azaltılarak muhasebe bilgi kullanıcılarına, yöneticilerin takdir yetkilerinden arındırılmış, gerçek zamanlı, güvenilir ve karşılaştırılabilir finansal bilgi sağlanabilmektedir.

Dolayısıyla blokzincir teknolojisinin sağladığı merkeziyetsizlik, şeffaflık, izlenebilirlik, değişmezlik, kurcalamaya dayanıklılık, güvenilirlik, denetlenebilirlik, inkâr edilemezlik ve otomasyon özellikleri, finansal kayıtların güvenilirliğini artırarak manipülasyon risklerini minimize etme potansiyeli ile dikkat çekmektedir. Bu kapsamda muhasebe bilgi kalitesini artırma, hatalı işlemleri azaltma, hileli işlemleri kolaylıkla tespit etme, belge dolandırıcılığını

engelleme, varlıkların kötüye kullanımını azaltma, ilişkili taraf işlemlerini tespit etme, bilgi asimetrisini azaltma, kazanç yönetimini azaltma ve yasa dışı ve etik dışı faaliyetleri engelleme gibi avantajlar sunmaktadır. Bununla birlikte işlem kaynağının gerçekliği, akıllı sözleşmelerin hatalı kodlanması, işletme varlıklarının kaybedilmesi, işletme mahremiyetinin tehlikeye girmesi, güvenlik ihlali ve anonimlik özelliğinin yarattığı yasa dışı işlem risklerini de bünyesinde barındırmaktadır.

Bu çerçevede blokzincir teknolojisine geçişin muhasebe ve denetim sektörüne olası etkileri değerlendirildiğinde; işletmeler üzerinde denetim verimliliğini artırma, operasyonel sadeleşme, tedarik zincirinde güven artışı sağlama ve hisse senedi fiyatları, borçlanma oranları ve diğer finansal göstergeleri iyileştirme gibi olumlu etkilerin yanı sıra büyük veri dolayısıyla artan maliyetler, bilgi ifşası ve mülkiyet riski, güvenlik ihlali riski ve geleneksel sistemler ile entegrasyon sorunları gibi olumsuz etkilerin gerçekleşmesi muhtemeldir.

Kamu üzerine etkileri incelendiğinde; düzenleyicilerin detaylı gözetim yapmasını ve etkin karar almasını sağlama, vergi tahsilatını hızlı, doğru ve düşük maliyetle gerçekleştirebilme, vergi kaçırma ve kayıt dışı ekonomiyi ortadan kaldırma, finansal piyasalarda güven ve istikrarı sağlama gibi olumlu etkilerinin gerçekleşmesi beklenmektedir. Bununla birlikte blokzincir teknolojisinin etkin bir şekilde uygulanabilmesi için, farklı ülkelerdeki yasal düzenlemelerin uyumlaştırılması ve vergi sistemlerinde gerekli dönüşümlerin gerçekleştirilmesi için uluslararası iş birliklerinin ve anlaşmaların sağlanması gerekmektedir.

Meslek mensupları üzerine blokzincir teknolojisinin etkilerine baktığımızda ise muhasebe ve denetim süreçlerinde sağlanan otomasyon ile işlemlerin gerçekliğini tespit etme ve daha değerli faaliyetlere odaklanma gibi meslek mensuplarının rollerinde dönüşüm gerçekleşecektir. Ayrıca meslek profesyonellerinin bağımsızlıkları korunarak meslek etiğine aykırı davranışlara zorlanmaları da engellenecektir. Ancak blokzincirin yeni ve karmaşık bir teknoloji olması, yetkin personel ihtiyacını doğuracak ve dönüşen mesleki yetkinlikler dolayısıyla yeni teknolojiye adaptasyon sağlayamayan meslek mensuplarının, iş piyasasında rekabet avantajını kaybederek istihdamları üzerinde olumsuz sonuçlara da yol açabilecektir.

Sonuç olarak blokzincir teknolojisi henüz gelişim aşamasında olduğundan aşılması gereken teknik, düzenleyici ve operasyonel zorluklar bulunmaktadır. Teknoloji olgunlaştıkça bu

zorlukların aşılması ve finansal bilgi manipölasyonlarına yönelik olası risk ve tehditlerin bertaraf edilmesi mümkündür. Bu bağlamda söz konusu çalışmada, blokzincir teknolojisinin, finansal bilgi manipölasyonlarını azaltmada kullanılabilecek etkili bir alternatif araç olarak değerlendirilmesi önerilmektedir. Nitekim literatürde de teorik açıdan çoğunluk görüşü bu yönde destekleyicidir. Bununla birlikte blokzincir teknolojisinin muhasebe ve denetim süreçlerinde kullanılmasına ilişkin teknik ve teknolojik uygulanabilirliğin sağlanması için çeşitli özel sektör ve denetim firmaları girişimleri de mevcuttur.

Dolayısıyla muhasebe ve denetim süreçlerinde yeni bir yaklaşım olarak blokzincir teknolojisinin benimsenme düzeyinin belirlenmesi ve sektör uygulayıcılarının ilgili teknolojiye ne kadar hazırlıklı olduklarının değerlendirilmesi büyük önem taşımaktadır. Bu bakış açısından hareketle çalışmada, muhasebe ve denetim sürecini yönetmede aktif rol oynayan mali müşavirlerin blokzincir teknolojisini benimseme düzeyleri, Teknoloji Kabul Modeli kullanılarak araştırılmıştır. Ek olarak da mali müşavirlerin muhasebe hileleri ile karşılaşma sıklıkları ve blokzincir teknolojisinin muhasebe hilelerini önlemedeki rolüne ilişkin görüşleri incelenmiştir.

Bu kapsamda İstanbul ilindeki SMMM ve YMM Odaları'na kayıtlı toplamda 408 meslek mensubunun blokzincir teknolojisine yönelik algıladıkları engeller, fayda ve kullanım kolaylığı ile kullanıma yönelik tutum, niyet ve gerçekleşen davranışlarının etkileri ölçülmüştür. Araştırma çerçevesinde elde edilen sonuçlar, önce demografik, mesleki özellikler ve teknolojik ürün kullanım sıklığı itibarıyla ardından TKM modeli itibarıyla ve son olarak hile araştırmaları kapsamında aşağıda özetlenmiştir:

Araştırmaya katılan mali müşavirlerinin demografik özellikleri itibarıyla; çoğunluğunun erkek (%69,4) ve lisans (70.3) düzeyinde eğitim seviyesine sahip olduğu görülmektedir. Mesleki özellikleri itibarıyla da çoğunluğunun, SMMM (%91,7) ünvanına sahip oldukları, bağımsız olarak (%71,3) kendi ofislerinde faaliyette bulundukları, 21 yıldan fazla (%47,1) mesleki tecrübeye ve 31'den fazla (%45,1) mükellef sayısına sahip oldukları tespit edilmiştir. Blokzincir teknolojisi hakkındaki bilgi düzeylerinin ise çoğunlukla orta düzey (%32,4) olarak belirtilmiş olmasına rağmen toplamda düşük bilgi düzeyinde yoğunlaştığı görülmektedir.

Araştırmaya katılan mali müşavirlerin teknolojik ürün kullanım sıklıkları incelendiğinde çoğunluğunun;

- a. Mesleki teknolojik ürünlerden, meslektaşları, sosyal çevresi ve meslek odaları dışındaki kaynaklar (%31,86) aracılığıyla haberdar olduğu,
- b. Mesleki araştırmalarında, teknolojik ürünleri her gün (%79,66) kullandıkları ve bu ürünlerin çok önemli (%73,77) bir yere sahip olduğu,
- c. Yeni teknolojik ürünlerin gündelik hayatta çok önemli (%75,74) olduğunu ifade etmeleriyle birlikte genel bir teknolojik ürün satışa çıktığında büyük çoğunluğunun ihtiyaç olduğunda (%91,18) satın aldığı ve mesleki teknolojik ürün satın almak için yine ihtiyaç olduğunda (%78,68) bütçe oluşturduğu,
- d. Mesleki teknolojik ürün kullanımında teknik desteği, program satıcılarından (%71,81) aldıkları,
- e. İş hayatında her gün (%97,06) internette işlem yaptığı, bununla birlikte gündelik hayatta 5 saatten (%37,75) fazla akıllı telefon kullandığı,
- f. İş hayatında teknolojik ürün kullanmak zorunda olduğu mükellef sayısının 1-20 arasında (%52,45) olduğu

tespit edilmiştir. Bununla birlikte mali müşavirlerin çoğunluğu açısından, blokzincir teknolojisinin benimsenmesinin önündeki en büyük engellerinin müşteri direnci (%37,02) ve kamu direnci (%31,62) olarak görüldüğü tespit edilmiştir.

TKM hipotez testlerinin sonuçlarına göre; blokzincir teknolojisine yönelik yetenekli iş gücü, data güvenliği, mevcut sisteme uyum, karmaşık süreçler gerektirmesi “Engel”lerini ifade eden dış değişkeninin, blokzincir teknolojisi kabulüne yönelik tutum, niyet ve davranışın üzerinde herhangi bir anlamlı etkisinin olmadığı görülmektedir. Diğer yandan tutum değişkeni üzerinde, algılanan kullanım kolaylığı değişkenin etkileri gözlemlenebiliyorken; algılanan fayda değişkeninin etkisi gözlemlenememektedir. Buna rağmen algılanan fayda, niyeti doğrudan etkilemekte ancak niyetin ise davranış üzerinde etkisi bulunmamaktadır. Dolayısıyla yalnızca algılanan kullanım kolaylığı ile tutum değişkenlerinin blokzincir kullanım davranışı üzerindeki toplam etkisi istatistiksel olarak anlamlı bulunmaktadır.

Sonuç olarak Teknoloji Kabul Modeli değişkenlerinin, blokzincir teknolojisi kullanım davranışı üzerindeki etkileri açığa çıkmamıştır. Bu durum, Turgut (2022) ve Moghrabi (2022)'nin çalışmaları ile tutarlıdır. Bir teknoloji ne kadar yeni ise olası kullanıcıların bu teknolojiyi benimsemesi ve özelliklerini tam olarak kavrayabilmesi başlangıçta daha zorlayıcı olabilmektedir, dolayısıyla teknolojinin kabul görmesi ve yaygınlaşması zaman almaktadır (Durach vd., 2021). Blokzincir teknolojisi de bu doğrultuda henüz olgunlaşma aşamasında olmakla birlikte teknolojik altyapısı ve teknik özellikleri de oldukça karmaşıktır. Yaygın olarak kripto para tanımı yerine kullanılmakta, ne olduğu, nasıl çalıştığı ve sağladığı faydalar tam olarak kavranamamaktadır. Bu nedenle blokzincir teknolojisinin, mali müşavirler tarafından benimsenmesi konusunda model değişkenleri etkili olmamıştır.

Demografik ve mesleki özelliklere göre TKM boyutlarına yönelik farklılık testleri sonuçlarına göre; mali müşavirlerin mesleki ünvan özellikleri, yani SMMM veya YMM olmaları, TKM ölçeği boyutları üzerinden meslek mensuplarının blokzincir teknolojisi kabullerinde herhangi bir farklılık yaratmamaktadır. Diğer yandan cinsiyet özelliği de davranış boyutu hariç diğer boyutlar üzerinde yine herhangi bir farklılık ortaya çıkarmamaktadır. Cinsiyete ilişkin blokzincir teknolojisi kabul davranışındaki farklılıklar incelendiğinde ise grup ortalamalarına göre erkeklerin (2.54), blokzincir teknolojisini kullanma eğilimlerinin kadınlara (2.31) kıyasla görece daha fazla olmasıyla birlikte aradaki farkın çok yüksek olmadığı görülmektedir. Bu durumun, erkek mali müşavir sayısının kadınlara göre daha fazla olmasından kaynaklandığı düşünülmektedir.

Katılımcıların demografik ve mesleki özellikleri itibarıyla hile belirtileri ile karşılaşma sıklıklarına yönelik farklılık testleri sonuçlarına göre; mali müşavirlerin çalışma şekli, mesleki tecrübesi ve mükellef sayısı, finansal bilgi manipülasyonu göstergeleri ile karşılaşma sıklıklarına ilişkin ifadelerinde farklılık yaratmıyor iken; cinsiyet, eğitim düzeyi ve mesleki ünvan özellikleri, ifadelerinde farklılıklar ortaya çıkarmaktadır. Ortaya çıkan farklılıkları incelediğimizde;

- a. Erkek mali müşavirlerin (213.63) finansal bilgi manipülasyonlarıyla karşılaşma sıklığının, kadınlara (180.46) göre daha fazla olduğu ve bu durumun erkek mali müşavir sayısının kadınlara göre daha fazla olmasından kaynaklandığı düşünülmektedir.

- b. Eğitim düzeyine göre, finansal bilgi manipölasyonlarıyla en sık karşılaşanların doktora ve yüksek lisans eğitimi görenler olduđu, bunun da eğitim seviyesinin artmasıyla manipölasyonların daha fazla fark edilmesinden kaynaklandığı öne sürölmektedir.
- c. YMM'lerin (264.97) finansal bilgi manipölasyonlarıyla karşılaşma sıklığının, SMMM'lere (197.88) göre daha fazla olduđu, bu farkın YMM ünvanı için gereken üst düzey eğitim ve yetkinliklerden kaynaklandığı düşünölmektedir.

Bu durum, finansal bilgi manipölasyonlarının, hileli işlemlerin özel beceri ve eğitim gerektirmesi nedeniyle akademik ve mesleki eğitim düzeylerinin artmasıyla daha fazla tespit edilebilir olduđuuna ilişkin yaygın görüşü desteklemektedir.

Son olarak katılımcıların demografik ve mesleki özellikleri itibarıyla blokzincir teknolojisinin finansal bilgi manipölasyonlarını önlemedeki rolüne yönelik farklılık testlerinin sonuçlarına göre ise meslek mensuplarının herhangi bir demografik ve mesleki özellikleri blokzincir teknolojisinin finansal bilgi manipölasyonunu önlemedeki rolüne ilişkin ifadelerinde farklılık yaratmıyor iken; blokzincir teknolojisi hakkındaki bilgi düzeyleri, ifadelerinde farklılıklar ortaya çıkarmaktadır. Bilgi düzeylerine ilişkin farklılıklar incelendiğinde; blokzincir teknolojisi hakkında bilgi düzeyi arttıkça, bu teknolojinin finansal bilgi manipölasyonlarını önlemede bir araç olarak kullanılabileceğine ilişkin görüşün hâkim olduđu görölmektedir.

## 8.1 TEORİK ÇIKARIMLAR

Bu çalışmada, finansal bilgi manipölasyonlarının azaltılmasında blokzincir teknolojisinin uygulanabilirliği derinlemesine incelenmiş ve teknolojinin, etkili bir alternatif araç olarak değerlendirilebileceği hususu teorik temellerle desteklenmiştir. Blokzincir teknolojisinin muhasebe ve denetim süreçlerine etkisi, ilgili literatürde pek çok araştırmacı tarafından kapsamlı bir şekilde ele alınmış olsa da finansal bilgi manipölasyonlarına doğrudan etkisi üzerine gerçekleştirilen çalışmaların sayısı oldukça sınırlıdır. Bu durum, ilgili literatürde önemli bir boşluk oluşturduğundan bu çalışmanın, blokzincir teknolojisinin finansal bilgi manipölasyonlarını azaltmadaki etkinliğini ortaya koyarak, alandaki bilgi birikimine anlamlı bir katkı sağlayacağı öngörölmektedir.

Diğer yandan çalışmada ikincil olarak; İstanbul'daki mali müşavirlerin blokzincir teknolojisini kabul etmelerini etkileyen faktörler, muhasebe hileleriyle karşılaşma sıklıkları ve blokzincir teknolojisinin bu hileleri önlemedeki rolüne ilişkin görüşleri, ampirik verilere dayandırılarak incelenmiştir. Ampirik araştırma sonuçlarına göre; İstanbul'daki mali müşavirlerin blokzincir teknolojisini benimseme düzeylerinde, teknolojiye dair bilgi seviyesi belirleyici bir faktör olarak öne çıkmaktadır. Ancak bu profesyonellerin çoğu, blokzincir teknolojisi hakkında oldukça düşük bir bilgi seviyesine sahip bulunmaktadır. Bu durum, büyük ölçüde teknolojinin yeni olmasından, kavramsal olarak anlaşılamamasından, karmaşık yapısından ve potansiyel faydalarının yeterince algılanamamasından kaynaklanmaktadır. Teknolojinin potansiyeli ve uygulama alanları konusunda eksik bilgi ve anlayış, sektördeki profesyonellerin blokzincire yönelik temkinli bir yaklaşım sergilemelerine yol açmaktadır. Nitekim destekleyici olarak, blokzincir teknolojisinin finansal bilgi manipülasyonlarını önlemedeki rolüne ilişkin İstanbul'daki mali müşavirlerin olumlu görüşleri, teknoloji hakkındaki bilgi düzeyi arttıkça etkili olmaktadır. Bunun yanı sıra muhasebe hileleri ile karşılaşma sıklığının, meslek mensuplarının akademik ve mesleki eğitim düzeyleriyle doğrudan ilişkili olduğu gözlemlenmiştir. Mesleki eğitim düzeyi arttıkça, mali müşavirlerin finansal bilgi manipülasyonlarını daha kolay tespit edebilme yeteneklerinin de arttığı anlaşılmaktadır.

Ayrıca bu çalışmada yapılan sistematik literatür taraması sonuçlarına göre; blokzincir teknolojisi kullanımının muhasebe ve denetim sektörlerinde benimsenmesinin Teknoloji Kabul Modeli (TKM) ile ölçülmesine yönelik alan yazında yapılan araştırmaların oldukça az olduğu tespit edilmiş, bununla birlikte Türk yazınında bu konuda yapılan herhangi bir çalışmaya rastlanmamıştır. Bu nedenle çalışmanın ortaya koyduğu sonuçlar, İstanbul'daki mali müşavirlerin blokzincir teknolojisine yönelik yaklaşımlarını anlamak açısından önemli bir ilk referans niteliği taşımaktadır. Diğer yandan mali müşavir meslek mensuplarının faaliyet gösterdikleri çok çeşitli alanlar bulunmakla birlikte bu çalışmada küçük ve orta büyüklükteki mali müşavirlik bürolarında faaliyet gösteren meslek mensupları araştırmaya katılım sağlamışlardır. Dolayısıyla çalışma, teknolojik gelişmeleri daha yakından takip eden büyük mali müşavirlik şirketleri ve denetim firmalarında çalışan meslek mensuplarının yaklaşımlarına yönelik bir çerçeve sunmamaktadır. Bununla birlikte çalışmanın, meslek profesyonellerinin yeni bir araç olan blokzincir teknolojisi hakkındaki farkındalıklarının arttırılarak finansal bilgi manipülasyonunu önlemede ilgili teknolojiyi kullanmalarını

sağlamak amacıyla potansiyel mesleki yetkinliklerinin ve iş alanlarının geliştirilmesi açısından meslek mensuplarına büyük katkılarının olacağı öngörülmektedir.

## 8.2 PRATİK ÇIKARIMLAR

Bu çalışmanın da ortaya koyduğu üzere; blokzincir teknolojisi, muhasebe ve denetim süreçlerinde sağladığı değiştirilemezlik ve şeffaflık ile finansal bilgi kalitesini artırarak, muhasebe sahtekarlıklarını ve finansal bilgi manipülasyonlarını azaltma potansiyeli sunmaktadır. Dolayısıyla gelişimi halen devam etmekte olan bu teknolojiye yönelik karşılaşılan teknik, yasal ve organizasyonel engellerin aşılması ile, muhasebe ve denetim ekosistemine dahil olan tüm paydaşların ilgili teknolojiyi benimsemesi ve etkin kullanımı hızlanacaktır.

Bu kapsamda işletmeler, kamu kurumları ve meslek mensuplarının iş birliği yapması önemlidir. İşletmeler, blokzincir teknolojisinin potansiyelini çalışanlarına anlatmak ve bu alanda eğitim programları düzenlemek suretiyle personelin teknolojiyi daha iyi anlamasını sağlamalıdır. Ayrıca yeni teknolojilere karşı oluşabilecek dirençleri kırmak amacıyla çalışanları motive edecek teşvikler ve bilinçlendirme kampanyaları oluşturulmalıdır. Kamu kurumları ve hükümetler ise blokzincir kullanımını destekleyecek yasal düzenlemeleri ve standartları belirlemeli, bu düzenlemeleri hızla uygulamaya koyarak teknolojinin güvenli ve verimli kullanımını garanti altına almalıdır. Kamu-özel sektör iş birliği aracılığıyla gerçekleştirilen blokzincir projeleri ile de sektördeki güven artırılarak teknolojinin yaygınlaşması sağlanmalıdır. Bununla birlikte yeni bir teknolojiye adaptasyon dolayısıyla işletmelerin üstlendikleri maliyetler, devlet destekleri ve finansal teşvikler yoluyla azaltılarak, işletmelere blokzincir yatırımlarını hızlandırma konusunda cesaret verilmeli; böylece muhasebe-denetim sektörünün güvenilir dijital dönüşümü kolaylaştırılmalıdır. Son olarak meslek mensuplarına yönelik düzenlenecek tanıtım ve eğitim programları ile blokzincir teknolojisinin muhasebe ve denetim süreçlerini nasıl iyileştirebileceği konusunda farkındalık yaratılmalı ve blokzincir teknolojisinin kabulüne hız kazandırılmalıdır.



### 8.3 ÖNERİLER

Araştırma sonucuna göre; blokzincir teknolojisinin muhasebe ve denetim süreçlerinde benimsenmesinin önündeki en büyük engel, meslek mensuplarının bu teknolojiye dair bilgi eksikliklerinden kaynaklanmaktadır. Ayrıca mali müşavirlerin teknolojik ürünlere ilişkin teknik destek için program satıcılarına başvurdukları; bununla birlikte mesleki teknolojik ürünlerden, meslektaşları, sosyal çevresi ve meslek odaları dışındaki kaynaklar aracılığıyla haberdar oldukları gözlemlenmiştir. Diğer yandan araştırmaya katılım sağlayan meslek mensubu kitlesinin küçük ve orta büyüklükteki mali müşavirlik bürolarında faaliyet gösteren meslek mensupları olması dolayısıyla bu profesyonellerin mesleki kaygılar sebebiyle yeni teknolojik gelişmelere karşı temkinli yaklaşıtları düşünülmektedir. Bu nedenle SMMM ve YMM Odaları gibi sektörde etkili profesyonel kuruluşların, blokzincir teknolojisini tanıtmak ve meslek mensuplarını bilgilendirmek amacıyla aktif olarak seminerler ve eğitimler düzenlemesi önerilmektedir.

Ayrıca blokzincir teknolojisinin, sunduğu potansiyel ve artan uygulama alanları ile gelece yön vermesi ve dolayısıyla muhasebe ve denetim süreçlerinde giderek daha fazla yer alması beklenmektedir. Bu nedenle geleceğin mali müşavirlerinin bu teknolojiye hâkim olabilmesi için bir diğer öneri, ilgili alanda eğitim veren yüksek öğretim kurumlarının, özel olarak blokzincir teknolojisi derslerini müfredata dahil etmeleri yönündedir.

### 8.4 AKADEMİSYENLERE ÖNERİLER

Bu çalışma, henüz gelişim aşamasında olan blokzincir teknolojisinin muhasebe ve denetim sektöründe uygulanabilirliği ile ilgili daha çok araştırma yapılması gerekliliğini ortaya koymuştur. Çalışma kapsamında finansal bilgi manipölasyonlarının önlenmesine yönelik blokzincir teknolojisinin potansiyeli, teorik çerçevede analiz edilmiş ve İstanbul'daki mali müşavirlerin ilgili teknolojiyi kabullerini etkileyen faktörler, standart çoklu regresyon analizi ile incelenmiştir. Gelecek araştırmalarda, yapısal eşitlik modelleri ile blokzincir teknolojisi kabulü üzerindeki aracı değişkenlerin etkileri de ölçülerek daha derinlemesine incelenmesi mümkün olabilir. Ya da hile denetmenleri, bağımsız denetçiler gibi farklı evren ve farklı bölge seçimi yapılarak araştırma tekrarlanabilir. Ayrıca blokzincir teknolojisinin, özellikle IoT ve yapay zeka olmak üzere Endüstri 4.0'ın diğer bileşenleriyle birlikte bu teknolojilerin birleşik etkileri ve disiplinlerarası çalışmalar ile bunların muhasebe ve denetim

süreçlerinde kullanımını sağlayan sistem geliřtirmeleri üzerinde de çalışılabilir. Sonuç olarak bu tür arařtırmalar, blokzincir teknolojisinin sektördeki kabulünü artırarak, finansal güvenlięi sağlamada oynayacağı kritik rolü daha iyi ortaya koyabilecektir.



## REFERANSLAR

- Abdioğlu, H. (2007). Hilelerin önlemesi ve ortaya çıkarılmasına yönelik proaktif yaklaşımlar. *Muhasebe Denetimine Bakış*, (22), 119-137.
- Abu Afifa, M.M., Vo Van, H. & Hoang Van, T. L. (2023). Blockchain adoption in accounting by an extended UTAUT model: Empirical Evidence From An Emerging Economy. *Journal of Financial Reporting and Accounting*, 21 (1), 5-44.
- Acar, D., Öztürk, M., & Usul, H. (2016). Dijital ortamda denetim: Sürekli denetim. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 21(Muhasebe Denetimi Özel Sayısı), 1561-1571.
- ACCA. (2017). *Divided We Fall, Distributed We Stand: The Professional Accountant's Guide to Distributed Ledgers and Blockchain*. Association of Chartered Certified Accountants.
- ACFE. (2022). *Occupational Fraud 2022: A Report To The Nations*.
- ACFE. (2024). *Occupational Fraud 2024: A Report To The Nations*.
- Ağcakaya, S. & Kaya, I. (2022). Blockchain Teknolojisi ve Uygulamaları. Serpil Ağcakaya (Ed.), *Blockchain Teknolojisinin Vergi Kayıp ve Kaçaklarına Etkisi* (1. Baskı) içinde (s.59-80). Ankara: Nobel Bilimsel.
- AICPA. *Statements on Auditing Standards (SAS) No.56 : Analytical Procedures*.
- AICPA. *Statements on Auditing Standards (SAS) No.99*.
- AICPA. (2014). *Forensic Accounting - Fraud Investigations*.
- AICPA. (2015). *Audit Analytics and Continuous Audit: Looking Toward the Future*.
- AICPA. (2017). *Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession*.
- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.

- Akleylek, S., Yıldırım, H.M. & Yüce Tok, Z. (2011). Kriptoloji ve uygulama alanları: Açık anahtar altyapısı ve kayıtlı elektronik posta. *Akademik Bilişim*, 1-7.
- Aktan, C.C. (2015). Organizasyonlarda yanlış uygulamalara karşı bir sivil erdem, ahlaki tepki ve vicdani red davranışı: Whistleblowing. *Organizasyon ve Yönetim Bilimleri Dergisi*, 7 (2), 19-36.
- Alagöz, A., Öge, S., & Ortakarpuz, M. (2014). Bir kurumsal zekâ teknolojisi olarak veri madenciliği ile muhasebe bilgi sistemi ilişkisi. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 31(Dr. Mehmet Yıldız Özel Sayısı), 1-21.
- Albayrak, A.S. & Kotan Yılmaz, Ş. (2009). Veri madenciliği: Karar ağacı algoritmaları ve İMKB verileri üzerine bir uygulama. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 14(1), 31-52.
- Alıcı, M. (2021). Kripto Varlıkların Muhasebeleştirilmesi. (Yayınlanmamış doktora tezi). Gazi Üniversitesi/ Sosyal Bilimler Enstitüsü, Ankara.
- Alkan, A. (2007). Finansal uygulamalarda veri madenciliği. *TBD İstanbul Bilişim Kongresi*, İstanbul.
- Alp, A. & Kılıç, S. (2014). *Kurumsal Yönetim*. İstanbul: Doğan Kitap.
- Andolfatto, D. & Martin, F. M. (2022). The blockchain revolution: Decoding digital currencies. *Federal Reserve Bank of St Louis Review*, 104 (3), 149-165.
- Aren, S. (2003). *Yöneticilerin Kar Yönetimi ile İlgili Tutumları ve İMKB'de Bir Uygulama*. (Yayınlanmamış doktora tezi). Gebze Yüksek Teknoloji Enstitüsü/Sosyal Bilimler Enstitüsü, Gebze.
- Arzova, B. (2003). İşletmelerde çalışanlar tarafından yapılan hilelerin kırmızı bayraklar yoluyla izlenmesi. *Muhasebe ve Finansman Dergisi*, (20), 118 – 126.
- Aslan, M. & Kasapbaşı, M.C. (2022). Blok zinciri platformları, fikir birliği mekanizmaları ve ağır güvenlik analizi. *Haliç Üniversitesi Fen Bilimleri Dergisi*, 5 (1), 43-72.

- Aslaner, B. (2022). *Kurumcu İktisat Okulu Perspektifinden Blokzinciri Teknolojisinin Anlamı*. (Yayımlanmamış doktora tezi). İstanbul Üniversitesi/Sosyal Bilimler Enstitüsü, İstanbul.
- Asrav, E. A. (2019). Blok zincir teknolojisi ve akıllı sözleşmelerin vergilendirme usulleri ile muhasebe ve denetim uygulamalarına muhtemel etkileri. *Vergi Raporu*, (232), Ocak, 245-268.
- Ataman, B. & Aydın, R. (2017). Hile Denetimi ve Denetçilerin Hile Tespitine Yönelik Bir Araştırma. *Marmara Business Review*. 2 (1). 1-23.
- Atik, A., & Kelten, G. S. (2021). *Blockchain technology and its potential effects on accounting: a systematic literature review*. *Istanbul business research*, 50(2), 495-515.
- Avaroğlu, E. (2017). Bilgi güvenliğinin temel yapı taşı: Kriptoloji. *Düşünce Dünyasında TÜRKİZE*, 8 (43), 53-65.
- Back, A. (2002). Hashcash - A Denial of Service Counter-Measure. *Tech Report*. <http://www.hashcash.org/papers/hashcash.pdf>.
- Bakırcı, Ç.M. (2017). Bizanslı General Problemi, SHA256 ve İşlem Kanıtı Sistemleri. *Evrin Ağacı*. <https://www.youtube.com/watch?v=gxF022yDcuw>.
- Balanc3. <http://balanc3.net/>.
- Baliga, A. (2017). *Understanding Blockchain Consensus Models*. Persistent, April.
- Baran, Paul (1964). On Distributed Communication Networks. *IEEE Transactions on Communications Systems*, 12 (1), 1-40.
- Bellare, M., Rogoway, P. (2005). *Introduction to Modern Cryptography*. University of California Press, 9, 50-54.
- Bellucci, M., Cesa Bianchi, D., & Manetti, G. (2022). Blockchain in accounting practice and research: systematic literature review. *Meditari Accountancy Research*, 30 (7), 121-146.

- Benford, F. (1938). The law of anomalous numbers. *Proceedings of The American Philosophical Society*, 78 (4), 551-572.
- Beşkirli, A., Özdemir, D. & Beşkirli, M. (2019). Şifreleme yöntemleri ve RSA algoritması üzerine bir inceleme. *Avrupa Bilim ve Teknoloji Dergisi, (Özel Sayı)*, 284-291.
- Bhasin, M. L. (2007). Forensic accounting: A new paradigm for niche consulting. *The Chartered Accountant, January*, 1000-1010.
- Bierstaker, J.L., Brody, R.G. & Pacini, C. (2006). Accountants' perceptions regarding fraud detection and prevention methods. *Managerial Auditing Journal*, 21 (5), 520-536.
- BİLGEM UEKAE Enstitüsü. (2020). *BİLGEM Teknoloji*, 8, 22-25. <https://bilgem.tubitak.gov.tr/tubitak-bilgem-teknoloji-dergisi/sayi-8/>.
- Bingöl, M.A. (2020). Blokzincirde Güvenlik ve Mahremiyet. *BİLGEM Teknoloji*, 8, 38-41. <https://bilgem.tubitak.gov.tr/tubitak-bilgem-teknoloji-dergisi/sayi-8/>.
- Birer, G.C. (2022). Kriptoloji. *Bilim ve Teknik*, 658, 16-31.
- Bitcoin Fiyatı. *BINANCE*. <https://www.binance.com/tr/price/Bitcoin>.
- Bitcoin Resmi İnternet Adresi. [https://en.bitcoin.it/wiki/Main\\_Page](https://en.bitcoin.it/wiki/Main_Page).
- BİTLO AKADEMİ. (2022). Bitcoin Çatalları: Yükseltmeler ve Radikal Blok Zincir Değişimleri. *BİTLO*. <https://akademi.bitlo.com/makale/bitcoin-catallari-yukseltmeler-ve-radikal-blok-zincir-degisimleri>.
- Bizans Hata Toleransı Nedir? *BINANCE ACADEMY*. <https://academy.binance.com/tr/articles/byzantine-fault-tolerance-explained>.
- BKM, Microsoft & VeriPark. (2020). *Herkes İçin Blokzincir (Faz II Güncellenmiş Versiyon)*. [https://bkm.com.tr/wp-content/uploads/2015/06/herkes\\_icin\\_blokzincir\\_2020\\_web.pdf](https://bkm.com.tr/wp-content/uploads/2015/06/herkes_icin_blokzincir_2020_web.pdf)
- Blockchain Türkiye. (2020). *Big Four Blokzincirini Nasıl Kullanıyor?*. <https://bctr.org/big-four-blokzincirini-nasil-kullaniyor-18470/>.

- Blockchain Türkiye Platformu (2019). *Dünyada Blokzinciri Regülasyonları ve Uygulama Örnekleri: Karşılaştırma Raporu.* <https://bctr.org/wp-content/uploads/2019/04/Du%CC%88nyada-Blokzinciri-Regulasyonlar%C4%B1.pdf>.
- Blockchain Türkiye Platformu. (2021a). *Akıllı Sözleşme Raporu.* [https://bctr.org/dokumanlar/Akilli\\_Sozlesme\\_Raporu.pdf](https://bctr.org/dokumanlar/Akilli_Sozlesme_Raporu.pdf).
- Blockchain Türkiye Platformu Teknoloji Çalışma Grubu. (2019a). *Blokzincir için Kavramsal Mimari.* <https://bctr.org/wp-content/uploads/2019/04/04-Blockchain-icin-kavramsal-mimari.pdf>.
- Blockchain Türkiye Platformu Teknoloji Çalışma Grubu. (2019b). *Blokzincir Teknolojisi Terminoloji Çalışması.* [https://bctr.org/dokumanlar/Blokzinciri\\_Teknoloji\\_Terminoloji.pdf](https://bctr.org/dokumanlar/Blokzinciri_Teknoloji_Terminoloji.pdf).
- Blokzincir Nedir? TÜBİTAK. <https://blokzincir.bilgem.tubitak.gov.tr/blokzincir-nedir/>.
- Blok Zinciri Teknolojisinin Artıları ve Eksileri. *Kriptomat.* <https://kriptomat.io/tr/blockchain/blok-zinciri-teknolojisinin-artilari-ve-eksileri/>.
- Bozkurt, N. (2000). Mali Tablolarda İşletme Yönetimleri Tarafından Yapılan Muhasebe Hileleri. *Muhasebe ve Finansman Dergisi*, 12, 15-22.
- Bozkurt, N. (2000b). Muhasebe ve denetim mesleğinde yeni bir alan : Adli muhasebecilik. *Yaklaşım Dergisi*, 8(94), 56-61.
- Bozkurt, N. (2011). *İşletmelerin Kara Deliği Hile: Çalışan Hileleri*. Alfa Basım Yayım.
- Bozkurt, N. (2015). *Muhasebe Denetimi*. İstanbul: Alfa Yayınları.
- Bozkurt Yüksel, A. E. (2015). Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış. *İÜHFM* 73 (2), 173-220.
- Bulut, Y.E. & Sertkaya, İ. (2020). Security problem definition and security objectives of cryptocurrency wallets in common criteria. *Bilişim Teknolojileri Dergisi*, 13 (2), 157-166.

Buterin, V. ( 2013). Ethereum White Paper. *ethereum.org*.

Buterin, V. (2015). Visions, Part 1: The Value of Blockchain Technology. *Ethereum Foundation Blog*. <https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology>.

But how does Bitcoin actually work? *3Blue1Brown*.  
<https://www.youtube.com/watch?v=bBC-nXj3Ng4>.

Cai, C. W. (2019). Triple-entry accounting with blockchain: How far have we come?. *Accounting & Finance*, 61(1), 71-93.

Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: a perspective from blockchain technology. *Financial Innovation*, 2, 1-10.

Cambridge İngilizce Sözlüğü.  
<https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce/manipulation>.

Can, A. V. (2007). Luca Pacioli Muhasebenin Babası mıdır?. *Akademik Bakış*, 12, 1-15.

Carda, H. (2021). *Blok Zincir Teknolojisinin Vergi Hukuku Açısından Değerlendirilmesi*. (Yayınlanmamış yüksek lisans tezi). Bandırma Onyedli Eylül Üniversitesi/Sosyal Bilimler Enstitüsü, Bandırma.

Castro, M. & Liskov, B. (1999). Practical Byzantine fault tolerance. *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, 99, 173–186.

CB Insights. (2022). Banking is only the beginning: 65 big industries blockchain could transform. <https://www.cbinsights.com/research/industries-disrupted-blockchain/>.

Champlain, J.J. (2003). *Auditing Information System*. (2. Edition). New Jersey: John Wiley & Sons, Inc..

Chartered Accountants Australia and New Zealand (CA ANZ). (2017). The Future of Blockchain: Applications and Implications of Distributed Ledger Technology. Chartered Accountants Australia and New Zealand.



- Chartered Professional Accountants Canada (CPA Canada). (2016). *Technological Disruption of Capital Markets and Reporting? An Introduction to Blockchain*.
- Chaum, D. (1983). Blind signatures for untraceable payments. *Proceedings of Crypto 82*, 199-203.
- Chaum, D. (1985). Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, 28 (10), 1030-1044.
- Chaum, D. (1992). Achieving electronic privacy. *Scientific American*, 267 (2), 96–101.
- Chedrawi, C., & Howayeck, P. (2018). Audit in the Blockchain era within a principal-agent approach. *Information and Communication Technologies in Organizations and Society (ICTO 2018): Information and Communications Technologies for an Inclusive World*.
- Chen, P.W., Jiang, B.S. & Wang, C.H. (2017). Blockchain-based payment collection supervision system using pervasive bitcoin digital wallet. *IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 139-146.
- Chowdhury, E., Stasi, A., & Pellegrino, A. (2023). Blockchain technology in financial accounting: emerging regulatory issues. *Review of Financial Economics*, 21, 862-868.
- CoinMarketCap Resmi İnternet Adresi. <https://coinmarketcap.com/>.
- COSO. (2020). *Blockchain And Internal Control*.
- COSO Internal Control Intergated Framework.
- COSO&ACFE. (2023). *Fraud Risk Management Guide*.
- Coyne, J. G. & McMickle, P. L. (2017). Can blockchains serve an accounting purpose?. *Journal of emerging technologies in accounting*, 14(2), 101-111.
- Crosby, M., Pattanayak, P., Verma, S. ve Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. *Applied Innovation*, 2, 6-19.

Cypherpunk. *BitcoinWiki*. <https://bitcoinwiki.org/wiki/cypherpunk>

Cypherpunk                      Manifesto                      Nedir?                      *BtcTURK*.  
<https://bilgiplatformu.btcturk.com/bitcoin/cypherpunk-manifesto-nedir/>.

Çalış, Y.E., Keleş, E. & Engin, A. (2014). Hilenin ortaya çıkartılmasında bilgi teknolojilerinin önemi ve bir uygulama. *Muhasebe ve Finansman Dergisi*, (63), 93-108.

Çankaya, F. & Gerekan, B. (2009). Hile denetçiliği mesleği ve sertifikalı hile denetçiliği mesleki standartları ve ahlâk kuralları. *Muhasebe ve Denetime Bakış. Nisan*. 93-108.

Çarkacıoğlu, A. (2016). *Kripto-Para Bitcoin*. Sermaye Piyasası Kurulu Araştırma Dairesi.

Çaşkurlu, E. & Arslan, C. B. (2021). Blokzincir teknolojisi, kripto paralar ve finansal derinleşme: Türkiye üzerine bir analiz. *Iğdır Üniversitesi Sosyal Bilimler Dergisi*. 10 (28). 97-124.

Çekmen, Y. (2022). *Muhasebede Yapılan Hatalar, Hileler ve Adli Muhasebe* (1. Baskı). Ankara: İKSAD Yayınevi.

Çetin, S. C. & Aydar, M. (2019). Blokzincir protokolleri üzerine örnek kodlar yardımıyla genel bir inceleme. *IV. INSAC International Natural and Engineering Sciences Congress*, 132-142.

Çıtak, N. (2009). Yaratıcı muhasebe hileli finansal raporlama mıdır? *Mali Çözüm*, (91), 81-109.

Çidem, D. (2012). *Anahtarlı ve Anahtarsız Kriptografik Hash Fonksiyonları*. (Yayınlanmamış yüksek lisans tezi). Erciyes Üniversitesi/Fen Bilimleri Enstitüsü. Kayseri.

Çölkesen, R. & Örencik, B. (2008). *Bilgisayar Haberleşmesi ve Ağ Teknolojileri* (5. Baskı). İstanbul: Papatya.

Dai, J. & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems*, 31(3), 5-21.

- Dai, W. (1998). B-money. Satoshi Nakamoto Institute.  
<https://nakamotoinstitute.org/library/b-money/>.
- Davis Fred, D. (1985). *A Technology Acceptance Model For Empirically Testing New End-User Information Systems: Theory And Results*. Massachusetts Institute of Technology, Massachusetts, USA.
- Davis, F. D., Bagozzi, R. P., and Warshaw, P.R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management Science* 35 (8), 982-1003.
- Deloitte. (2016). *Blockchain Technology: A Game-Changer in Accounting?*.
- Deloitte. (2017). *Blockchain Technology and Its Potential in Taxes*.
- Deloitte & TUSIAD. (2018). *Blokzincir Potansiyelinin Keşfi - 2018 Yılı Türkiye Blokzincir Araştırması*.
- Demir, V. & Bahadır, O. (2007). Muhasebe manipölasyonu muhasebe manipölasyonu yöntemler ve teknikler. *Mali Çözüm*, 17 (84), 103-119.
- Dereköy, F. (2020). Muhasebe Manipölasyonları: Toshiba Vakası. *Muhasebe ve Finansman Dergisi*, Ocak (85), 91-110.
- Dilek, Ş. (2018). *Blockchain Teknolojisi ve Bitcoin*. Analiz (231. sayı). SETA.
- Doğan, M., & Ertugay, E. (2019). Blokzinciri ve muhasebe alanındaki uygulamaları. *Üçüncü Sektör Sosyal Ekonomi Dergisi*, 54(4), 1654-1670.
- Dolev, D. (1982). The Byzantine generals strike again. *Journal of Algorithms*, 3 (1), 14-30.
- Dönmez, A. & Ersoy, A. (2011). Bağımsız Denetim Sürecinde Analitik İnceleme Prosedürleri: Türkiye’de SPK’dan Yetki Almış Denetim Firmaları Üzerine Bir Araştırma. *Bilgi : Türk Dünyası Sosyal Bilimler Dergisi*, (56), 121-142.
- Durach, C. F., Blesik, T., von Düring, M., & Bick, M. (2021). Blockchain applications in supply chain transactions. *Journal of Business Logistics*, 42(1), 7-24.

- Dursun, T. (2020). Blokzincir Teknolojisi. *BİLGEM Teknoloji*, 8, 10-15.  
<https://bilgem.tubitak.gov.tr/tubitak-bilgem-teknoloji-dergisi/sayi-8/>.
- Dupont, Q. (2014). The Politics of Cryptography: Bitcoin and the Ordering Machines. *Journal of Peer Production*, 4 (1), 1-29.
- Dwork, C. & Naor, M. (1993). Pricing via processing or combatting junk mail, advances in cryptology. *Crypto '92: Lecture Notes in Computer Science*, 740 Springer, 139–147.
- EBA. (2014). *EBA Opinion on Virtual Currencies*.
- ECB. (2012). *Virtual Currency Schemes*.
- Eğilmez, M. (2013). Bitcoin. *Kendime Yazılar*.  
<https://www.mahfiegilmez.com/2013/11/bitcoin.html>.
- Eğilmez, M. (2017). Kripto Paralar, Bitcoin ve Blockchain. *Kendime Yazılar*.  
<https://www.mahfiegilmez.com/2017/11/kripto-paralar-bitcoin-ve-blockchain.html>.
- Enofe, A.O., Okpako, P.O. & Atube, E.N. (2013). The impact of forensic accounting on fraud detection. *European Journal of Business and Management*, 5(26), 61-70.
- Erkorkmaz, Ü., Etikan, İ., Demir, O., Özdamar, K., & Sanisoğlu, S. Y. (2013). *Doğrulayıcı faktör analizi ve uyum indeksleri*. Türkiye Klinikleri Journal of Medical Sciences, 33(1), 210-223.
- Ertikin, K. (2017). Hile denetimi: kırmızı bayrakların tespiti için kullanılan proaktif yaklaşımlar. *Muhasebe ve Finansman Dergisi*, Temmuz, 71-94.
- Ethereum Resmi İnternet Adresi. <https://ethereum.org/en/>.

<https://worldwide.espacenet.com/patent/search/family/022107098/publication/US4309569A?q=ap%3DUS7236379A>.

Fawole, J., Malanii, O. & Ciattaglia, L. (2023). Blockchain Architecture Layers: A Comprehensive Guide. *HACKEN*. <https://hacken.io/discover/blockchain-architecture-layers/>.

Fiat, A. & Shamir, A. (1986). How to prove yourself: Practical solutions to identification and signature problems. *Proc. of Crypto 86 LNCS*, 263, 186-194.

Field, A. (2005). *Discovering Statistics Using SPSS*. London: Sage Publications Ltd.

Garg, V., Alam, T. and Madan, S. (2021). A Study On Blockchain Technology: History, Features And Applications. *International Research Journal of Modernization in Engineering Technology and Science*. 3 (5). 501-508.

Garnett, A. G. (2023). How smart contracts work with blockchain: A step-by-step guide. *Encyclopedia Britannica*. <https://www.britannica.com/money/how-smart-contracts-work>.

Gartner. (2017). Forecast: Blockchain business value, worldwide, 2017–2030. <https://medium.com/consensys-media/gartner-blockchain-will-deliver-3-1-trillion-dollars-in-value-by-2030-d32b79c4c560>.

Gegez, A.E. & Gegez, E.E. (2023). *Pazarlama Araştırmaları Metodolojik Yaklaşım*. İstanbul : Beta Basım Yayım Dağıtım A.Ş.

Gelir İdaresi Başkanlığı (GİB). (2010). *Transfer Fiyatlandırması Yoluyla Örtülü Kazanç Dağıtımı Hakkında Rehber*. Yayın No:114, Kasım.

Genesis Address. *Blockchain.com.*  
<https://www.blockchain.com/explorer/addresses/btc/1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa>.

Genesis Block (Başlangıç Bloğu) Nedir?. *Digicentralized.*  
<https://digicentralized.com/genesis-block-nedir/>.

Genesis Block (Başlangıç Bloku) Nedir?. *BtcTURK.*  
<https://bilgiplatformu.btcturk.com/blokszinciri/genesis-block-nedir/>.

Genet, T., Jensen, T. & Sauvage, J. (2020). Termination of Ethereum's smart contracts. *17th International Conference on Security and Cryptography, 1*, 39-51.

Giang, N. P., & Tam, H. T. (2023). Impacts of Blockchain on Accounting in the Business. *SAGE Open, 13*(4), 1-13.

Golumbia, D. (2016). *The Politics of Bitcoin: Software as Right-Wing Extremism*. University of Minnesota Press.

Goodhue, D. L., & Thompson, R. L. (1995). Task-technology fit and individual performance. *MIS Quarterly 19* (22), 213-236.

Gönen, M.E., Kara, O. & Karakoç, F. (2021). Siber Güvenlik ve Savunma: Blokzincir ve Kriptoloji. Şeref Sağıroğlu & Sedat Akyelek (Ed.), *Simetrik Sistemlerde Kriptoanaliz Yöntemleri* (1. Baskı) içinde (s.347-440). Ankara: Nobel.

Grigg, I. (2005). Triple entry accounting. *Systemics Inc*, 1-10.

Guleria, A. & Gupta, H. (2022). Review of blockchain technology. *Journal of Pharmaceutical Negative Results, 13* (5), 784-787.

- Gül, H. (2019). Sosyal, Beşerî ve İdari Bilimlerde Yenilikçi Yaklaşımlar. H. Hale Künüçen, Xatire Quliyeva & Yılmaz Seçgin (Ed.), *Blokzincir (Blockchain) Teknolojisi ve Muhasebe Bilgi Sistemine Etkileri* (1. Baskı) içinde (s.186-195). Bursa: Ekin Yayınevi.
- Güner, M. & Kurnaz, E. (2020). Muhasebe manipölasyonunun beneish modeli yardımıyla ölçülmesi: bıst kimya, petrol, plastik endeksi şirketleri üzerine bir araştırma. *Journal of Accounting and Taxation Studies*, 13(2), 195-214.
- Gürbüz, S. & Şahin, F. (2015). *Sosyal Bilimlerde Araştırma Yöntemleri, Sosyal Bilimlerde Araştırma Yöntemleri Felsefe-Yöntem-Analiz (IBM SPSS ve LISREL Uygulamalı, Veri CD'li)* (Gözden Geçirilmiş ve Güncellenmiş 2. Baskı). Ankara: Seçkin Yayıncılık.
- Haber, S. and Stornetta, W.S. (1991). How to Time-Stamp a Digital Document. *Journal of Cryptology*. 3 (2). 99-111.
- Hair, J.F., Anderson, R.E., Tatham, R.L. & Black, W.C. (1998). *Multivariate Data Analysis* (5. Edition). Englewood Cliffs, NJ: Prentice Hall.
- Han, H., Shiwakoti, R. K., Jarvis, R., Mordi, C., & Botchie, D. (2023). Accounting and auditing with blockchain technology and artificial Intelligence: A literature review. *International Journal of Accounting Information Systems*, 48, 100598.
- Han, J., Kamber, M. & Pei, J. (2012). *Data Mining Concepts and Techniques*. (3. Edition). Waltham: Morgan Kaufmann Publishers.
- Hashcash (2003). [www.hashcash.org](http://www.hashcash.org).

- Hatunoğlu, Z., Koca, N. & Kılılı M. (2012). İç kontrolün muhasebe sistemindeki hata ve hilelerin önlenmesindeki rolü üzerine bir alan çalışması. *Mustafa Kemal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 9(20), 169-189.
- Hayes, A. (2024). Blockchain Facts: What is it, how it works, and how it can be used. *Investopedia*. <https://www.investopedia.com/terms/b/blockchain.asp>.
- Hoffman, M. R. (2018). Can blockchains and linked data advance taxation. *In Companion Proceedings of the The Web Conference 2018*, 1179-1182.
- Hughes, E. (1993). A Cypherpunk's Manifesto. <https://www.activism.net/cypherpunk/manifesto.html>.
- Investopedia Team. (2024). Cryptocurrency Wallet: What It Is, How It Works, Types, and Security. *Investopedia*. <https://www.investopedia.com/terms/b/bitcoin-wallet.asp>.
- İbiş, C. & Çatıkkaş, Ö. (2012). İşletmelerde iç kontrol sistemine genel bakış. *Sayıştay Dergisi*, (85), 95-121.
- Ijiri, Y. (1986). A Framework for triple-entry bookkeeping. *The Accounting Review*, 61 (4), 745–759.
- İlkbahar, R. (2019). Araştırma şirketlerinin gözünden Blokzincir'in geleceği. <https://bctr.org/arastirma-sirketlerinin-gozunden-blokszincirin-gelecegi-8127/>.
- İlk Bitcoin Transferi. *BtcTURK*. <https://bilgiplatformu.btcturk.com/bitcoin/ilk-bitcoin-transferi/>.
- İşgüden Kılıç, B. & Anadolu, Z. (2018). Dijital çağın yarattığı muhasebe uygulamalarının muhasebe hilelerinin önlenmesine etkisi. *Muhasebe ve Vergi Uygulamaları Dergisi, Özel Sayı*, 55-97.
- Jakobsson, M & Juels, A. (1999). Proofs of Work and Bread Pudding Protocols. B. Preneel (Ed.), *Secure Information Networks* içinde (s. 258-272) Springer Science+Business Media Dordrecht.
- Jarvis, C. (2022). Cypherpunk ideology: objectives, profiles, and influences (1992–1998). *Internet Histories*, 6 (3), 315-342.



- Jia, W. & Zhou, W. (2005). *Distributed Network Systems From Concepts to Implementations*. Springer Science+ Business Media Inc., New York, USA.
- Jiang, L. (2024). The use of blockchain technology in enterprise financial accounting information sharing. *Plos One*, 19 (2), 1-17.
- Jokić, S., Cvetković, A.S., Adamović, S., Ristić, N. & Spalević, P. (2019). Comparative analysis of cryptocurrency wallets vs traditional wallets. *Ekonomika*, 65 (3), 65-75.
- Juels, A. & Brainard, J. (1999). Client puzzles: A cryptographic countermeasure against connection depletion attacks. In *Network and Distributed System Security Symposium*.
- Kaminski, J. (2011). Diffusion of innovation theory. *Canadian Journal of Nursing Informatics*, 6(2), 1-6.
- Kamu Gözetim Kurumu (KGK). *Bağımsız Denetim Standardı 200*.
- Kamu Gözetim Kurumu (KGK). *Bağımsız Denetim Standardı 240*.
- Kandemir, C. & Kandemir, Ş. (2012a). Muhasebe hilelerinin önlenmesi ve ortaya çıkarılmasında kullanılan geleneksel araç ve yöntemler. *Mali Çözüm*. Eylül-Ekim. 39-78.
- Kandemir, C. & Kandemir, Ş. (2012b). Muhasebe hilelerinin önlenmesi ve ortaya çıkarılmasında kullanılan çağdaş araç ve yöntemler. *Mali Çözüm Kasım-Aralık*, 37-70.
- Kara, O. (2009). Kriptografinin yapıtaşları kriptografik algoritmalar ve protokoller. *Bilim ve Teknik*, Temmuz, 34-41.
- Kara, S. & Karan, L. (2023). Hile denetimi yaklaşımları ve bir vaka çalışması. *Denetişim*, 14 (28), 75-87.
- Karaarslan, E. & Yazıcı Yılmaz, S. (2022). Metaverse ve merkeziyetsizlik. Fatih Sinan Esen (Ed.), *METaverse Geleceğin Dünyalarını İnşa Edecek Teknolojiler, Fırsatlar ve Tehditler* (1. Baskı) içinde (s.45-61). Ankara: Nobel.

- Karacan, A.İ. & Erişir Karacan, E. (2021). *Kripto Varlıklar* (1. Baskı). İstanbul: Scala Yayıncılık.
- Karadeniz, Ş. (2011). Ağlar ve Veri İletişimi. Abdullah Kuzu (Ed.), *Bilgisayar Ağları ve İletişim* (2. Baskı) içinde (s. 1-33). Ankara: Nobel.
- Karahan, Ç. & Tüfekçi, A. (2019). Blokzincir Teknolojisinin İç Denetim Faaliyetlerine Etkileri: Fırsatlar ve Tehditleri. *Denetim*. 9 (19), 55-72.
- Karahanna, E., Straub, D. W., ve Chervany, N. L. (1999). Information technology adoption across time: a cross-sectional comparison of pre adoption and post-adoption beliefs. *MIS Quarterly*, 23(2), 183-213.
- Karakuş, M. (2021). Siber Güvenlik ve Savunma: Blokzincir ve Kriptoloji. Şeref Sağıroğlu & Sedat Akyelek (Ed.), *Blokzinciri ve Yazılım Tanımlı Ağlar* (1. Baskı) içinde (s.165-216). Ankara: Nobel.
- Kardaş, S. (2019). Blokzincir teknolojisi: uzlaşma protokolleri. *DÜMF Mühendislik Dergisi*, 10 (2), 481-496.
- Kasireddy, P. (2017). How does Ethereum work, anyway? <https://www.preethikasireddy.com/post/how-does-ethereum-work-anyway>.
- Kaşıkcı, B. & Dalgat, H. (2021). Muhasebe hilelerinin ortaya çıkarılmasında Benford Yasası'nın kullanılmasına yönelik bir uygulama. *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, 12 (32), 1196-1211.
- Kaya, P. & Uzay, Ş. (2018). Hileli finansal raporlama ve bağımsız denetçinin sorumluluğu. *Muhasebe Bilim Dünyası Dergisi Özel Sayı*, 20, 721-740.
- Kazan, G. (2021). Hile üçgeni, hile elması ve hile beşgeni: hile eylemlerinin nedenlerine ilişkin teorilere kavramsal bakış. *Muhasebe ve Denetime Bakış*, 20 (62), 245-258.
- Kılıç, B. (2020). Blokzincir Uygulama Alanları. *BİLGEM Teknoloji*. 8, 16-20. <https://bilgem.tubitak.gov.tr/tubitak-bilgem-teknoloji-dergisi/sayi-8/>.

- Kılıçer, K. (2011). Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bireysel Yenilikçilik Profilleri. (Yayınlanmamış doktora tezi). Anadolu Üniversitesi/Eğitim Bilimleri Enstitüsü, Eskişehir.
- Kılınç, Y. (2020). Blockchain teknolojisi: Muhasebe ve denetim mesleği açısından bir inceleme. *Muhasebe ve Vergi Uygulamaları Dergisi*. 13 (3), 989-1011.
- Kıllı, M. & Evci, S. (2017). Muhasebe manipülasyonlarının tespitinde kullanılan modeller. *Osmaniye Korkut Ata Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 1 (1), 68-79.
- King, S. & Nadal, S. (2012). PPCoin: Peer-to-peer crypto-currency with proof-of-stake. *Self-Published Paper*, 19.
- Kiracı, M. (2005). Hile riski değerlemesinin ve hileleri bulmanın denetimin etkinliğindeki rolü ve Türkiye'deki denetim firmalarına yönelik bir araştırma. *Muhasebe ve Denetim Bakış*, (14), 103-126.
- Kocameşe, M. & Güçlü, F.C. (2010). Muhasebe hilelerinin ortaya çıkartılmasında Benford Kanunu ve rakamsal analiz yönteminin kullanımı. *İç Denetim*, (29), 28-37.
- Koç, F. (2022). *A Decentralized BIM Document Management System With Blockchain And IPFS Integration For Construction Project Delivery*. Middle East Technical University/The Graduate School Of Natural And Applied Sciences, Ankara.
- Kodaz, H. & Botsalı, F.M. (2010). Simetrik ve asimetrik şifreleme algoritmalarının karşılaştırılması. *Selçuk-Teknik Dergisi*, 9 (1), 10-23.
- Kokina, J., Mancha, R., Pachamano, D. (2017). Blockchain: Emergent Industry Adoption and Implications for Accounting. *Journal Of Emerging Technologies In Accounting*. 14 (2). 91-100.
- Kozlowski, S. (2018). *An audit ecosystem to support blockchain-based accounting and assurance*. In *Continuous Auditing: Theory and Application* (pp. 299-313). Emerald Publishing Limited.
- KPMG. (2020). *Bir Suistimalcinin profili 2020*.

- Kripto cüzdanı nedir? COINBASE. <https://www.coinbase.com/tr/learn/crypto-basics/what-is-a-crypto-wallet>.
- Kroon, N., Alves, M.d.C. & Martins, I. (2021). The Impacts of Emerging Technologies on Accountants' Role and Skills: Connecting to Open Innovation - A Systematic Literature Review. *Journal of Open Innovation Technol. Mark. Complex.* 7 (163), 1-27.
- Küçükkocaoğlu, G., Keskin Benli, Y & Küçüksözen, C. (1997). Finansal bilgi manipülasyonunun tespitinde yapay sinir ağı modelinin kullanımı. *İMKB Dergisi*, 9 (36), 1-30.
- Küçükkocaoğlu, G. & Küçüksözen, C. (2005). Gerçeğe aykırı finansal tabloların ortaya çıkarılması: İMKB şirketleri üzerine ampirik bir çalışma. *Muhasebe ve Finansman Dergisi*, (28), 160-171.
- Küçüksözen, C. (2004). *Finansal Bilgi Manipülasyonu: Nedenleri, Yöntemleri, Amaçları, Teknikleri, Sonuçları ve İMKB Şirketleri Üzerine Ampirik Bir Çalışma*. Ankara Üniversitesi/Sosyal Bilimler Enstitüsü, Ankara.
- Küçüksözen, C. & Küçükkocaoğlu, G. (2005). Kurumsal şirket yönetiminde finansal bilginin rolü. *Muhasebe ve Denetime Bakış. Eylül*. 81-104.
- Kwiatkowska, M., Norman, G. & Parker, D. (2008). Analysis of a gossip protocol in PRISM. *ACM SIGMETRICS Performance Evaluation Review*, 36 (3), 17-22.
- Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4 (3), 382–401.
- Landu, M., Mota, J.H., Moreira, A.C. & Bandeira, A.M. (2024). Factors influencing the quality of financial information: A systematic literature review. *South African Journal of Accounting Research*, 1-28.
- Lansiti, M. & Lakhani, K.R. (2017). The truth about blockchain. *Harvard Business Review*, January-February, 2-11 .

- Lazanis, R. (2015). How technology behind bitcoin could transform accounting as we know it. *BrainStation*. <https://brainstation.io/magazine/how-technology-behind-bitcoin-could-transform-accounting-as-we-know-it>.
- Lehman, D.R., Gupta, S. & Steckel, J.H. (1998). *Marketing Research*. Reading, Massachusetts: Addison-Wesley Educational Publishers Inc.
- Liu, C., Muravskiy, V., & Wei, W. (2024). Evolution of blockchain accounting literature from the perspective of CiteSpace (2013–2023). *Heliyon*, 10, 1-17.
- May, T. (1988). *The Crypto Anarchist Manifesto*. <https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html>.
- McCallig, J., Robb, A., & Rohde, F. (2019). Establishing the representational faithfulness of financial accounting information using multiparty security, network analysis and a blockchain. *International Journal of Accounting Information Systems*, 33, 47-58.
- McNally, J.S. (2013). *The 2013 COSO Framework & SOX Compliance*. COSO.
- Melse, E. (2008). Accounting in three dimensions: a case for momentum revisited. *The Journal of Risk Finance*, 9(4), 334-350.
- Mercan, N., Altınay, A. & Aksanyar, Y. (2012). Whistleblowing (bilgi ifşası, ihbar) ve yolsuzlukla mücadelede iç denetimin değişen ve gelişen rolü. *Organizasyon ve Yönetim Bilimleri Dergisi*, 4 (2), 167-176.
- Merkle, R.C. (1987). A digital signature based on a conventional encryption function. *Advances in Cryptology CRYPTO'87 Conference Paper*, 369-378.
- Mert, H., Türedi, E. & Bayar, E. (2022). Hilenin ortaya çıkartılmasına yönelik reaktif ve proaktif yaklaşımların karşılaştırmalı incelenmesi ve perakende sektöründe bir uygulama. *İda Academia Muhasebe ve Maliye Dergisi*, 5 (2), 67-82.
- Monrat, A.A., Schelen, O., ve Andersson, K. (2019). A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. *IEEE Access*, 7, 117134 - 117151.

- Mosakheil, J.H. (2018). *Security Threats Classification in Blockchains*. (Master Thesis). St. Cloud State University/Department of Information Systems, St. Cloud-Minnesota.
- Mulford, C.W. & Comiskey, E.E. (2002). *The Financial Numbers Game : Detecting Creative Accounting Practices*. John Wiley & Sons.
- Murdock, H. (2017). *Operational Auditing: Principles And Techniques For A Changing World*. New York: CRC Press Taylor & Francis Group.
- Murthy, C.V., Shri, M.L., Kadry, S.N., & Lim, S. (2020). Blockchain based cloud computing: Architecture and research challenges. *IEEE Access*, 8, 205190-205205.
- Nakamoto, S. (2008a). Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin*. <https://bitcoin.org/bitcoin.pdf>.
- Nakamoto, S. (2008b). Bitcoin P2P e-cash paper. *Cryptography Mailing List*. <https://satoshi.nakamotoinstitute.org/emails/cryptography/1/>.
- Nakamoto, S. (2009). Bitcoin open source implementation of P2P currency. *P2P Foundation*. <https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>.
- Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton University Press.
- Newcomb, S. (1881). Note on the frequency of use of the different digits in natural numbers. *American Journal of Mathematics*, 4(1), 39-40.
- Nguyen, G.T. & Kim, K. (2018). A survey about consensus algorithms used in blockchain. *Journal of Information Processing Systems*, 14 (1), 101-128.
- Nordgren, A., Weckström, E., Martikainen, M., & Lehner, O. M. (2019). Blockchain in the fields of finance and accounting: a disruptive technology or an overhyped phenomenon. *ACRN Journal of Finance and Risk Perspectives*, 8(Special Issue; Digital Accounting), 47-58.
- Nowroozi, E., Seyedshoari, S., Mekdad, Y., Savaş, E. & Conti, M. (2023). Cryptocurrency wallets: assessment and security. Yassine Maleh, Mamoun Alazab & Umed

- Romdhani (Ed.), *Blockchain for Cybersecurity in Cyber-Physical Systems* içinde (s.1-19). Springer.
- Ocak, M. & Güçlü, F.C. (2014). Muhasebe Manipülasyonu: Hile, Yaratıcı Muhasebe, Kar ve İzlenim Yönetimine İlişkin Kavramsal Çerçeve. *Uluslararası Alanya İşletme Fakültesi Dergisi*, 6 (3), 123- 135.
- Oğuz, R., Kınacı, E. & Babacan, H.H. (2023). Kripto para cüzdanının (sıcak cüzdan) adli bilişim açısından incelenmesi. *Journal of Computer Science*, 8 (2), 130-147.
- Onocak, D. (2022). Güncel İşletme Yönetimi Çalışmaları I. Serkan Yılmaz Kandır & İlksun Didem Ülbeği (Ed.), *Muhasebe Hilelerinin Tespitinde Kullanılan Yöntemler* (1. Baskı) içinde (s. 217-229). Ankara: Akademisyen Kitabevi.
- Oyovwe, A. (2023). Triple – entry accounting: transcending the double – entry system
- Öngen, K.B. (2010). *Doğrulamalı Faktör Analizi İle Bir Uygulama* (Yayınlanmamış yüksek lisans tezi). Uludağ Üniversitesi/Sosyal Bilimler Enstitüsü, Bursa.
- Ös, M. (2021). *Endüstri 4.0'ın Muhasebe Mesleğine Etkisinin Teknoloji Kabul Modeli İle Ölçümü*. (Yayınlanmamış doktora tezi). Hasan Kalyoncu Üniversitesi/Lisansüstü Eğitim Enstitüsü, Gaziantep.
- Özalp, A. (2018). *Uluslararası Ticaretin Finansmanı, Prensipleri ve Blockchain*, Türkmen Kitabevi, İstanbul.
- Özçetin, N. (2022). Muhasebe Denetiminde Yapay Zekâ. *Uşak Üniversitesi Uygulamalı Bilimler Fakültesi Dergisi*, 2(1), 29-41.
- Özdemir, F.S. (2013). Finansal bilginin kapsamı ve finansal bilgi türlerinin sınıflandırılmasına yönelik bir öneri. *Muhasebe Bilim Dünyası*, 15 (4), 155-175.
- Özdoğan, B. & Karğın, S. (2018). Blok Zinciri Teknolojisinin Muhasebe Ve Finans Alanlarına Yönelik Yansımaları Ve Beklentiler. *Muhasebe ve Finansman Dergisi*. (80), 161-190.
- Özekes, S. (2003). Veri madenciliği modelleri ve uygulama alanları. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, 2(3), 65-82.

- Özmen, Ş. (2001). İş hayatı veri madenciliği ile istatistik uygulamalarını yeniden keşfediyor. *Ulusal Ekonometri ve İstatistik Sempozyumu*, Adana.
- Özseven, T. (2014). *Bilgisayar Ağları* (Gözden Geçirilmiş 2. Baskı). Bursa: Ekin.
- Öztoprak, Y. (2017). *Denetimde Hata ve Hile, Önleme ve Tespit Yöntemleri ile Serbest Muhasebeci Mali Müşavirlerin Hata ve Hileler ile İlgili Bilinç ve Tutumları*. (Yayınlanmamış doktora tezi). İstanbul Gelişim Üniversitesi/Sosyal Bilimler Enstitüsü, İstanbul.
- Pacio. <https://pacio.io/docs/PacioWhitePaper.pdf>.
- Peercoin Resmi İnternet Adresi <https://www.peercoin.net/university/#/9-peercoin-proof-of-stake-consensus>.
- Pehlivanlı, D. (2011). Denetim yaklaşımlarından butik denetime. *Denetışim*, (8), 14-17.
- Peters, G.W., Panayi, E. & Chapelle, A. (2015). Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective. *SSRN Electronic Journal*, 1-25.
- Potekhina, A., & Riumkin, I. (2017). *Blockchain – A New Accounting Paradigm: Implications For Credit Risk Management*. Umeå University/School of Business and Economics.
- Prisco, G. (2016). Deloitte Team Launches Custom Blockchain Solution Rubix Core. *Bitcoin Magazine*. <https://bitcoinmagazine.com/business/deloitte-team-launches-custom-blockchain-solution-rubix-core-1463687003>.
- Proof of Stake (Hisse Kanıtı) Nedir? Nasıl Çalışır? *BtcTURK*. <https://bilgiplatformu.btcturk.com/blokzinciri/proof-of-stake-hisse-kaniti-nedir-nasil-calisir/>.
- PwC. (2016). *Technology In The PwC Audit - Driving Innovation*. <https://www.pwccn.com/en/audit-assurance/technology-in-pwc-audit.pdf>.
- PwC. (2022). *Global Economic Crime and Fraud Survey 2022*.



- Rezaee, Z., Elam, R., & Sharbatoghlie, A. (2001). Continuous auditing: the audit of the future. *Managerial Auditing Journal*, 16(3), 150-158.
- Ripple Resmi İnternet Adresi. <https://ripple.com/>.
- Rogers, E. M. (1995). Diffusion of innovations (Fifth Edition). New York: Free Press.
- Rogers, E.M. (2003). Diffusion of innovations (5th ed.). New York: Free Press.
- Rozario, A. M., & Vasarhelyi, M. A. (2018). Auditing with Smart Contracts. *International Journal of Digital Accounting Research*, 18, 1-27.
- Rosic, A. (2023). Cryptocurrency Wallet Guide: A Step-By-Step Tutorial. *Blockgeeks*. <https://blockgeeks.com/guides/cryptocurrency-wallet-guide/>.
- Ryan, P. (2018). PwC shuts DeNovo, its 'Fintech Insights' platform. *Bank Automation News*. <https://bankautomationnews.com/allposts/payments/pwc-shuts-denovo-its-fintech-insights-platform/>.
- Ryan, B. ve Gross, N. C. (1943). The diffusion of hybrid seed corn in two Iowa communities. *Rural Sociology*, 8 (1), 15-24.
- Saifi, R. (2020). *Blockchain and its impact on Auditing and Assurance profession*. ASA.
- Saldamli, G., Upadhyay, C., Jadhav, D., Shrishmal, R., Patil, B. & Tawalbeh, L. (2022). Improved gossip protocol for blockchain applications. *Cluster Computing*, 25, 1915-1926.
- Sangster, A. (2016). The genesis of double entry bookkeeping. *The Accounting Review*, 91(1), 299-315.
- Sangster, A. (2021). The life and works of Luca Pacioli (1446/7–1517), humanist educator. *Abacus*, 57(1), 126-152.
- Sarmah, S.S. (2018). Understanding blockchain technology. *Computer Science and Engineering*, 8 (2), 23-29.

- Sayğan, S. & Bedük, A. (2013). Ahlaki olmayan davranışların duyurulması (whistleblowing) ve etik iklimi ilişkisi üzerine bir uygulama. *Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 28 (1), 1-23.
- Scherer.R. & Teo, T. (2019). Editorial To The Special Section—Technology Acceptance Models: What We Know And What We (Still) Do Not Know. *British Journal of Educational Technology* 50 (5), 2387–2393.
- Schmitz, J. & Leoni, G. (2019). Accounting and Auditing at the Time of Blockchain Technology: A Research Agenda. *Australian Accounting Review* No. 89. 29 (2). 331-343.
- Sedgwick, K. (2019). Bitcoin History Part 18: The First Bitcoin Wallet. *Bitcoin.comNews*. <https://news.bitcoin.com/bitcoin-history-part-18-the-first-bitcoin-wallet/>.
- Selg, M. (2023). *Blockchain Based Auditing: A Qualitative Research Into The Suitability Of Blockchain-Based Auditing To Eliminate Weaknesses Of Contemporary Auditing Their Effectiveness In Auditing Of Accounts Receivable And Compliance Towards GAAS Standard AU-C505*. European Business University of Luxemburg/Graduate School of Business Administration, Luxemburg.
- Shah, G., Padhiar, S. & Parmar, M. (2018). Introduction to Blockchain.
- Shao, A.T. (1999). *Marketing Research: An Aid To Decision Making*. Cincinnati, Ohio: South Western College Publishing.
- Sharma, T.K. (2023). What Is Merkle Tree & Merkle Root In Blockchain? *Blockchain Council*. <https://www.blockchain-council.org/blockchain/what-is-merkel-tree-merkel-root-in-blockchain/>.
- Shi, M. (2021). On the influence of blockchain technology on Accounting. *Financial Forum*, 10(1), 88-92.
- Singleton, T. W., & Singleton, A. J. (2010). *Fraud Auditing and Forensic Accounting* (4. Edition). New Jersey: John Wiley & Sons Inc.

- Smigelski, K. (2019). Ey Ops Chain industrializes the blockchain at scale for enterprises. *Ernst&Young Press Release*. [https://publish-ey-prod-cdn.adobecqms.net/en\\_tw/news/2019/04/ey-ops-chain-industrializes-the-blockchain-at-scale-for-enterprises](https://publish-ey-prod-cdn.adobecqms.net/en_tw/news/2019/04/ey-ops-chain-industrializes-the-blockchain-at-scale-for-enterprises).
- Socea, A. (2012). Managerial decision-making and financial accounting information. *Procedia - Social and Behavioral Sciences*, 58, 47-55.
- Stolowy, H. & Breton, G. (2000). A review of research on accounts manipulation. *In Paper for the Annual Congress of European Accounting Association*, 8 (3), 1-65.
- Sudman, S. (1976). *Applied sampling*. Academic Press.
- Sugiura , N. & Luyat, J.J. (Translation). (2009). Electronic Money and the Law: Legal Realities and Future Challenges. *Pacific Rim Law & Policy Journal*, 18 (3), 511 - 524.
- Suratkar, S., Shirole, M. & Bhirud, S. (2020). Cryptocurrency wallet: A review. *4th International Conference on Computer, Communication and Signal Processing. IEEE*.
- Swan, M. (2015). Blockchain: Blueprint of a New Economy. California: O'reilly Media, Inc.
- Szabo, N. (1994). Smart Contracts. *Nick Szabo's Papers and Concise Tutorials*. <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>.
- Szabo, N. (1995). Smart Contracts Glossary. *Nick Szabo's Papers and Concise Tutorials*. [https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart\\_contracts\\_glossary.html](https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_glossary.html).
- Szabo, N. (1996). Smart Contracts: Building Blocks for Digital Markets. *Nick Szabo's Papers and Concise Tutorials*.
- Szabo, N. (1997a). The Idea of Smart Contracts. *Nick Szabo's Papers and Concise Tutorials*. <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html>.

- Szabo, N. (1997b). Formalizing and Securing Relationships on Public Networks. *Nick Szabo's Papers and Concise Tutorials*.  
<https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/formalize.html>.
- Szabo, N. (2005). Bitgold. *Nick Szabo's Papers and Concise Tutorials*.  
<https://web.archive.org/web/20151121081112/http://unenumerated.blogspot.com/2005/12/bit-gold.html>.
- Şahin, A., Buluş, E. & Sakallı, M.T. (2006). 24-bit renkli resimler üzerinde en önemsiz bite ekleme yöntemini kullanarak bilgi gizleme. *Trakya Univ J Sci*, 7 (1), 17-22.
- Tabatabaei, M.H., Vitenberg, R. & Veeraragavan, N.R. (2023). Understanding blockchain: definitions, architecture, design, and system comparison. *Computer Science Review*, 50 (4).
- Tanenbaum, A.S. (1996). *Computer Networks* (3.Edition). New Jersey: Prentice Hall PTR.
- Tangem Team. (2023). Soft Fork vs Hard Fork: Definiton and Differences. *TANGEM*.  
<https://tangem.com/tr/blog/post/what-are-hard-forks-and-soft-forks/>.
- Tanrıverdi, M., Uysal, M. & Üstündağ, M.T. (2019). Blokzinciri Teknolojisi Nedir ? Ne Değildir?: Alanyazın İncelemesi. *Bilişim Teknolojileri Dergisi*, 12 (3), 203-217.
- Tapscott, D. & Tapscott, A. (2017). How Blockchain will change organizations. *MIT Sloan Management Review*, 58 (2), 9–13.
- Tekerek, M. (2008). Bilgi güvenliği yönetimi. *KSÜ Fen ve Mühendislik Dergisi*, 11 (1), 132-137).
- Terzi, S., & Şen, İ. K. (2015). Adli muhasebede hilelerin tespitinde yapay sinir ağı modelinin kullanımı. *Uluslararası İktisadi ve İdari İncelemeler Dergisi*, 7(14). 477-490.
- Terzi, S., Votis, K., Tzovaras, D., Stamelos, I., & Cooper, K. (2019). Blockchain 3.0 smart contracts in E-government 3.0 applications. *arXiv preprint arXiv:1910.06092*.
- Tetik, N. & Öner, A. (2020). Ülkemiz girişimcileri için yeni bir yatırım desteği modeli: initial coin offering (ICO). *Muhasebe ve Finans İncelemeleri Dergisi*, 3 (1), 13 – 26.

- Tim May'in Kripto Para Teknolojisini 1988'de Gördüğü Metin: Kripto Anarşist Manifestosu. *Eksiseyler*. <https://eksiseyler.com/tim-mayin-kripto-para-teknolojisini-1988de-gordugu-metin-kripto-anarsist-manifestosu>.
- Tokatlı, E. (2013). XBRL (Geliştirilebilir İşletme Raporlama Dili)'nin Muhasebe Bilgi Sistemine Etkileri. (Yayımlanmamış yüksek lisans tezi). Marmara Üniversitesi/Sosyal Bilimler Enstitüsü, İstanbul.
- Toplu, N., Calayoğlu, İ & Azaltun, M. (2021). Finansal bilgi manipülasyonu ortaya çıkarmaya yönelik bir araştırma (beneısh modeli). *MUFİDER*, 4 (1), 16 -25.
- Tornatzky, L. ve Fleischer, M. (1990). The processes of technological innovation. New-york:Lexington Books.
- Turan, Kenan. Dördüncü Sanayi Devriminin Uluslararası İlişkilere Sosyoekonomik Etkileri. Ege Üniversitesi SBE, *Yayınlanmamış Yüksek Lisans Tezi*. 2018.
- Turgut, A. (2022) Blokzincir Kabulünün Lojistik Performansa Etkileri: Türk Lojistik Firmalarında Bir Araştırma. (Yayımlanmamış doktora tezi). Alanya Alaaddin Keykubat Üniversitesi/Lisansüstü Eğitim Enstitüsü, Alanya.
- Türk Dil Kurumu Sözlükleri. <https://sozluk.gov.tr/>.
- Türkiye'nin Endüstri Platformu, <https://www.endustri40.com/endustri-tarihine-kisa-bir-yolculuk/>.
- Türkiye Muhasebe Standartları (TMS) : Kavramsal Çerçeve.
- Türkiye Muhasebe Standartları (TMS) 1: Finansal Tabloların Sunuluşu.
- Türkiye Sanayi ve İş Adamları Derneği (TÜSİAD). *Türkiye'nin Küresel Rekabetçiliği için Bir Gereklilik Olan Sanayi 4.0 Gelişmekte olan Ekonomi Perspektifi*. Mart 2016, Yayın No: TÜSİAD-T/2016-03/576. <http://www.tusiad.org/indir/2016/sanayi-40.pdf>.
- Tyra, J.M. (2014). *Triple Entry Accounting With Bitcoin*. <https://tyracpa.com/ethereum-hits-street/>.

- Uğurlu, M. & Sevim, Ş. (2015). Finansal tablolardaki hile riskinin tahmin edilmesinde karma modellerin nispi başarısı üzerine karşılaştırmalı bir analiz. *Gaziantep University Journal of Social Sciences*, 14 (1), 65-88.
- Ulucan Özkul, F. & Alkan, B. Ş. (2020). Dijital çağda muhasebenin dönüşümü: “Blockchain” teknolojisinde muhasebe ve mali controller. *Muhasebe Bilim Dünyası Dergisi*. 22 (2), 218-236.
- Understanding the BitGo Blockchain Services Layer. BITGO. <https://blog.bitgo.com/understanding-the-bitgo-blockchain-services-layer-2a054a5999b1>.
- Usta, A. & Doğanterkin, S. (2019). *Blockchain 101 v2*. Bankalararası Kart Merkezi.
- USUID. Sertifika. [https://acfetr.com/index.php?pg=sertifika\\_main](https://acfetr.com/index.php?pg=sertifika_main).
- Usul, H. (2013). *Türkiye Finansal Raporlama Standartları Uygulamalı Bağımsız Denetim*. Ankara: Detay Yayıncılık.
- Usul, H., & Topçuoğlu, M. (2011). Finansal Manipülasyonların Ortaya Çıkarılması ve Önlenmesinde Adli Muhasebenin Önemi: Türk Hukuk Sisteminde Var Olması Gerekliği Üzerine Bir Tartışma. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 16(3), 53-66.
- Uyar, S. & Yelgen, E. (2015). Bilgi ifşası (whistleblowing) ve denetim. *Yönetim ve Ekonomi Araştırmaları Dergisi*, 13 (1), 85-106.
- Uysal, Ö. (2011). Ağ Topolojileri. Abdullah Kuzu (Ed.), *Bilgisayar Ağları ve İletişim* (2. Baskı) içinde (s. 1-33). Ankara: Nobel.
- Ünkaracalar, T. (2021). Muhasebe, Finans ve Denetim Alanlarında Yenilikçi Yaklaşımlar. Yakup Aslan. (Ed.), *Denetim Sektörü ile Blokzincir Teknolojisinin Entegrasyonu* (1. Baskı) içinde (s.75-93). İstanbul: Efe Akademi Yayınevi.
- Ünsal, E. & Kocaoğlu, Ö.(2018). Blok zinciri teknolojisi: Kullanım alanları, açık noktaları ve gelecek beklentileri. *Avrupa Bilim ve Teknoloji Dergisi*, (13), 54-64.

- Üzer, B. (2017). Sanal Para Birimleri. (Uzmanlık yeterlik tezi) Türkiye Cumhuriyet Merkez Bankası Ödeme Sistemleri Genel Müdürlüğü, Ankara.
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, 46 (2), 186-204.
- Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User acceptance of information technology: Towards a unified view. *MIS Quarterly* 27 (3). 479–501.
- Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, 39(2), 273-315.
- Venkatesh, V., Thong, J.Y.L. & Xu. X. (2012). Consumer Acceptance And Use Of Information Technology: Extending The Unified Theory Of Acceptance And Use Of Technology. *MIS Quarterly* 36 (1). 157-178.
- Vondráčková, A. (2016). Regulation of virtual currency in the European Union. *Prag Law Working Papers Series III/3*.
- Walker, M., 2013. How far can we trust earnings numbers? What research tells us about earnings management. *Account. Bus. Res.* 43 (4), 445–481.
- Wang, C., Jiang, H., Zeng, J., Yu, M., Huang, Q. & Zuo, Z. (2021). A review of blockchain layered architecture and technology application research. *Wuhan University Journal of Natural Science*, 26 (5), 415-428.
- Wang, Y. & Kogan, A. (2018). Designing confidentiality-preserving Blockchain-based transaction processing systems. *International Journal of Accounting Information Systems*, 30, 1-18.
- Wolfe, D.T. & Hermanson, D.R. (2004). The fraud diamond: considering the four elements of fraud. *The CPA Journal*, 74, 38-42.
- Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. (Yellow Paper) *GitHub Pages*. <https://ethereum.github.io/yellowpaper/paper.pdf>.
- Wüst, K. & Gervais, A. (2018). Do you need a Blockchain? *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 45-54.

- Yaga, D., Mell, P., Roby, N. & Scarfone, K. (2018). *National Institute of Standards and Technology Internal Report (NISTIR) 8202 : Blockchain Technology Overview*.
- Yaman, T. (2008). *Finansal Tablolar Aracılığı ile Kullanıcılara Yanıltıcı Bilgi Sunulması Ve Sonuçları*. (Yayımlanmamış doktora tezi). Marmara Üniversitesi/Sosyal Bilimler Enstitüsü, İstanbul.
- Yanar, H.İ., Çetin, M.Ş. & Kılıç, V. (2022). Devletsiz yönetişimin yeni ekonomik enstrümanı: Kripto para ve geleceği. *Kırıkkale Üniversitesi Sosyal Bilimler Dergisi*, 12 (1), 23-48.
- Yaylalı, İ. (2024). Yönetim ve Çalışan Hilelerinin Önlenmesinde Hile Denetiminin Önemi Üzerine Bir Değerlendirme. *İşletme*, 5(1), 105-131.
- Yermack, D. (2017). Corporate governance and blockchains, *Review of Finance*, 21(1), 7-31.
- Yıldız, E. & Baskan, D. T. (2014). Muhasebe hilelerinin önlenmesinde kullanılan araçlar: bist şirketleri üzerine bir araştırma. *Muhasebe ve Finansman Dergisi*, Nisan (62), 1-18.
- Yılmaz, E. (2022). Bitcoin Siyaseti ve Tekno-Ekonomik Hayalleri. *International Journal of Social, Humanities and Administrative Sciences (JOSHAS)*, 8 (50), 410-420.
- Yılmaz, G. (2014). Suistimali Önlemede 10 Yöntem. *USİUD*. [https://acfetr.com/index.php?pg=topluluk\\_makaledetay&qsicerikid=251](https://acfetr.com/index.php?pg=topluluk_makaledetay&qsicerikid=251).
- Yılmaz, G. (2019). *Hilenin Önlenmesi ve Tespitinde Büyük Veri Analitiğinin Kullanımı ve Türkiye'deki Çalışan Hileleri Üzerine Bir Araştırma*. (Yayımlanmamış doktora tezi). Marmara Üniversitesi/Sosyal Bilimler Enstitüsü, İstanbul.
- Yılmaz, S. (2023). Hash Fonksiyonu (Hash Function) Nedir? *METATIME*. <https://metatime.com/tr/blog/hash-fonksiyonu-hash-function-nedir>
- Yli-Hummo, J. Vd. (2016). Where are Current Researches in Blokchain Technology? A Systematic Review. *Plos One*, 1-27.



- Young, M.R. (2002). *Accounting Irregularities and Financial Fraud, A Corporate Governance Guide*. (2. Edition). Aspen Law & Business.
- Yu, T., Lin, Z., Tang, Q. (2018). Blockchain: The Introduction and Its Application in Financial Accounting. *The Journal Of Corporate Accounting & Finance*. October. 37-47.
- Yurdabak, M.K. (2022). *Blokzincir Uygulamalarında Akış Deneyiminin Online Satın Alma Niyetine Etkisi Üzerine Bir Araştırma*. Marmara Üniversitesi/Sosyal Bilimler Enstitüsü, İstanbul.
- Zhai, S., Yang, Y., Li, J., Qui, C. & Zhao, J. (2019). Research on the application of cryptography on the blockchain. *Journal of Physics: Conference Series*, 1168 (3), 032077.
- Zheng, R. (2021). Applications research of blockchain technology in accounting system. *In Journal of Physics: Conference Series*, 1955 (1), 012068- 012077.
- Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *EEE 6th International Congress on Big Data*, 557-564.
- Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. (2018). Blockchain Challenges and Opportunities: A Survey. *International Journal of Web and Grid Services*, 14 (4), 352-375.
- Zheng, W., Zheng, Z., Chen, X., Dai, K., Li, P., & Chen, R. (2019). Nutbaas: A blockchain-as a-service platform. *IEEE Access*, 7, 1-12.
- 1 No.lu Muhasebe Sistemi Uygulama Genel Tebliği (MSUGT).
- 5018 Sayılı Kamu Malî Yönetimi ve Kontrol Kanunu.
- 6362 Sayılı Sermaye Piyasası Kanunu.
- 6493 Sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun.

## Ek A

### ETİK KURUL KARARI



T.C.  
ALTINBAŞ ÜNİVERSİTESİ REKTÖRLÜĞÜ

Sayı : E-96136591-050.06.04-47183  
Konu : Kararlar

19.07.2023

#### DAĞITIM YERLERİNE

Üniversitemiz Bilimsel Araştırma ve Yayın Etik Kurulu'nun 17.07.2023 tarihli ve 2023/18 sayılı toplantısında alınan karar ekte yer almakta olup, bilgilerini ve gereğini rica ederim.

Prof.Dr. Çağrı ERHAN  
Vekil Rektör

Ek:ETİK ONAY 2023-18 (2 Sayfa)

Dağıtım:  
Lisansüstü Eğitim Enstitüsü Müdürlüğüne  
Prof.Dr. Saim KILIÇ  
Aysegul Guner ALGAN  
Dr.Öğr.Üyesi Duygu TAŞFİLİZ

Bu belge, görevli elektronik imza ile imzalanmıştır.

Belge Doğrulama Kodu :BISM3ZD28M2

Belge Takip Adresi : <https://www.makkiye.gov.tr/altinbas-universitesi-ebys>

Adres:Mahmutbey Döğmenler Caddesi, No:26, 34217 Bağcılar - İstanbul  
Telefon:(0 212) 604 01 00 Faks:(0 212) 445 81 71  
e-Posta:info@altinbas.edu.tr Web: <http://www.altinbas.edu.tr/>  
Kep Adresi:altinbasuniversitesi@be01.kep.tr

Bilgi için: Saim KILIÇ  
Unvanı: Kurul Başkanı  
Tel No: (0 212) 604 01 00



**ALTINBAŞ ÜNİVERSİTESİ**  
**BİLİMSEL ARAŞTIRMA VE YAYIN ETİK KURUL TOPLANTISI**  
**KARAR TUTANAĞI**

**Toplantı No:** 2023/18

**Toplantı Tarihi:** 17/07/2023

**Toplantı Yeri:** Çevirim içi

**Kurul Başkan ve Üyeleri:**

Prof. Dr. Saim KILIÇ -İşletme Fakültesi/Öğretim Üyesi- Başkan

Prof. Dr. Osman Nuri UÇAN -Uygulamalı Bilimler Fakültesi/Öğretim Üyesi -Üye

Prof. Dr. Dilek ŞİRVANLI ÖZEN-İktisadi, İdari ve Sosyal Bilimler Fakültesi Dekan- Üye

Doç. Dr. Nuray YILMAZ ALTINTAŞ- Dış Hekimliği Fakültesi/Öğretim Üyesi- Üye

Doç. Dr. Hasan SINAR -Hukuk Fakültesi/Öğretim Üyesi- Üye

Doç. Dr. Yasa EKŞİOĞLU ÖZOK- Mühendislik ve Mimarlık Fakültesi/Öğretim Üyesi- Üye

Dr. Öğr. Üyesi Gaye HAFEZ -Eczacılık Fakültesi/Öğretim Üyesi- Üye

Dr. Öğr. Üyesi Yalda HEKMATSHOAR -Tıp Fakültesi/Öğretim Üyesi -Üye

Dr. Öğr. Üyesi Leyla ULUSMAN- Güzel Sanatlar ve Tasarım Fakültesi/Öğretim Üyesi-Üye

Doç. Dr. Hakan KAYGUSUZ- Bilimsel Araştırma ve Projeler Daire Başkanı- Üye

**Kararlar:**

1.

2.

3. Üniversitemiz İşletme Fakültesi'nde görev yapmakta olan **Prof. Dr. Saim Kılıç**'in tez danışmanlığını yaptığı İşletme Doktora Programı öğrencisi **Selmin Gürdal Çelik**'in *"Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu (Muhasebe Hilelerini) Azaltmada Kullanılması: Türkiye'deki Mali Müşavirler Üzerine Ampirik Araştırma"* başlıklı doktora tezi kapsamında anket/ölçek/soru yoluyla veri toplama önerisi

görüldü. Araştırmanın bilimsel içeriği, metodolojisi, orijinalliği ve kaynakları etik onay kapsamı dışında olup, başvuru sahibinin sunduğu belgeler ışığında "belirtilen yöntemle veri toplamada ve araştırma yapmada herhangi bir sakınca bulunup bulunmadığı" hususuyla ilgili değerlendirme yapıldı. Bu yönüyle yapılan değerlendirmede, araştırma önerisinde etiğe aykırı unsurlar tespit edilmediğinden uygun bulunmasına ve Rektörlük Makamına arz edilmesine karar verildi\*. (Saim Kılıç bu madde görüşülürken müzakereye/oylamaya katılmamıştır.)

4.

**e-imza**  
Prof. Dr. Saim KILIÇ  
Başkan

**e-imza**  
Prof. Dr. Osman Nuri UÇAN  
Üye

**e-imza**  
Prof. Dr. Dilek ŞİRVANLI ÖZEN  
Üye

**e-imza**  
Doç. Dr. Nuray YILMAZ ALTINTAŞ  
Üye

**e-imza**  
Doç. Dr. Hasan SINAR  
Üye

**e-imza**  
Doç. Dr. Yasa EKŞİOĞLU ÖZOK  
Üye

**e-imza**  
Dr. Öğr. Üyesi Gaye HAFEZ  
Üye

**e-imza**  
Dr. Öğr. Üyesi Yalda HEKMATSHOAR  
Üye

**e-imza**  
Dr. Öğr. Üyesi Leyla ULUSMAN  
Üye

**e-imza**  
Doç. Dr. Hakan KAYGUSUZ  
Üye

## EK B

### ANKET FORMU

Sayın Meslek Mensubu;

Altınbaş Üniversitesi İşletme Fakültesi öğretim üyesi Değerli Hocam Prof. Dr. Saim KILIÇ danışmanlığında yürütmüş olduğum **“Blokzincir Teknolojisinin Finansal Bilgi Manipülasyonunu (Muhasebe Hilelerini) Azaltmada Kullanılması : İstanbul’daki Mali Müşavirler Üzerine Ampirik Araştırma”** konulu doktora tezi çalışmam için araştırma yapmaktayım. Araştırmaya dayanak olacak anket uygulamasında, Teknoloji Kabul Modeli (TKM) ve Hile Araştırmaları ölçekleri kullanılacaktır. *Kişisel Verileri Koruma Kanunu* (KVKK) hükümlerine uygun olarak anket kapsamında vereceğiniz bilgiler gizli tutulup anket sonucunda çıkan bulgular kişi, kurum veya kuruluşları bağlayıcı nitelikte olmayacak sadece bilimsel amaç için kullanılacaktır. Aşağıdaki ankete katılımda gönüllülük esas olup katılmanız halinde 2-3 dakika sürecek anket sorularına doğru ve samimi cevaplar vermeniz araştırmanın geçerliliği ve doğru sonuçlara ulaşılması açısından büyük önem arz etmektedir. Değerli vaktinizi ayırdığınız ve akademik bir çalışmaya destek verdiğiniz için teşekkür eder, çalışmalarınızda başarılar dilerim.

Saygılarımla.

SMMM Selmin ÇELİK GÜRDAL

### ANKET FORMU

#### BÖLÜM 1 : Demografik Bilgiler

1- Cinsiyetiniz

☐ Kadın

☐ Erkek

2- Eğitim durumunuz

☐ Lise

☐ Lisans

☐ Yüksek Lisans

☐ Doktora

3- Mesleki unvanınız

☐ Serbest Muhasebeci Mali Müşavir (SMMM)

☐ Yeminli Mali Müşavir (YMM)

4- Çalışma şekliniz

☐ Bağımlı

☐ Bağımsız

5- Mesleki tecrübeniz

☐ 1-5 yıl

☐ 6-10 yıl

☐ 11-15 yıl

☐ 16-20 yıl

☐ 21 yıl ve üzeri

6- Mükellef sayınız

☐ 1-5

☐ 6-10

☐ 11-20

☐ 21-30

☐ 31 ve üzeri

7- Blokzincir teknolojisi hakkındaki bilgi düzeyiniz

☐ Bilgim yok

☐ Çok az

☐ Orta

☐ İyi

☐ İleri

## BÖLÜM 2 : Teknolojik Ürün Kullanma Sıklığı

### 1- Mesleki Teknolojik ürünlerden haberdar olma kaynağınız

- ☐ Meslektaşlarımdan ☐ Sosyal çevreden ☐ Meslek Odalarından ☐ Diğer çeşitli kaynaklardan

### 2- Yeni teknolojik ürünlerin gündelik hayattaki önem düzeyi (Akıllı Telefon, Laptop, Pc, vb. gibi)

- ☐ Çok önemli ☐ Önemli ☐ Önemsiz ☐ Çok önemsiz

### 3- Mesleki araştırmalarda teknolojik ürünleri kullanma sıklığı ( E Defter, E Fatura, E Arşiv, vb. gibi)

- ☐ Her gün ☐ Haftada bazı günler ☐ Haftada birkaç gün ☐ Çok nadir

### 4- Teknolojik ürünlerin mesleki araştırmalardaki önemi

- ☐ Çok önemli ☐ Önemli ☐ Önemsiz ☐ Çok önemsiz ☐ Kararsızım

### 5- Mesleki teknoloji ürünlerin satın alınması için bütçe oluşturma sıklığınız

- ☐ Her yıl ☐ Her ay ☐ İhtiyaç olduğunda ☐ Yeni bir ürün üretildiğinde

### 6- Genel bir teknolojik ürün satışa çıktığında (Akıllı Telefon, Laptop, Pc vb):

- ☐ Hemen satın alırım ☐ Birkaç ay beklerim ☐ İhtiyaç olduğunda satın alırım ☐ Satın almam

### 7- Mesleki teknoloji ürünlerinin kullanılması hakkında teknik destek alımı (Akıllı Telefon,Laptop, Pc

- ☐ Arkadaşlarımdan ☐ Program satıcılarımdan ☐ Meslektaşlarımdan ☐ Meslek odalarından

### 8- Gündelik hayatta akıllı telefon kullanma sıklığınız:

- ☐ 0-1 saat ☐ 1-3 saat ☐ 3-5 saat ☐ 5 saat ve üzeri

### 9- İş hayatında internette işlem yapma sıklığınız:

- ☐ Her gün ☐ Nadiren ☐ Kullanmıyorum ☐ İnternet kullanmıyorum

### 10- İş hayatınızda teknolojik ürünleri kullanmak zorunda olduğunuz mükellef sayısı (E-Arşiv, E-Fatura, E-Defter, E-İrsaliye vb.):

- ☐ 1-20 ☐ 21-40 ☐ 41-60 ☐ 60 ve üzeri

### 11- Blokzincir teknolojisinin muhasebe alanında benimsenmesinde en büyük engel

- ☐ Kamunun direnci ☐ Müşterinin direnci ☐ Sektörün direnci ☐ Meslektaşın direnci

| BÖLÜM 3 : Blokzincir Teknolojisinin Muhasebe Mesleğine Etkisi                                                                                                               |  | Hic Katılmıyorum | Katılmıyorum | Kararsızım | Katılıyorum | Tamamen Katılıyorum |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|------------------|--------------|------------|-------------|---------------------|
| <b>ENGELLER</b>                                                                                                                                                             |  |                  |              |            |             |                     |
| Blokzincir teknolojinin muhasebe alanında benimsenmesinde en büyük engel <b>yetenekli iş gücüdür.</b>                                                                       |  |                  |              |            |             |                     |
| Blokzincir teknolojinin muhasebe alanında benimsenmesinde en büyük engel <b>data güvenliğidir.</b>                                                                          |  |                  |              |            |             |                     |
| Blokzincir teknolojinin muhasebe alanında benimsenmesinde en büyük engel <b>mevcut sistem ve yapılarına uyum güçlüğüdür.</b>                                                |  |                  |              |            |             |                     |
| Blokzincir teknolojinin muhasebe alanında benimsenmesinde en büyük engel <b>karmaşık süreçler gerektirmesidir.</b>                                                          |  |                  |              |            |             |                     |
| Blokzincir teknolojinin muhasebe alanında benimsenmesinde en büyük engel <b>stratejik öneminin anlaşılmasındır.</b>                                                         |  |                  |              |            |             |                     |
| Blokzincir teknolojinin muhasebe alanında benimsenmesinde en büyük engel <b>iş gücünün ve orta düzey yöneticilerin blokzincir teknolojisine karşı direnç göstermesidir.</b> |  |                  |              |            |             |                     |
| Blokzincir teknolojinin muhasebe alanında benimsenmesinde en büyük engel <b>firma büyüklüğüdür.</b>                                                                         |  |                  |              |            |             |                     |
| Blokzincir teknolojinin muhasebe alanında benimsenmesinde en büyük engel <b>ilk yatırım maliyetleridir.</b>                                                                 |  |                  |              |            |             |                     |
| Blokzincir teknolojinin muhasebe alanında benimsenmesinde en büyük engel <b>rekabete katkısının algılanamamasıdır.</b>                                                      |  |                  |              |            |             |                     |
| Blokzincir teknolojinin muhasebe alanında benimsenmesinde en büyük engel <b>dijital yetenek eksikliğidir.</b>                                                               |  |                  |              |            |             |                     |
| <b>ALGILANAN FAYDA</b>                                                                                                                                                      |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini kullanmak <b>iş performansını geliştirir.</b>                                                                                               |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini kullanmak <b>işimdeki üretkenliği artırır.</b>                                                                                              |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini kullanmak <b>iş etkinliğimi artırır.</b>                                                                                                    |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini işimde kullanmayı <b>yararlı buluyorum.</b>                                                                                                 |  |                  |              |            |             |                     |
| <b>ALGILANAN KULLANIM KOLAYLIĞI</b>                                                                                                                                         |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini kullanmak <b>açık ve anlaşılırdır.</b>                                                                                                      |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini kullanmak <b>çok fazla zihinsel çaba gerektirmemektedir.</b>                                                                                |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini kullanmak <b>kolaydır.</b>                                                                                                                  |  |                  |              |            |             |                     |
| <b>TUTUM</b>                                                                                                                                                                |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini işimde kullanmak <b>beni mutlu eder.</b>                                                                                                    |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini işimde kullanmak <b>beni gerginleştirir.</b>                                                                                                |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini işimde kullanımım <b>bezdirci olduğunu düşünüyorum.</b>                                                                                     |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini işimde kullanımımı <b>gereksiz buluyorum.</b>                                                                                               |  |                  |              |            |             |                     |
| <b>NİYET</b>                                                                                                                                                                |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini işimde kullanacağımı <b>tahmin ediyorum.</b>                                                                                                |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini işimde kullanmayı <b>planlıyorum.</b>                                                                                                       |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini işimde kullanacağımı <b>tahmin ediyorum.</b>                                                                                                |  |                  |              |            |             |                     |
| <b>DAVRANIŞ</b>                                                                                                                                                             |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini <b>sık sık kullanmaktayım.</b>                                                                                                              |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünleri <b>olmadan ve rimli çalışmam.</b>                                                                                                             |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini <b>kullanmam.</b>                                                                                                                           |  |                  |              |            |             |                     |
| Blokzincir teknoloji ürünlerini <b>seyrek kullanırım.</b>                                                                                                                   |  |                  |              |            |             |                     |

|                                                                                               | 1            | 2       | 3     | 4       | 5         |
|-----------------------------------------------------------------------------------------------|--------------|---------|-------|---------|-----------|
| <b>BÖLÜM 4 : Hile Belirtileri Görülen İşlemler ve Hile Belirtileri İle Karşılaşma Sıklığı</b> | Hiçbir zaman | Nadiren | Bazen | Sıkıkla | Her zaman |
| Çek düzenleme işlemlerinde hile belirtileri                                                   |              |         |       |         |           |
| Fatura düzenleme işlemlerinde hile belirtileri                                                |              |         |       |         |           |
| Satışlar ve satış iadeleri işlemlerinde hile belirtileri                                      |              |         |       |         |           |
| Bordro düzenleme işlemlerinde hile belirtileri                                                |              |         |       |         |           |
| Çeşitli gider ödemeleri işlemlerinde hile belirtileri                                         |              |         |       |         |           |
| Stoklar ve duran varlıklar işlemlerinde hile belirtileri                                      |              |         |       |         |           |
| Banka havaaleleri işlemlerinde hile belirtileri                                               |              |         |       |         |           |
| Nakit ödemeler/taahhütler işlemlerinde hile belirtileri                                       |              |         |       |         |           |
| Envanter ve satın alma işlemlerinde hile belirtileri                                          |              |         |       |         |           |
| Borç ve ödeme işlemlerinde hile belirtileri                                                   |              |         |       |         |           |
| Alacak ve tahsilat işlemlerinde hile belirtileri                                              |              |         |       |         |           |
| Belge ve kayıt düzeninde hile belirtileri                                                     |              |         |       |         |           |

|                                                                              | Hiç Katılmıyorum | Katılmıyorum | Kararsızım | Katılıyorum | Tamamen Katılıyorum |
|------------------------------------------------------------------------------|------------------|--------------|------------|-------------|---------------------|
| <b>BÖLÜM 5 : Muhasebe Hilelerinin Önlenmesine Yönelik Faaliyetler</b>        |                  |              |            |             |                     |
| Muhasebe hilelerinin önlenmesinde hangisi veya hangileri faydalı olmaktadır? |                  |              |            |             |                     |
| İç denetim                                                                   |                  |              |            |             |                     |
| İç kontrol                                                                   |                  |              |            |             |                     |
| Bağımsız denetim                                                             |                  |              |            |             |                     |
| İhbar hatları                                                                |                  |              |            |             |                     |
| Bilgi teknolojileri denetimi                                                 |                  |              |            |             |                     |
| Tesadüf                                                                      |                  |              |            |             |                     |
| Özel hile incelemeleri                                                       |                  |              |            |             |                     |
| Veri madenciliği teknikleri                                                  |                  |              |            |             |                     |
| XBRL Raporlama Dili                                                          |                  |              |            |             |                     |
| Hile ve suistimal denetimleri                                                |                  |              |            |             |                     |
| YMMlerce yürütülen tam tasdik çalışmalarındaki denetim faaliyetleri          |                  |              |            |             |                     |
| Blokszincir teknolojisi                                                      |                  |              |            |             |                     |
| Diğer                                                                        |                  |              |            |             |                     |

|                                                                                                            | Hiç Katılmıyorum | Katılmıyorum | Kararsızım | Katılıyorum | Kesinlikle Katılıyorum |
|------------------------------------------------------------------------------------------------------------|------------------|--------------|------------|-------------|------------------------|
| <b>BÖLÜM 6 : Blokszincir Teknolojisinin Muhasebe Hilelerini Önlemedeki Rolü</b>                            |                  |              |            |             |                        |
| Muhasebe bilgi sisteminin blokszincir tabanlı olması muhasebe bilgilerinin güvenilirliğini olumlu etkiler. |                  |              |            |             |                        |
| Blokszincir tabanlı mali denetim vergi mükelleflerinin hileli finansal raporlama eğilimini engeller.       |                  |              |            |             |                        |
| Blokszincir tabanlı mali denetim devletin vergi gelirlerini artırır.                                       |                  |              |            |             |                        |
| Blokszincir tabanlı mali raporlama finansal sistemin şeffaflığını olumlu etkiler.                          |                  |              |            |             |                        |
| Muhasebe bilgi sisteminin blokszincir tabanlı olması finansal bilgilerin mahremiyetini zedeler.            |                  |              |            |             |                        |
| Finansal bilgilerin blokszincir üzerinden denetlenmesi ekonomik sistemi olumlu etkiler.                    |                  |              |            |             |                        |
| Blokszincir teknolojisi işlemlerin kontrol ve denetimini yapmayı kolaylaştırır.                            |                  |              |            |             |                        |
| Blokszincir teknolojisi elektronik beyannameleri kolay bir şekilde hazırlama imkânı sunar.                 |                  |              |            |             |                        |
| Muhasebe verilerinin güvenliği, kayıt ve dosyalama sisteminin güvencesine bağlıdır.                        |                  |              |            |             |                        |
| Muhasebe yazılımlarında geriye dönük işlem yapılmasında sakınca yoktur.                                    |                  |              |            |             |                        |
| Blokszincir teknolojisi hileli işlemleri ortaya çıkarabilir.                                               |                  |              |            |             |                        |