T.C.
İSTANBUL ÜNİVERSİTESİ-CERRAHPAŞA
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

# BLOK ZİNCİR VE FİNANSAL TEKNOLOJİ ÇÖZÜMLERİ İÇİN UYGULAMALARI

Hatice KARAYILAN

DANIŞMAN
Dr. Öğr. Üyesi Gülsüm Zeynep GÜRKAŞ AYDIN

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

İSTANBUL-2019

Bu çalışma 01.07.2019 tarihinde aşağıdaki jüri tarafından Bilgisayar Mühendisliği Anabilim Dalı, Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı Yüksek Lisans Tezi olarak kabul edilmiştir.

TEZ JÜRİSİ

Dr.Öğr.Üyesi Gülsüm Zeynep GÜRKAŞ AYDIN
İstanbul Üniversitesi-Cerrahpaşa
Mühendislik Fakültesi

Dr.Öğr.Üyesi Oğuzhan ÖZTAŞ
İstanbul Üniversitesi-Cerrahpaşa
Mühendislik Fakültesi

Dr.Öğr.Üyesi Akhan AKBULUT
İstanbul Kültür Üniversitesi
Mühendislik Fakültesi

20.04.2016 tarihli Resmi Gazete'de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince; Bu Lisansüstü teze, İstanbul Üniversitesi-Cerrahpaşa'nın abonesi olduğu intihal yazılım programı kullanılarak Lisansüstü Eğitim Enstitüsü'nün belirlemiş olduğu ölçütlere uygun rapor alınmıştır.

# ÖNSÖZ

Son yıllarda, bilişim teknolojilerinin hızlı gelişimiyle birlikte, finansal hizmetler daha kullanıcı dostu haline getirilerek tüketicilerin finansal hizmetlere erişimi yeni yollardan sağlanmaktadır. Blok zincir teknolojisi de finansal hizmetler için bir çözüm olarak uygulanmaya başlanan yeni teknolojiler arasındadır. Ancak blok zincir teknolojisi henüz gelişim aşamasındadır, potansiyeli ve etkileri hakkındaki araştırmalar devam etmektedir.

Bu tez çalışmasında, blok zincir alt yapısının, temel bileşenlerinin, finansal teknolojiler için nasıl kullanıldığının, mevcut platformlarının ve uygulamalarının, blok zincir uygulamalarında karşılaşılan zorlukların ve güvenliğinin incelenmesi planlanmaktadır. Bunların yanında, finansal teknoloji hizmetleri için gelecekte yaygın olarak blok zincir teknolojisi kullanılması beklenen alanlardaki uygulamaları hakkında bilgi verilmesi ve finansal hizmetlerin sağlanmasında önemli bir rolü olan KYC çözümleri için blok zincir teknolojisinin nasıl uygulanabileceğinin ve sağlayabileceği faydaların anlaşılması amaçlanmaktadır.

Yüksek lisans eğitimim boyunca bana yol gösteren Dr. Öğr. Üyesi Muhammed Ali AYDIN'a ve tez çalışmalarım boyunca güler yüzü ve tecrübeleriyle bana yol gösteren danışmanım Dr. Öğr. Üyesi Gülsüm Zeynep GÜRKAŞ AYDIN'a saygı ve şükranlarımı sunuyorum.

Çalışmalarım boyunca beni sabırla destekleyen ve yardımlarını esirgemeyen sevgili aileme sonsuz teşekkürlerimi sunuyorum.

Temmuz 2019 Hatice KARAYILAN

# İÇİNDEKİLER

**Sayfa No**

# ŞEKİL LİSTESİ

**Sayfa No**

# TABLO LİSTESİ

**Sayfa No**

# SİMGE VE KISALTMA LİSTESİ

| Kısaltmalar | Açıklama |
|---|---|
| **AI** | : Artificial Intelligence - Yapay Zeka |
| **AML** | : Anti Money Laundering - Kara Para Aklamayı Önleme |
| **API** | : Application Programming Interface - Uygulama Programlama Arayüzü |
| **DAO** | : Decentralized Autonomous Organization - Merkezi Olmayan Özerk Organizasyon |
| **DLT** | : Distributed Ledger Technology - Dağıtılmış Defter Teknolojisi |
| **e-KYC** | : Electronic Know Your Customer - Dijital Müşterini Tanı |
| **ETH** | : Ethereum - Ethereum Blok Zincirinin Kripto Para Birimi |
| **EVM** | : Ethereum Virtual Machine - Ethereum Sanal Makinesi |
| **Gwei** | : 0.000000001 ETH |
| **HTTP** | : Hyper-Text Transfer Protocol - Hiper-Metin Transfer Protokolü |
| **IoT** | : Internet of Things - Nesnelerin İnterneti |
| **IPC** | : Interprocess Communication |
| **KYC** | : Know Your Customer - Müşterini Tanı |
| **ms** | : Milisaniye |
| **NIST** | : National Institute of Standards and Technology - Ulusal Standartlar ve Teknoloji Enstitüsü |
| **NSA** | : National Security Agency - Ulusal Güvenlik Ajansı |
| **P2P** | : Peer-to-Peer - Uçtan Uca |
| **PBFT** | : Practical Byzantine Fault Tolerance - Bizans Hata Toleransı |
| **PoA** | : Proof of Authority - Otorite Kanıtı |
| **PoS** | : Proof of Stake - Hisse Kanıtı |
| **PoW** | : Proof of Work - İş Kanıtı |
| **SHA** | : Secure Hash Algortihm |
| **SPOF** | : Single Point of Failure - Tek Hata Noktası |
| **XRP** | : Ripple'ın Kripto Para Birimi |

# ÖZET

## YÜKSEK LİSANS TEZİ

### BLOK ZİNCİR VE FİNANSAL TEKNOLOJİ ÇÖZÜMLERİ İÇİN UYGULAMALARI

**Hatice KARAYILAN**

**İstanbul Üniversitesi-Cerrahpaşa**

**Lisansüstü Eğitim Enstitüsü**

**Bilgisayar Mühendisliği Anabilim Dalı**

**Danışman : Dr. Öğr. Üyesi Gülsüm Zeynep GÜRKAŞ AYDIN**

Gelişen bilişim teknolojileri ile birlikte finansal hizmetler sektöründe pek çok yenilik yaşanmaktadır. Finansal hizmetlerin geliştirilmesi için kullanılan yeni teknolojilerden birisi blok zincir teknolojisidir. Blok zincir teknolojisi, güvenlik ve değişmezlik ilkeleriyle oluşturulmuş dağıtılmış veritabanı sayesinde aracılara olan ihtiyacı ortadan kaldırarak finansal hizmetler sektörü için pek çok avantaj sağlamaktadır. Dijital kimlik yönetimi ve müşterini tanı (KYC) çözümleri blok zincirin finansal hizmetleri kolaylaştırması için kullanılması üzerinde araştırmalar yapılan alanlardandır. Bu tez çalışmasında, finans kuruluşların dahil olduğu iki farklı KYC modelinin uygulaması blok zincir üzerinde geliştirilmiş ve bu modeller karşılaştırılmıştır. Modeller tasarlanırken kimlik verilerinin tüm düğümlere kopyalanmasının güvenlik riskini artıracağı ve blok zincirin silinemez olması sebebiyle veri sahibinin verilerini tamamen yok edemeyecek olmasının kişisel verilerin korunması hakkındaki yasa ve düzenlemelere aykırılık oluşturacağı değerlendirilmiştir. Kişisel veriler içeren KYC sistemlerinin özel veya konsorsiyum blok zincir modelleri olarak tasarlanması ve kimlik bilgilerinin blok zincir dışında bir ilişkisel veritabanında saklanması ile hem kişisel verileri koruma düzenlemelerine uyumun sağlanabileceği hem de güvenliğin ve performansın artırılabileceği sonucuna ulaşılmıştır.

Temmuz 2019, 68 sayfa.

**Anahtar kelimeler:** Blok zincir, DLT, dijital kimlik, KYC, kendine egemen kimlik

# SUMMARY

## M.Sc. THESIS

### BLOCKCHAIN AND ITS APPLICATIONS FOR FINANCIAL TECHNOLOGY SOLUTIONS

**Hatice KARAYILAN**

**Istanbul University-Cerrahpasa**

**Institute of Graduate Studies**

**Department of Computer Engineering**

**Supervisor : Assist. Prof. Dr. Gülsüm Zeynep GÜRKAŞ AYDIN**

With the improving information technologies, many innovations are experienced in the financial services industry. One of the new technologies used for the advancement of financial services is blockchain. Blockchain provides many advantages for the financial services with its distributed database provided by its principles of security and immutability by eliminating the need for intermediaries. Identity management and KYC are from the areas where research has been carried out on the use of blockchain to facilitate financial services. In this thesis, the application of two different KYC models are developed on blockchains and then these models are compared. When designing the models, it was considered that copying the identity data to all nodes would increase the security risk. It was also considered that blockchains immutability will cause violating the regulations on the protection of personal data because the owner will not be able to destroy own data. It was concluded that KYC applications which contain personal data should be designed as private or consortium blockchain models and the identity data should be stored in a relational database outside the blockchain. This will ensure compliance with personal data protection regulations and increase security and performance.

July 2019, 68 pages.

**Keywords:** Blockchain, DLT, digital identity, KYC, self-sovereign identity

# 1. GİRİŞ

Finansal hizmetler son yıllarda gerçekleşen teknolojik gelişmelerden önemli ölçüde etkilenmektedir. Bu gelişmelerle birlikte karşımıza Fintech: Finansal Teknoloji kavramı çıkmıştır. Pek çok girişimci gelişen bilişim teknolojilerinden faydalanarak finansal hizmetlere yenilikler getirmektedir. Finansal hizmetlerin geliştirilmesinde kullanılan yeni teknolojilerden birisi de blok zincir teknolojisidir. Geleneksel olarak, finansal işlemlerin gerçekleştirilmesi için merkezi bir otoriteye veya aracıya ihtiyaç duyulmaktadır. Blok zincir mimarisi, dağıtılmış bir bilgisayar ağının bir aracıya ihtiyaç duymadan fikir birliğine ulaşıp işlemlerin gerçekleştirilmesini sağlamaktadır.

Bilişim teknolojilerindeki yenilikler ile alternatif iletişim protokollerinin ve yazılım mimarilerinin gelişimi sayesinde uçtan uca iletişim ile merkezi olmayan bir sistem oluşturulabilmektedir. Belirli bir merkez olmadan eşler arasında iletişim sağlayan şifrelenmiş veriler ve dağıtık bir sistem yapısına sahip yeni bir teknoloji olarak blok zincir bu alanda öne çıkmaktadır. Blok zincir, işlemlerin bir dijital kayıt defterinin oluşturulmasını ve dağıtılmış bir bilgisayar ağı arasında paylaşılmasını mümkün kılan bir veri yapısıdır. Blok zincir, merkezi bir otoriteye gerek kalmaksızın, ağdaki her bir katılımcı tarafından, şifreleme kullanılarak kayıt defterinin güvenli bir şekilde işlenmesini sağlamaktadır.

Bu tez kapsamında öncelikle, Fintech kavramı ve gelişen bilişim teknolojilerinin finansal hizmetlere etkisi açıklanmış, teknolojide yaşanan gelişmelerle birlikte son yıllarda finansal teknolojiler için kullanılmaya başlanan blok zincirin temelleri anlatılmış, örnek uygulamaları ve çeşitli açılardan zorlukları incelenmiştir.

Daha sonra, blok zincirin gelecekte yaygın olarak kullanılması beklenen finansal hizmetler alanları incelenmiştir. Bunlardan biri olan dijital kimlik konusu ele alınarak Müşterinin Tanı (KYC) işlemlerinde blok zincirin nasıl kullanılabileceğine ilişkin iki farklı model oluşturulmuştur. Finans kuruluşları arasında bir konsorsiyum blok zincirinin kullanıldığı iki farklı modelin uygulaması geliştirilmiş ve bu modeller karşılaştırılmıştır. Bu modeller incelenerek kişisel veriler içeren KYC uygulamalarının blok zincir teknolojisi kullanılarak nasıl tasarlanabileceğinin anlaşılması amaçlanmıştır.

# 2. GENEL KISIMLAR

Bu kısımda öncelikle, Fintech kavramı ve finansal hizmetlerin geliştirilmesinde kullanılan yeni teknolojiler açıklanmaktadır. Blok zincir teknolojisi detaylı olarak incelendikten sonra finansal hizmetlerde blok zincir teknolojisinin kullanımına yönelik bilgiler verilmektedir. Son olarak, dijital kimlik ve KYC konusunda bilgi verilip bu alanda blok zincir teknolojisinin nasıl kullanılabileceği açıklanmaktadır.

## 2.1. FINTECH: FİNANSAL TEKNOLOJİ

Finansal İstikrar Kurulu (FSB)[1] Fintech'i "finansal hizmetlerde teknoloji destekli yenilik" olarak tanımlamaktadır (FSB, 2017). Fintech "Finansal Teknoloji" kavramını ifade etmektedir ve finansal hizmetlerin daha iyi, daha hızlı ve daha kolay verilebilmesi amacıyla finans ve teknolojinin bir araya getirilmesinden oluşmaktadır. Teknolojinin yardımıyla, finansal hizmetler daha kullanıcı dostu haline getirilerek tüketicilerin finansal hizmetlere erişimi yeni yollardan sağlanmaktadır (Deloitte Türkiye, 2017).

Fintech kavramı, ürün ve hizmetler ile birlikte bunların temelini oluşturan teknolojileri de kapsamaktadır. Fintech'i tam olarak anlamak ve risk ve fırsatlarını değerlendirebilmek için işletmeler, ürünler ve hizmetler ile birlikte kullanılan teknolojileri iyi analiz etmek gerekmektedir.

### 2.1.1. Fintech'in Finansal Hizmetler Üzerindeki Etkileri

Mevcut işletmelerin finansal teknolojilerin getirdiği değişikliklere karşı koyması mümkün görünmediğinden bu yeni sektörü anlaması ve uyum sağlaması önemlidir. Fintech aşağıda sıralanan spesifik ve rekabetçi özellikleri ile finansal hizmet sektörünü etkilemektedir (William, 2016):

- Bankacılık ihtiyaçları için daha geniş seçenekler sunulması
- Kolaylık ve elverişlilik
- Düşük gelirli müşteriler için seçenekler sunulması

[1] Finansal İstikrar Kurulu (FSB), küresel finansal sistemi izleyen ve gelişimine yönelik tavsiyelerde bulunan uluslararası bir organizasyondur.

- Daha hızlı finansal hizmet sağlanması
- Fiziksel gereklere olan ihtiyacı giderek ortadan kaldırabilmesi
- Startup'ların yani yeni girişimcilerin büyük bankalarla aynı işleri yaptıkları halde bazı açılardan bankalara göre daha avantajlı olmaları

### 2.1.2. Fintech'in Gelişimi

Finansal hizmetler, ödeme uygulamaları, robo-danışmanlar, mobil cüzdan seçenekleri, hisse senedi toplama platformları, emeklilik planlama hizmetleri ve yatırımlara ve kredilere erişim ile daha da dijital hale gelmektedir. İlk bakışta, bu hizmetler mevcut hizmetlerde çok gerekli iyileştirmeler gibi görünse de, bunların yerini tamamen almaları da mümkündür.

Dünya genelinde finansal ürünler ve hizmetlerde birçok yenilik gözlemlenmiştir, bunlardan bazıları aşağıda özetlenmiştir (Toronto Centre, 2017):

#### *2.1.2.1. Dijital Ödemeler ve Elektronik Para*

Özellikle ödemelerin çoğunlukla nakit olarak yapıldığı ve debit ve kredi kartlarının yaygın olarak kullanılmadığı gelişmekte olan ülkelerde, Fintech firmaları uçtan uca para transferleri, fatura ödemeleri ve elektronik ödemeler için seçenekler sunmaktadır. Genellikle bu hizmetler, müşterilerin belirsiz bir süre için parasal değerlerini saklayabilecekleri bir dijital cüzdanda tutulan bir elektronik para ürünü ile sağlanmaktadır.

#### *2.1.2.2. Uluslararası Fon Transferi*

Büyük uluslararası para transferi rotalarına odaklanmış birçok Fintech girişimi bulunmaktadır. Fintech, prosedürleri basitleştirerek ve transfer maliyetlerini düşürerek çeşitli ülkelerde hizmet vermektedir. Söz konusu hizmetler e-para ürünlerine, geleneksel banka hesaplarına, kripto para birimlerine veya bunların kombinasyonlarına dayanmaktadır.

#### *2.1.2.3. Bireysel ve Ticari Krediler*

Fintech kredisi, gelişmekte olan bir pazar olup düşük gelirli borçlular ve mikro, küçük ve orta ölçekli işletmeler de dahil olmak üzere çeşitli müşteri gruplarını hedeflemektedir. Fintech kredisi çoğunlukla, büyük veri, fatura ödeme geçmişi, cep telefonu kullanımı gibi finansal sektör dışından toplanan alternatif verilere dayalı yeni kredi puanlama yöntemlerini kullanmaktadır. Bu kapsamdaki birçok ürün, otomatize edilmiş kredi karar mekanizmalarına

dayanmakta olup müşteri cep telefonu üzerinden kredi başvurusunda bulunmakta ve kredi kullandırımı birkaç dakika içerisinde gerçekleşmektedir.

#### *2.1.2.4. Uçtan Uca (P2P) Kredi Platformları*

Fintech kredisi kapsamında önemli bir gelişme olan uçtan uca kredi platformları, kredi verenler ile alanları bir araya getirmekte ve bir Fintech firması tarafından çoğunlukla internet üzerinden hizmetler sağlanmaktadır. Platformlar format ve çalışma kurallarına göre çeşitlilik arz etmektedir.

#### *2.1.2.5. Kitle Fonlama Platformları*

Kitle fonlama platformları ile Fintech firmaları tarafından, finansman veya yatırım fırsatlarını kolaylaştırmak amacıyla, sermaye yatırımları ve bağışlar dahil olmak üzere internet tabanlı hizmetler sunulmaktadır. P2P kredi platformları gibi, bunlar da şekil ve işletme kurallarında geniş çapta farklılık göstermektedir.

#### *2.1.2.6. Robo-danışmanlar*

Robo-danışmanlar "otomatik" veya "dijital yatırım" danışmanları olarak da adlandırılmaktadırlar. Mümkün olan en az insan müdahalesi ile veya hiç insan müdahalesi olmaksızın finansal danışmanlık ve çoğunlukla portföy yönetimi gibi hizmetler sunan çevrimiçi platformlardır.

#### *2.1.2.7. Kripto Para Birimleri*

Bitcoin, yaygın olarak kullanılan ilk kripto para birimidir, ancak Bitcoin'in piyasaya sürüldüğü 2009'dan bu yana başka birçok kripto para birimi de ortaya çıkmıştır. Kripto para birimleri devlet otoriteleri tarafından piyasaya sunulmamakta ve genellikle yasal para birimi olarak kabul edilmemektedir. Bitcoin gibi, diğer kripto para birimleri de Dağıtılmış Defter Teknolojisi'ne (DLT) dayanmaktadır. Bireyler ve şirketler, dağıtılmış defterlere taraf olmak suretiyle veya özel kripto para birimi çevrimiçi borsalarını kullanarak kripto para satın alabilmekte veya kripto paralarını satabilmektedirler.

Fintech ürünlerinin geliştirilmesinde makine öğrenmesi, yapay zeka (AI), uygulama programlama arayüzü (API), kriptografi, biyometri, büyük veri, bulut bilişim, nesnelerin interneti (IoT) ve blok zincir gibi pek çok yeni teknolojiden faydalanılmaktadır. Finansal teknolojiler değerlendirildiğinde, özellikle finansal hizmetler sektörünün birçok kesimini

ilgilendiren blok zincir teknolojisinde gelecek için önemli bir potansiyel olduğu düşünülmektedir (Deloitte Türkiye, 2017).

## 2.2. BLOK ZİNCİR TEKNOLOJİSİ

Blok zincir ilk olarak 2008'de Satoshi Nakamoto tarafından 2008 finansal krizinin ortasında, uçtan uca kripto para olarak tasarlanan Bitcoin'in alt yapısını oluşturan bir dağıtılmış defter olarak öne sürülmüştür (Nakamoto, 2008). Bir blok zincir, işlemlerin bir dijital kayıt defterinin oluşturulmasını ve dağıtılmış bir bilgisayar ağı arasında paylaşılmasını sağlayan bir veri yapısıdır. Blok zincirde, merkezi bir otoriteye gerek kalmaksızın ağdaki her bir katılımcı tarafından güvenli bir şekilde kayıt işlenmesini sağlamak için şifreleme kullanılmaktadır. Blok zincire bir veri bloğu kaydedildiğinde, değiştirilmesi veya kaldırılması son derece zordur. Blok zinciri tam olarak anlayabilmek için öncelikle temelini oluşturan teknolojilerin anlaşılması gerekmektedir.

### 2.2.1. Dağıtılmış Defter Teknolojisi

DLT, çeşitli konumlarda bulunan veya birden çok katılımcı arasında paylaşılan bir veritabanına dayanır. Dağıtılmış bir defter merkezileşmeyi ortadan, kaldırarak işlemlerin işlenmesi, onaylanması veya doğrulanması için merkezi bir otoriteye veya aracıya olan ihtiyacı ortadan kaldırmaktadır. İşlemleri veya diğer veri alışverişi türlerini işlemek, onaylamak veya doğrulamak için dağıtılmış defter teknolojisi kullanılabilmektedir. İşlem kayıtları sadece ilgili taraflarca mutabakata varıldığı zaman defterde saklanmaktadır. Dağıtılmış defterdeki tüm işlemler zaman damgası almakta ve benzersiz bir kriptografik imza ile kaydedilmektedir. Dağıtılmış defterdeki tüm katılımcılar, söz konusu kayıtların tümünü görüntüleyebilmektedir. Bu teknoloji, belirli bir veri kümesinde saklanan tüm bilgilerin doğrulanabilir ve denetlenebilir bir işlem geçmişinin oluşmasını sağlamaktadır (Belin, 2018). DLT'nin finans sektörünü temelden değiştirerek daha verimli, esnek ve güvenilir hale getirebileceği değerlendirilmektedir (The World Bank, 2018).

Genellikle blok zincir ve DLT kavramları birbirinin yerine kullanılmaktadır. Ancak blok zincir bir dizi blok olmasına rağmen, dağıtılmış defterler böyle bir zincir gerektirmemektedir. Blok zincirden farklı olarak, dağıtılmış bir defterin bloklarda bir veri yapısına sahip olması gerekmemektedir. DLT, yalnızca birden çok site, bölge veya katılımcıya yayılmış bir veritabanı

türüdür. Bununla birlikte, tüm blok zincirler dağıtılmış defterlerdir, ancak tüm dağıtılmış defterler blok zincir değildir (Belin, 2018).

### 2.2.2. Blok Zincir Teknolojisi

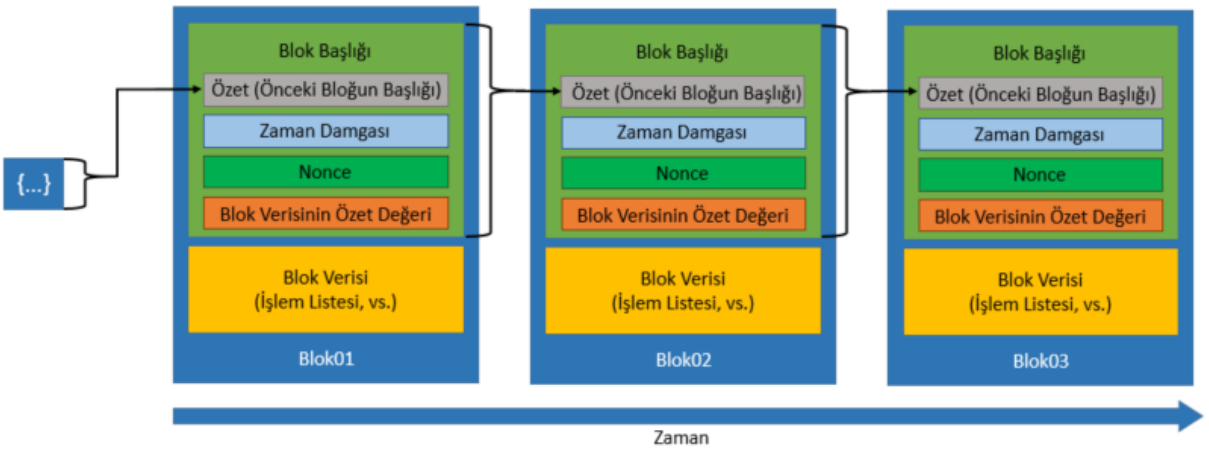
Merkezi ağlar savunmasız bir SPOF barındırmaktadır. Bu sorunu çözmek için blok zincir teknolojisi bizlere dağıtılmış bir ağ yapısı sunmaktadır. Blok zincirde veri sisteme dahil olan bütün katılımcılar tarafından kayıt altına alınmaktadır. Bir blok zincir, birbirlerini tanımayan kişilerin paylaşılan işlem kayıtlarına güvenmelerini sağlayan bir teknolojidir. Başka bir deyişle birbirine güvenmeyen katılımcıların bulunduğu bir ağda işlemleri güvence altına alarak güveni sağlamaktadır. Sistemin en başından tanımlanan kurallar ve bu kurallara göre oluşturulan kayıt zincirinin tüm katılımcılara dağıtılması ile güven sağlanmaktadır (Usta & Doğantekin, 2018). Paylaşılan işlem kayıtları, bilgisayarlarını kullanarak işlemleri doğrulayabilmeleri için ağdaki tüm katılımcılara dağıtılmaktadır. Bu doğrulama yöntemi ile üçüncü bir tarafa olan ihtiyaç ortadan kalkmaktadır. Görünüşteki karmaşıklığına rağmen, bir blok zincir aslında katılımcı bir ağdaki tüm bilgisayarlara kopyalanan işlemleri kaydetmek için kullanılan bir veritabanı türüdür (Deloitte LLP, 2016).

#### *2.2.2.1. Blok*

Bir blok zincirdeki veriler ‘blok’ adı verilen sabit yapılarda saklanmakta olup bir blok iki kısımdan oluşmaktadır:

1. Blok başlığı (Header); Şekil 2.1’de görüldüğü üzere, benzersiz bir blok referans numarası (Nonce), bloğun oluşturulduğu zaman (Timestamp), bir önceki bloğun başlığının özeti ve bu bloğun merkle root’unun özetinden (Hash of Block Data) oluşmaktadır.

2. Blok gövdesi; genellikle yapılan işlemler gibi sayısal varlıkların ve talimatların onaylanmış bir listesi, miktarları ve bu işlemlerin taraflarının adreslerinden oluşmaktadır.




**Şekil 2.1:** Blok yapısı (Yaga ve diğ., 2018).[2]

En son bloktan itibaren, zincirde birbirine bağlı önceki tüm bloklara erişmek mümkündür, bu nedenle bir blok zincir, birinciden itibaren blok zincirde yer alan tüm varlıkların ve gerçekleştirilen işlemlerin tüm tarihçesini korumaktadır. Böylece blok zincirde yer alan veriler doğrulanabilir ve denetlenebilir hale gelmektedir.

#### *2.2.2.2. Düğüm*

Blok zinciri oluşturan veri bloklarının saklandığı her türlü cihaz düğümler olarak adlandırılmaktadır. Düğümler bir blok zincirin altyapısını oluşturmakta olup, verileri depolama, yayma ve koruma görevlerini yerine getirmektedirler. Teorik olarak her bir düğümde blok zincirin bir kopyası yer almaktadır.

Bir madenci blok zincire yeni bir işlem bloğu eklemeyi denediğinde, bloğu ağdaki tüm düğümlere yayınlamaktadır. Bloktaki imza ve işlemlerin geçerliliğine göre, düğümlerin bloğu kabul etmesi veya reddetmesi mümkündür. Bir düğüm yeni bir işlem bloğunu kabul ettiğinde bu bloğu daha önce kaydettiği blokların sonuna eklemektedir. Düğümlerin görevlerini aşağıdaki şekilde ifade etmek mümkündür:

- Bir işlem bloğunun geçerli olup olmadığını kontrol etmek, bu bloğu kabul etmek veya reddetmek
- Blokları kaydetmek ve saklamak

[2] (Yaga ve diğ., 2018)'den alınarak tekrar çizilmiştir.

- İşlem geçmişini blok zincir ile senkronize edilebilmesi için diğer düğümlere yayınlamak ve yaymak

Farklı blok zincir yapılarında düğümlerin görev ve yetkileri sınırlandırılıp çeşitlendirilebilmektedir. Aşağıda düğüm çeşitleri sıralanmıştır (Pinto, 2018):

**Düğüm:** İşlemleri gönderebilen ve alabilen blok zincir ağında çalışan bir istemcidir.

**Tam düğüm:** Ağda çalışan ve blok zincirin tam bir kopyasını tutan bir istemcidir. İşlemleri gönderip alma ve blok zinciri blok girişleri ve madencilerin onayları ile güncelleme işlemlerini yapabilmektedir.

**Ana düğümler:** Ana düğümler, merkezi olmayan yönetim ve bütçeleme sağlamaktadır. Özet olarak, bir düğümün tam bir kopyasının yanı sıra, istenmeyen işlem çıkışları önbelleği veya onaylanmamış işlemlerin bellek havuzu gibi ek veri yapılarını da tutmakta, böylece yeni alınan işlemleri ve çıkarılmış blokları hızlı bir şekilde doğrulayabilmektedir. Alınan işlem veya blok geçerliyse, ana düğüm veri yapılarını güncellemekte ve bağlı düğümlere aktarmaktadır. Ana düğümün, diğer düğümlere güvenmesi gerekmemektedir, çünkü onlardan aldığı tüm bilgileri bağımsız olarak doğrulamaktadır.

#### *2.2.2.3. Özet Fonksiyonları*

Kriptografi, blok zincir teknolojisinde göndericinin kimliğinin güvence altına alınması, geçmiş kayıtların saklanması ve değiştirilemez olmasının sağlanması amacıyla kullanılmaktadır. Böylece işlemlerin güvenli bir şekilde yapılması ve tüm bilgilerin güvence altına alınması sağlanmaktadır.

Kriptografik özet fonksiyonları, düz metinden oluşan verileri, sabit boyutlu rasgele verilere dönüştürmek için kullanılmaktadır. Özet fonksiyonları tek yönlü çalışmakta olup, bu sayede baştaki düz metnin sonuç değerlerden geri dönüştürülmesi mümkün olmamaktadır. Özet fonksiyonlar için genellikle tek yönlülük ve zayıf çakışmaya dayanıklılık adlı iki güvenlik gereksinimi bulunmaktadır; bunlardan ilki, temel özet fonksiyonunun tersine çevrilememesini sağlarken, ikincisi aynı özet değerine sahip iki giriş metnini bulmanın kolay olmadığını göstermektedir (Wang ve diğ., 2019).

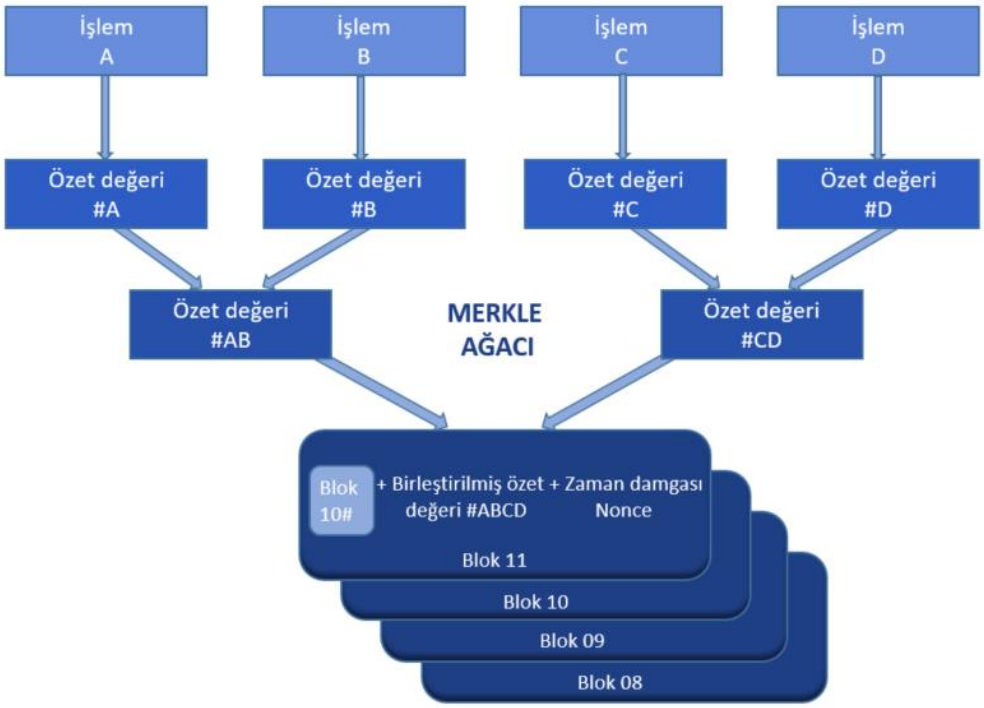
Blok zincirin en önemli özelliklerinden birisi değişmezliğidir ve özet fonksiyonlarının bunda önemli bir rolü vardır. Her blok, önceki bloğun bir özetini içermektedir ve bu şekilde "genesis" olarak adlandırılan ilk bloktan sonuncuya giden bir bloklar zinciri oluşturulmaktadır. Bu yöntem, zincirin içindeki herhangi bir bloktaki verinin değiştirilmesini zorlaştırmaktadır çünkü bir blok değiştiğinde takip eden tüm blokların da yenilenmesi gerekecektir.

Blok zincirlerde kullanılan en popüler özet fonksiyonu, SHA (Secure Hash Algorithms) adlı bir özet fonksiyonu ailesinin algoritmalarından biri olan SHA256'dır. SHA Amerika Birleşik Devletleri Federal Bilgi İşleme Standardıdır. SHA0 (1993), SHA1 (1995), SHA2 (2001) dahil olmak üzere bu ailedeki algoritmaların çoğu Amerika Birleşik Devletleri Ulusal Güvenlik Ajansı (NSA) tarafından tasarlanmıştır. SHA3 (2014), Keccak'tan üretilmiştir ve yalnızca dolgu yöntemi Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından değiştirilmiştir. Mevcut güvenlik gereksinimini karşılamak için, SHA2 ve SHA3'ün blok zincirlerinde ve kripto para birimlerinde kullanılması önerilmektedir (Wang ve diğ, 2019).

#### *2.2.2.4. Merkle Ağaç Yapısı*

Her işlemin, işlemin orijinal bilgisini içeren özet olarak bilinen bir tanımlama kodu vardır. Bir blokta bir araya getirilen işlemlerin özet değerleri, "Merkle Ağacı" olarak adlandırılan bir sistemde birleştirilmektedir (Şekil 2.2). Bu özet değeri, önceki bloğun özeti ve zaman damgası gibi bazı diğer bilgilerle birlikte yeni bir bloğun başlığına eklenmektedir. Yeni bloktaki önceki özet değeri, blokların değiştirilmesini ve hile yapılmasını engellemekte, zaman damgası ise verilerin o anda var olduğunu kanıtlamaktadır. Bir Merkle ağacı, temel olarak bloktaki tüm işlemleri organize etmek için kullanılmaktadır.

Merkle ağacı, Ralph Merkle tarafından veri entegrasyonunu verimli bir şekilde doğrulamak için önerilmiştir. Bütünlüklerini kontrol etmek için veriler düğümler halinde ele alınmaktadır. Üst düğümler, iki alt düğümün birleşiminin özetinden oluşmaktadır. Bu hesaplama kök düğümüne doğru devam eder ve bütün ağacın son özeti kökün özetidir.

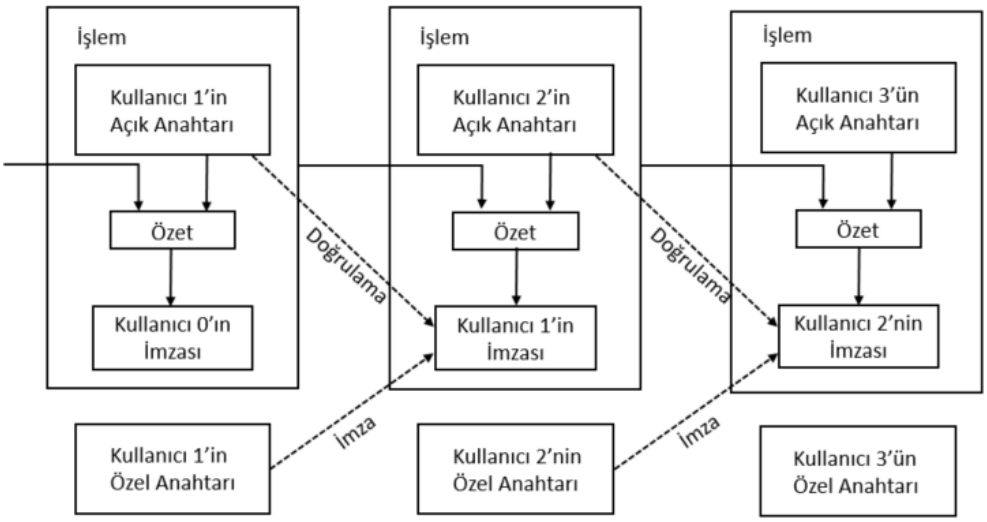



**Şekil 2.2:** Bitcoin blok zinciri[3]: Merkle ağaç yapısı ve bloklar **(The Economist, 2015)**[4].

### *2.2.2.5. Dijital İmzalar*

Blok zincirde bir işlem oluşturmak için bir dijital imza ile işlemi doğrulamak gerekmektedir. Tipik bir dijital imza işleminin iki aşaması vardır. Bunlar imzalama aşaması ve doğrulama aşamasıdır. Gönderen taraf bir işlemi imzalamak istediğinde, önce işlemden türetilen bir özet değeri üretmektedir. Daha sonra, bu özet değer özel anahtar kullanılarak şifrelenmekte ve alıcı tarafa şifreli özet orijinal verilerle birlikte gönderilmektedir. Alıcı taraf, alınan işlemi, şifrelenmiş özet ve alınan verilerden elde edilen özet değerinin, gönderenin kullandığı özet fonksiyonuyla karşılaştırılması yoluyla doğrulamaktadır. Şekil 2.3'te Bitcoin blok zincirinde gerçekleştirilen dijital imza işlemi görülmektedir.

[3] Farklı blok zincir platformlarında kullanılan yöntemler arasında farklılıklar bulunmaktadır. Bu kısımda, en genel kapsamda blok zincir altyapısı Bitcoin blok zincirine göre açıklanmıştır.
[4] (The Economist, 2015)'ten alınarak tekrar çizilmiştir.




**Şekil 2.3:** Bitcoin blok zincirinde dijital imza işlemi (Nakamoto, 2008).[5]

#### *2.2.2.6. Mutabakat*

Blok zincirde, her düğümün gelen blokları onaylaması ve kendi blok zincir kopyasına eklemesi, yani ağdaki tüm kullanıcılar tarafından kabul ve doğrulama gerçekleştirilmesi gerekmektedir. Bu kabul ve doğrulama işlemi mutabakat olarak adlandırılmaktadır. Ancak her düğüm için tüm ağ durumunun farklı bir görünümü vardır. Bu nedenle, bu sorunla başa çıkmak için dağıtılmış bir mekanizmaya ihtiyaç duyulmaktadır. Dağılmış mekanizmada uzlaşmaya varmak, blok zincirin önemli bir parçasıdır. Yaygın olarak uygulanan üç mutabakat algoritması vardır.

**İş Kanıtı (PoW)**

İş kanıtı (PoW) mutabakat algoritması blok zincirde en çok kullanılan algoritmadır. Tüm katılımcıların PoW örneklerini çözerek ve uygun blokları oluşturarak bilgi işlem gücü ile oy kullandığı kabul edilmektedir. Örneğin, Bitcoin hash tabanlı bir PoW kullanmaktadır. Bu yöntemde, merkle kök özeti ve önceki blok özeti gibi ek blok parametreleri ile birlikte özeti alındığında bir hedef değerinden daha küçük olması gereken bir değer bulmak gerekmektedir. Bu değer "nonce" değeridir. Böyle bir değeri bulan madenci bloğu bu değerle oluşturmakta ve diğer düğümlere iletmektedir. Yapılan bu işleme de "madencilik" adı verilmektedir. Ağdaki diğer düğümler bloğun özet değerini hesaplayıp, hedef değerinden daha az olma koşulunu

[5] (Nakamoto, 2008)'den alınarak tekrar çizilmiştir.

karşılayıp karşılamadığını kontrol ederek iş kanıtını gerçekleştirmektedir. PoW oldukça yavaştır ve çok büyük miktarda enerji gerektirmektedir.

**Hisse Kanıtı (PoS)**

PoS'a göre bir blok oluşturan düğüm, ağ tarafından kabul edilmeden önce belirli bir miktar kripto paraya erişebildiğinin kanıtını sağlamalıdır. Bu yöntem, daha fazla para birimi olan kişilerin ağa saldırma ihtimalinin düşük olacağı düşünülerek, katılımcıların belli miktardaki değere sahip olduklarını kanıtlamasını gerektirmektedir (Zheng ve diğ., 2018). Bu nedenle, sadece PoS'yi sağlayabilenler blok zincirin korunma sürecine katılabilmektedir. Enerji tasarrufu açısından PoS, PoW ile karşılaştırıldığında enerji tüketiminde daha verimli bir şekilde hizmet verdiği değerlendirilmektedir.

**Bizans Hata Toleransı**

Bizans Hata Toleransı (PBFT), dağıtılmış bir bilgisayar ağının istenen şekilde işlev görmesi ve sistemin kötü niyetli düğümlerin diğer düğümlere yanlış bilgi vermesine veya yaymasına karşı yeterli bir uzlaşma sağlamasıdır. Amaç, bu kötü niyetli düğümlerin ağın doğru işlevi ve sistemdeki dürüst düğümlerin ulaştığı doğru mutabakat üzerindeki etkilerini azaltmak suretiyle sistemi arızalara karşı savunmaktır.

Bu algoritma, Bizans hataları ile başa çıkmak için bir durum makinesi çoğaltma tekniği sunmaktadır. Esasen, PBFT modelindeki tüm düğümler, bir düğümün birincil düğüm ve diğerlerinin yedek düğümler olarak adlandırıldığı bir sırayla sıralanmaktadır. Sistemdeki tüm düğümler birbirleriyle iletişim kurmaktadır ve amaç, tüm dürüst düğümlerin, sistemin çoğunluğunun sistem durumuyla ilgili bir anlaşmaya varmasıdır. Düğümler mesajların belirli bir eş düğümden geldiğini kanıtlamakta ve aynı zamanda mesajın aktarım sırasında değiştirilmediğini doğrulamaktadır.

### 2.2.3. Blok Zincir Türleri

Blok zincirler teknolojik alt yapılarına göre ve iş bakış açısından olmak üzere iki şekilde ele alınmaktadır.

#### *2.2.3.1. Teknolojik Altyapısına Göre Blok Zincir Türleri*

**Özel Blok Zincir**

Tamamen özel bir blok zincir için, yazma izinleri bir kuruluşta merkezi olarak tutulmakta olup okuma izinleri herkese açık olabileceği gibi keyfi bir şekilde kısıtlanabilmektedir (Zheng ve diğ., 2018). Tek bir şirkete ait veritabanı yönetimi buna örnek gösterilebilir, bu durumda blok zincirin kamuya açık olması gerekli değildir.

**Konsorsiyum Blok Zincir**

Konsorsiyum blok zincir kısmen özeldir ve mutabakat süreci önceden seçilmiş bir düğüm kümesi tarafından kontrol edilmektedir (Zheng ve diğ., 2018). Blok zinciri okuma hakkı kamuya açık veya katılımcılarla sınırlı olabilmektedir. Bir konsorsiyum platformu özel bir blok zincir ile aynı şekilde verimlilik ve işlem gizliliği gibi faydaların çoğunu sağlamaktadır. Konsorsiyum blok zincir platformları, özel bir blok zincir ile aynı avantajlara sahiptir, ancak tek bir varlık yerine bir grubun liderliğinde çalışmaktadır (Hileman & Rauchs, 2017).

**Açık Blok Zincir**

Açık blok zincir dünyadaki herkesin verilere erişebileceği prensibiyle oluşturulmuştur (Zheng ve diğ., 2018). Bunun sağlanması amacıyla, verileri açık blok zincire yazmak için mutabakat süreci işletilmektedir. Kamuya açık blok zincir, PoW ve PoS gibi mutabakat algoritmaları tarafından desteklenen kriptografik doğrulama ile güvence altına alınan açık kaynaklı bir sistemdir. Açık blok zincirlerin en bilinen örneği Bitcoin'dir.

#### *2.2.3.2. İş Bakış Açısından Blok Zincir Türleri*

**Kapalı Blok Zincir**

Özel ya da konsorsiyum blok zincirlerin her ikisi de benzer avantajları sebebiyle kapalı blok zincirler olarak sınıflandırılmıştır (Hileman & Rauchs, 2017). Bu çözümlerde, blok zincir sabit bir ortamda kullanılmaktadır veya başka bir deyişle bunlar kurumsal odaklı çözümlerdir. Böyle bir modelde blok zincirin yararı, sürecin optimizasyonunu sağlamasıdır. Kapalı blok zincirler PoW gibi bir mutabakat mekanizmasına ihtiyaç duymamaktadır. Katılımcılar zaten birbirlerini tanıdıklarından, güven bir sorun değildir.

**Açık Blok Zincir**

Kamuya açık bir blok zincir, önemli değişiklikler meydana getirme ve programlanabilir bir ekonomi oluşturma potansiyeline sahiptir. Açık bir blok zincir üzerinde herkes herhangi biri tarafından kullanılabilecek çözümler üretebilmektedir.

### 2.2.4. Blok Zincirin Uygulama Alanları

Blok zincirin şeffaflık, değişmezlik ve merkeziyetsizlik özellikleri ağ katılımcılarının işlemlerini 7/24 güvenilir şekilde gerçekleştirmesine ve üçüncü tarafa olan ihtiyacın ortadan kaldırılmasına olanak tanımaktadır. Blok zincir, masrafları önemli ölçüde azaltmakta, riskleri ortadan kaldırmaktadır. Diğer yandan, kötü niyetli saldırılara karşı da önlemler alınmasını sağlamaktadır. Blok zincir teknolojisi, kullanıcıların işlemlerini ve verilerini kontrol etmelerini sağlarken aynı zamanda operasyonların tek bir merkezde gerçekleştirilmesiyle ilgili karmaşıklığı ve komplikasyonları azaltmaktadır.

Blok zincir bir güvenlik protokolüne benzemekle birlikte, gerçekte birbirinden farklı yaklaşımların kullanılabildiği farklı platformlarda, farklı uygulamaların hayata geçirilebileceği bir teknolojik yaklaşımdır (Usta & Doğantekin, 2018). Blok zincirin uygulama alanlarından bazılarını aşağıdaki gibi sıralayabiliriz:

- Kripto Para ve Token Çözümleri
- Dijital Kimlik
- Müşterini Tanı (KYC)
- Küresel Ödeme Sistemleri
- Girişimler İçin Sermaye İhtiyacı Karşılama
- Bağış Toplama ve Yönetimi
- Vergi Toplama ve Yönetimi
- Mal ve Kaza Sigortası Tazmin Süreci
- P2P Kredi Uygulamaları
- Mikro Finans Hizmetleri
- Otomatikleştirilmiş Uyum Mekanizması
- Oy Kullanma
- Tedarik Zinciri Yönetimi

- Telif Kayıt Sistemleri
- Kopya Ürün Koruması

### 2.2.5. Blok Zincir Platformları

Uygulamalar geliştirerek blok zincir teknolojisini keşfetmek amacıyla açık kaynak kodlu blok zincir platformlarını kullanmak mümkündür. Aşağıda bu platformlardan bazıları ile ilgili bilgi verilmektedir.

#### *2.2.5.1. Bitcoin*

Bitcoin, 2008'de Satoshi Nakamoto adı ile yayınlanan bir makale ile duyurulmuştur (Nakamoto, 2008). 2009 yılında geliştirildikten sonra hızla tanınmıştır. Bitcoin en çok bilinen ve tanınan blok zincir platformudur. Bitcoin platformunda, onaylanmış tüm işlemler blok zincire dahil edilmiştir. Bitcoin'de, blok zincirin bütünlüğü ve işlemlerin kronolojik olarak kayıt altına alınması kriptografi ile sağlanmaktadır. Mutabakat mekanizması olarak PoW kullanılmaktadır.

Bitcoin blok zincirindeki işlem, Bitcoin cüzdanları arasındaki değer aktarımlarını ifade etmektedir. Bitcoin cüzdanları, işlemleri imzalamak için kullanılan ve cüzdanın sahibinden geldiklerine dair bir matematik kanıtı sağlayan özel anahtarı tutmaktadır. İmza ayrıca, işlemin yapıldıktan sonra herhangi bir kişi tarafından değiştirilmesini engellemek için de kullanılmaktadır. Tüm işlemler ağa yayınlandıktan sonra, madencilik ile 10-20 dakika içinde onaylanmaya başlamaktadır.

Madencilik, bekleyen işlemleri blok zincire dahil ederek onaylamak için kullanılan dağıtılmış bir mutabakat mekanizmasıdır. Madencilik, blok zincirdeki işlemlerin bir kronolojik sıraya uymasını, ağın tarafsızlığını ve farklı bilgisayarların sistem durumu üzerinde hemfikir olmasını sağlamaktadır. Onay işleminin gerçekleşebilmesi için, işlemlerin, ağ tarafından doğrulanacak çok sıkı şifreleme kurallarına uyan bir blokta paketlenmesi gerekmektedir. Bu kurallar önceki blokların değiştirilmesini engellemektedir.

#### *2.2.5.2. Ethereum*

Ethereum, merkezi olmayan uygulamalar oluşturmak için alternatif bir protokol olarak ortaya çıkmıştır. Ağa programlanabilirlik ve ölçeklenebilirlik eklemektedir ve yukarıda Bitcoin'de açıklanan blok zincir özelliklerine dayanmaktadır. Ethereum, Bitcoin'in yaptığı gibi sadece bir

dijital para birimini temsil etmekle kalmamakta, birçok farklı iş modelinin blok zincirde uygulama düzeyinde kod olarak saklanmasına olanak tanımaktadır.

Ethereum blok zincirinde derlenen ve saklanan bilgisayar programları olan akıllı sözleşmeler bulunmaktadır. Akıllı sözleşmeler kriptopara işlemleri yapabildikleri gibi fonksiyon çağrılarıyla farklı işlevleri de yerine getirebilmektedirler. Ethereum'daki programlanabilirlik, Bitcoin blok zincirinde mevcut değildir, bu açıdan Ethereum'un Bitcoin'e göre daha avantajlı olduğu değerlendirilmektedir.

Ethereum madenci düğümleri, bloklar ağa iletildiğinde tüm durum değişikliklerini doğrulamaktadır. Akıllı sözleşmeler yoluyla çalıştırılan programlar, ağ tarafından mutabakat ile yapılan bir durum değişikliği olarak kabul edilmektedir. Ethereum Sanal Makinesi (EVM) ile bu mutabakat kod yürütme yoluyla gerçekleştirilmektedir.

Microsoft, Intel, J.P. Morgan gibi şirketler tarafından kurulan "Enterprise Ethereum Alliance" ile Ethereum, kurumsal dünyada özel blok zincir yapılarının oluşturulabilmesi için önemli bir potansiyel sunmaktadır (Usta & Doğantekin, 2018).

#### *2.2.5.3. Hyperledger*

Hyperledger, Aralık 2015'te Linux Vakfı tarafından başlatılan açık kaynak kodlu bir blok zincir platformudur ve tek bir blok zincir yapısı oluşturmak yerine kendi içerisinde farklı alt projelere destek vermeyi amaçlayan, sektörler arası blok zincir teknolojilerini geliştirmek için oluşturulmuş bir işbirliğidir (Usta & Doğantekin, 2018).

Hyperledger, genişletilebilir ve esnek bir mimari sunmak için kapalı ve izin tabanlı bir blok zincir platformu olarak tasarlanmış ve geliştirilmiştir. Hyperledger'ın birincil hedeflerinden biri, kurumsal düzeyde dağıtılmış defter kodları ve çerçeveleri oluşturmaktır. Bu platform, kurumsal çözümler için uygun bir blok zincir platformu olarak ortaya çıkmaktadır.

#### *2.2.5.4. Ripple*

Ripple, gerçek zamanlı bir uluslararası fon transfer platformudur. Uluslararası ödemelerde günümüzde kullanılan Swift gibi aracıların gereksinimleri ve bunlardan kaynaklanan yavaşlık, yüksek maliyet gibi olumsuzlukları ortadan kaldırmak için blok zincir teknolojisi ile oluşturulmuştur (Usta & Doğantekin, 2018).

Ripple, kendisine ait özel bir mutabakat protokolü olan “Interledger Protocol”ünü kullanmaktadır. Bu protokol, blok zincir yapısına ihtiyaç duymamakta, gerçekleşen işlemler hakkında saniyeler kadar kısa sürede mutabakat sağlayabilmektedir. Ripple, yapı itibari ile para birimlerinden bağımsızdır. Ripple’ın kendi para birimi olan XRP dahil olmak üzere, üzerinde kripto para birimleri ve her türlü para birimi ile işlem yapılabilmektedir.

### 2.2.6. Blok Zincirin Zorlukları

Blok zincir ekosistemi geliştikçe ve farklı kullanımları ortaya çıktıkça, tüm sektörlerde, yeni bağımlılıkların yanı sıra karmaşık ve tartışmalı sorunlarla karşı karşıya kalınacaktır (Deloitte LLP, 2016).

1. Kültür ve Organizasyon: Blok zincirin yeni bir teknoloji olması ve gelişimin ilk aşamalarında olması sebebiyle kurumsal bir çözümün parçası olarak kullanmanın sakıncaları olduğu düşünülmektedir. Bugünkü sistemlerle gerçekleştirilen işlerin blok zincir tabanlı bir sisteme geçişi zaman alacaktır. Bu teknolojinin yaygın bir şekilde kullanılmasının en az on yıl alacağına inanılmaktadır (The Economist, 2016).

2. Maliyet ve Performans: Blok zincirde yeni blokların yaratılması, çevre üzerinde olumsuz bir etkiye sahiptir. Madencilik süreci, her yeni blok oluşturulduğunda veya yeni bir işlem doğrulandığında çok miktarda elektrik kaynağı tüketmektedir. Ayrıca, bu yeni teknoloji, imza doğrulama, mutabakat mekanizmaları ve aynı işlemin her düğüm tarafından yapılması gibi özellikleri sebebiyle merkezi veritabanlarına göre işlemlerinde daha fazla karmaşıklığa sahiptir, bu da işlem süresinin geleneksel bir merkezi veritabanına göre daha fazla olmasına sebep olabilmektedir.

3. Düzenleme: Blok zincir teknolojisinin uygulanmasında ayrıca düzenlemeye dair yasal engeller de vardır. Bitcoin blok zinciri gibi bazı teknolojiler geleneksel ödeme ağlarındaki verimsizlikle başa çıkabilmek için özellikle düzenlemelere uyumsuz olarak tasarlanmıştır. Ayrıca blok zincirin orijinal hedeflerinden biri gözetimin azaltılmasıdır (Deloitte LLP, 2016). Sıkı düzenlemelerin, blok zincir teknolojisinin gelişimini engelleme riskini ortaya çıkarabileceği öngörülmektedir.

4. Güvenlik ve Gizlilik: Bitcoin gibi kripto para birimleri, işlemlerin bireylere değil "cüzdanlara" bağlanması ile takma isim kullanımını yani südonimliği sunarken blok zincirin

birçok potansiyel uygulaması işlemlerin ve akıllı sözleşmelerin belirli kimliklerle tartışmasız bir şekilde ilişkilendirilmesini gerektirmekte ve bunun sonucunda paylaşılan defterde saklanan ve erişilebilir olan verilerin gizlilik ve güvenliği ile ilgili önemli soruları gündeme getirmektedir (Deloitte LLP, 2016).

### 2.2.7. Blok Zincirin Güvenliği

Nakamoto çalışmasında (Nakamoto, 2008), geçmişi bir blokta değiştirmek için tüm blokları blok zincire tekrardan eklemek gerektiğini vurgulamaktadır. İşlem geçmişini değiştirmek için bir girişimde bulunulduğunda, değiştirilen bloğun özet değeri farklı olacak ve artık önceki bloklarla eşleşmeyecektir. Bu durum blok zincirde hile yapmayı oldukça zorlaştırmaktadır. Ayrıca, madenciler sürekli olarak işlemleri gözetlemekte ve tutarlı görünmeyen işlemleri kabul etmemektedirler.

Blok zincir her ne kadar kriptografi ile güvenli bir altyapı oluştursa da bu sistemde de hile yapmanın yolları vardır. Aşağıda bunlardan bazıları açıklanmıştır:

Birincisi, geliştiriciler test edilmiş ve onaylanmış kriptografi araçları kullansalar bile, istemeden güvenli olmayan yollarla bunları bir araya getirme ihtimalleri vardır. Özellikle de kullanılan algoritmalar geliştirilmek amacıyla değiştirilirken çok dikkatli olunması gerekmektedir, çünkü oluşturulan algoritmalarda güvenlik açıkları bırakmak mümkündür.

Ayrıca, blok zincir teknolojisinin kötüye kullanımı da mümkündür. Sistemi kötüye kullanmanın yollarından birisi, yüzde 51 olarak adlandırılan bir saldırıdır. Bu, birinin ağın yüzde 51'ini kontrol ettiği anlamına gelir, böylece işlemlerin olması gerektiği gibi doğrulanamaması ve sonuç olarak blok zincire yanlış bilgi eklenmesi söz konusu olmaktadır.

Diğer yandan araştırmacılar tarafından mevcut blok zincir sistemlerinde de pek çok açık keşfedilmiştir. Diğer madencilerin madencilik gücünün yarısından daha azına sahip olunsa bile, bir blok zinciri bozmanın bir yolu olduğu açıklanmıştır (Eyal & Sirer, 2018). Buna göre, "bencil bir madenci", zaten çözülmüş kripto-bulmacalar üzerinde diğer düğümleri zaman harcamaya sevk ederek haksız bir avantaj elde edebilmektedir.

Diğer bir olasılık da "tutulma atağı" (eclipse attack)'dır. Verileri karşılaştırmak için blok zincirdeki düğümlerin sürekli iletişim halinde kalması gerekmektedir. Bir düğümün iletişiminin kontrolünü ele geçiren ve ağın geri kalanından gelmiş gibi görünen yanlış verileri kabul

etmesini sağlayan bir saldırgan, bunu kaynak israfı ya da sahte işlemlerin onaylanması için kullanabilmektedir.

Blok zincir sistemlerinin gerçek dünyayla bağlantı kurduğu noktalarda, örneğin yazılım istemcileri ve üçüncü taraf uygulamalarında önemli sorunlar yaşanmaktadır. Örneğin, saldırganlar, kripto para birimine sahip olan herkesin özel anahtarlarını saklamak için kullandığı internet bağlantılı cüzdan uygulamalarına sızabilmektedir. Özellikle çevrimiçi cüzdanlar ana hedef haline gelmiştir. Birçok kripto para borsası, kullanıcılarının paranın çoğunu çevrimdışı donanım cüzdanlarında tuttuklarını iddia etmektedir, ancak Japonya merkezli bir kripto para borsası olan Coincheck'in 500 milyon doların üzerindeki kripto para değerinin çalınması, bunun her zaman doğru olmadığını göstermektedir (Cheng, 2018).

Blok zincirler ile gerçek dünya arasındaki belki de en karmaşık temas noktaları, işlemlerin otomatikleştirilebileceği bazı blok zincirlerde saklanan bilgisayar programları olan "akıllı sözleşmeler"dir. 2016 yılında, bilgisayar korsanları tarafından Ethereum'un blok zincirine yazılan akıllı bir sözleşmedeki öngörülemeyen bir açıklıktan yararlanılarak, yeni bir blok zincir tabanlı yatırım fonu olan DAO'dan o zaman yaklaşık 70 milyon dolar değerinde olan 3,6 milyon ETH çalınmıştır (Siegel, 2016). DAO kodu blok zincirde yaşadığı için, Ethereum topluluğu parayı geri almak için "hard fork" olarak adlandırılan tartışmalı bir yazılım güncellemesi yapmak zorunda kalmış, böylece para çalınmadan önceki blok zincir kayıtlarına kadar geri dönülerek yeni bir blok zincir versiyonu oluşturulmuştur.

## 2.3. FİNANSAL TEKNOLOJİLER İÇİN BLOK ZİNCİR

Geleneksel olarak, finans kuruluşları işlemlerini yapabilmek için merkezi bir otoriteye veya aracıya güvenmektedir. Blok zincir teknolojisi ise, kuruluşların merkezi bir otorite olmaksızın anında bir ağ üzerinde finansal işlemleri yapmasını ve doğrulamasını sağlamanın bir yolu olarak ortaya çıkmaktadır. Bu bölümde, blok zincir teknolojisinin finans sektöründeki uygulamalarından bahsedilecektir.

### 2.3.1. Finansal Sektördeki Değişim

Finans sektörü ve özellikle bankacılık sektörü, sıkı bir şekilde düzenlenmiş bir alan olarak görülmekte ve gelir modeli uzun bir süredir değişmemektedir. Bununla birlikte, yeni ve ileri

teknolojilerin bankacılık sektörünü önümüzdeki yıllarda önemli bir şekilde şekillendirmesi beklenmektedir.

Blok zincir teknolojisinin finans sektörünü nasıl etkileyeceği konusunda çelişkili görüşler mevcuttur. En uç görüş, blok zincir teknolojisinin bankaları gereksiz kılmasıdır. Tüm bankacılık sektörünün teknoloji nedeniyle ortadan kalkacağı çok aşırı bir ifadedir. Finansal kurumların blok zincir teknolojisinden faydalanma ihtimallerinin, blok zincir kullanmamaları nedeniyle ortadan kalkma ihtimallerinden daha yüksek olduğu düşünülmektedir. Bankaların sunduğu birçok hizmetin ortadan kalkması muhtemeldir, ancak bir yandan da yeni hizmetler ortaya çıkmaktadır.

Blok zincir teknolojisinin tüm endüstrileri, özellikle de güvene dayalı olanları yeniden şekillendirmek için büyük fırsatlar sunduğu değerlendirilmektedir. Finansal sektör, güvene dayalı bir endüstri olduğundan bu yeni teknolojiden yararlanabileceği öngörülmektedir.

### 2.3.2. Blok Zincirin Finansal Sektöre Etkisi

Finansal hizmetler sektörü, verimliliği artırıp masrafları azaltma yeteneğine sahip nispeten yeni olan blok zincir teknolojisiyle ilgili heyecan duymaktadır. İspanyol bankası Santander, 2022 yılına kadar blok zincir teknolojisinin bankacılık sektöründe yılda 20 milyar dolara kadar tasarruf sağlayabileceğini iddia etmektedir (The Economist, 2015).

Finansal hizmetler sektörü açısından, açık ve özel blok zincirler arasında bir ayrım yapılması gerekmektedir. Bu ikisinin arasındaki ana fark blok zincirdeki bilgilere erişim iznidir. Özel blok zincirler bilgiye erişimi ve blok zinciri değiştirme ya da kayıtları okuma hakkını daha sıkı bir şekilde kontrol etmektedir. Finans kuruluşları, özellikle gizli bilgilerin güvenli bir şekilde saklanabilmesi ve bu bilgilere erişimin kontrol altına alınabilmesi nedeniyle özel blok zincirlere ilgi duymaktadır. Özel blok zincirlerdeki bilgi ve işlemler, kontrol edilebildiği için daha sonradan değiştirilebilmektedir, açık blok zincirlerde ise bu çok zor veya imkansızdır.

Blok zincir teknolojisinin şimdilik ne tür uygulamalarda ne zaman ve ne ölçüde uygulanacağını söylemek zordur. Her şeyi blok zincirlere sokmanın makul olmadığı da değerlendirilmelidir. Bazı hizmetler için blok zincir teknolojisinden daha uygun teknolojilerin bulunması ihtimali her zaman vardır.

### 2.3.3. Finansal Teknolojilerde Blok Zincir Kullanımı

Blok zincir teknolojisi, finans sektöründe çeşitli uygulamaları mümkün kılma potansiyeline sahiptir. Şimdiye kadar araştırılan, üzerinde çalışılan ve uygulanmaya başlanan alanlardan bazıları aşağıda açıklanmıştır.

#### *2.3.3.1. Uluslararası Fon Transferi*

Blok zincir teknolojisinin, uluslararası fon transferi gibi finansal sektördeki birçok süreci iyileştirmesi mümkündür. Blok zincir teknolojisinin, geleneksel aracıların çoğunu ortadan kaldırarak süreçleri hızlandırması ve basitleştirmesi söz konusu olabilmektedir. Aynı zamanda, para transferi maliyetlerini daha uygun hale getirmesi mümkündür (Deloitte, 2017).

Bu sebeple blok zincir teknolojisi fon transferi alanında kullanılmaya başlanmıştır. Ancak, aşılması gereken bazı engeller mevcuttur. En önemlisi, kripto para birimleri için düzenleme eksikliğidir. Diğer bir sorun da, kripto paranın hedefte yerel olarak kabul edilen para birimine dönüştürülmesinin gerekmesidir.

#### *2.3.3.2. Kimlik Yönetimi*

Finansal hizmetler sektöründe kimlik yönetimi, yüksek maliyetli bir süreçtir. Bir müşterinin kayıt olup finansal hizmetlere erişebilmesi için, bankaların ve diğer finans kuruluşlarının KYC düzenlemelerine uygun güvenlik koşullarını sağlaması gerekmektedir. Bu da bir tür fiziksel kontrol ve/veya resmi kimlik belgelerinin kontrol edilmesi gerektiği anlamına gelmektedir. Müşterilerin bir kimlik doğrulama aracına ihtiyacı vardır ve başvuracakları her hizmette kim olduklarını kanıtlamaları gerekmektedir. Ayrıca, yetkilendirme; yani yapmak istediklerini yapmalarına izin verildiğinin de kanıtı olmalıdır ve bunlara ek olarak, her yeni hizmet sağlayıcı için bu adımları tekrarlamaları gerekmektedir (Deloitte, 2017).

Blok zincir teknolojisi ile gerçekleştirilen kimlik yönetiminde, kullanıcılar kendilerini nasıl tanımladıklarını ve kimliklerinin hangi taraflarla paylaşılacağını seçebilmektedir. Kimliklerini blok zincir üzerinde kaydettiklerinde, sağlayıcılar da blok zincire bağlıysa, her servis sağlayıcısı için yeni bir kayda gerek duyulmayacağı ve aynı kaydın tekrar tekrar kullanılabileceği öngörülmektedir.

Blok zincir teknolojisindeki kimlik standartları henüz belirlenmemiştir ve en iyi uygulamalar hala geliştirilme aşamasındadır. Ayrıca, uygulamada mahremiyetin ne ölçüde korunabileceği

konusunda araştırma yapılması gerekmektedir. Veri, blok zincire kaydedildikten sonra, ağdaki tüm taraflar tarafından erişilebilir olmaya devam etmektedir. Bu nedenle, kullanıcılar, açıkladıkları kişisel verileri en aza indirmek zorundadır. Elbette, bu zor bir denge sağlanmasını gerektirmektedir, çünkü kimliğin kanıtlanabilmesi için yeterli bilginin paylaşılması gerekmektedir (Deloitte, 2017).

#### *2.3.3.3. Akıllı Sözleşmeler*

Akıllı sözleşmeleri, genellikle geleneksel sözleşme hükümlerinin mantığını taklit eden bilgisayar programları olarak değerlendirmek mümkündür. Bu nedenle akıllı sözleşmelerle, pek çok türden sözleşmenin kısmen veya tamamen kendi kendini idare etmesi veya kendi kendini uygulamasının gerçekleştirmesinin sağlanması mümkündür.

Akıllı sözleşmeler katı kurallarla kodlandığında geleneksel sözleşmelerden daha güvenli olmaları mümkündür. Blok zincir teknolojisi herhangi bir aracıya ihtiyaç duymadığı için sözleşmeyle ilgili birtakım işlem maliyetlerinin azaltılması da mümkün olabilecektir. Ancak akıllı sözleşmeler, kullanıcı niyetini anlayan ve her zaman kusursuz olan yapılar değildir. Akıllı sözleşmenin kuralları bilgisayar koduna kaydedilmekte ve sözleşmenin amacına göre serbestçe yorumlanamamaktadır. Bu sebeple, eğer metinde bir yanlışlık varsa, geleneksel bir sözleşmede olduğundan çok daha büyük sorunlar yaşanması olasıdır (Deloitte, 2017).

DAO'ya olanlar bu durumu en iyi şekilde açıklamaktadır. Yatırımcılardan biri olan saldırgan, sözleşmenin kodunda istenmeyen bir boşluk bulmuş ve bundan faydalanarak parayı ele geçirmiştir (Siegel, 2016). Bu durum, teknik olarak yasal olmayan bir eylem ya da normal anlamda bir saldırı olmayıp, sözleşmenin hatalı kodu bu durumun gerçekleşmesine izin vermiştir. Bu örnekte görüldüğü üzere, blok zincir teknolojisindeki akıllı sözleşmeler henüz karmaşık yasal sözleşmelerden beklenen olgunluk seviyesine ulaşmamıştır (Deloitte, 2017).

#### *2.3.3.4. Düzenleme ve Denetim*

Düzenleyici hizmetlere olan küresel talebin 2020 yılına kadar 118,7 milyar dolar olması beklenirken, Fintech firmaları blok zincir gibi modern teknolojilerle mevzuata uygunluğu geliştirmektedir (Daryna, 2018). Blok zincirin, düzenlemelerle bağlantılı riskleri, belirsizliği ve karmaşıklığı ortadan kaldırabileceği üzerinde durulmaktadır.

Bir blok zincirin doğrulanmış işlemleri izlemesi ve işleme katılanlar tarafından gerçekleştirilen tüm eylemleri kaydetmesi sayesinde, denetçilerin kayıtların gerçekliğini doğrulaması

gerekliliği ortadan kalkmaktadır. Bir blok zincir, denetçilerin, işlemlerin kopyalarından ziyade asıl işlemin kendisini incelemesine olanak tanımaktadır.

Blok zincirin silinemezliği de hata olasılığını azaltıp finansal raporlama ve denetimler için kayıtların bütünlüğünü sağlamaktadır. Tüm veriler tek bir yerde depolandığından, blok zincirin raporlama ve muhasebeyi standartlaştırması ve denetçilerin bilgileri elde etmesini ve analiz etmesini kolaylaştırması mümkün olacaktır.

#### *2.3.3.5. Kredi Skorlama*

Geleneksel bankacılık sistemi, dünya çapında 1,7 milyar yetişkin ve 160 milyon küçük işletme gibi büyük bir potansiyel kitleyi yok saymaktadır (Daryna, 2018). İhmal edilen bu müşteriler, kırsal alanlarda yaşayanlardan, mevduat veya tasarruf hesabı olmayanlardan, sigortalı bir kurumda hesap sahibi olan ancak düşük bütçeli alternatif finans sağlayıcılarını da kullananlardan ve geleneksel bir bankada bir mevduat veya tasarruf hesabına sahip olmanın hiçbir anlamını görmeyen milenyum neslinden oluşmaktadır. Bu tüketici gruplarını göz ardı ederek, bankaların potansiyel gelirinde yıllık yaklaşık 380 milyar dolar kaybettiği öngörülmektedir (Daryna, 2018).

Blok zincirin, yeni bir kredi puanlama yolu sağlayarak ihmal edilen bu kitlenin de finans sektörüne katılımını sağlayabileceği düşünülmektedir. Blok zincir destekli bir kredi puanlama platformunun mevcut sistemlerden farklı olarak kredi verileri, kimlik bilgileri, geçmiş veriler, borç verileri gibi daha fazla veri kaynağını analiz ederek müşterilerin kredi skorunu hesaplamasının mümkün olabileceği üzerinde durulmaktadır.

## 2.4. FİNANSAL HİZMETLERDE DİJİTAL KİMLİK YÖNETİMİ

Kamu, finans ve bireysel alanların artan dijitalleşmesi, kimliklerin yönetimini ve doğrulanmasını zorlaştırmaktadır. Kimlik, tamamen işlem bazlı olup, yüksek derecede risk içeren işlemlerin yapıldığı finansal hizmetler için kritiktir ve kesinlik gerektirmektedir. Bu nedenle, kimlik sorunları finansal hizmet sağlayıcılarının iş modellerinde sorunlar olarak ortaya çıkmaktadır (World Economic Forum, 2016). Bu bölümde, finansal hizmetler sektöründe iş verimliliğini arttırmak, yasalara ve düzenlemelere uyumluluğu geliştirmek ve sahtekarlığı önlemek açısından kritik öneme sahip olan dijital kimlik incelenmiştir.

### 2.4.1. Dijital Kimlik

Finansal hizmetler sektöründe, fiziksel kimlik protokolleri kullanılarak dijital hizmetler verilmeye çalışılmasından kaynaklanan sorunlarla karşılaşılmaktadır. Bu sorunlar Tablo 2.1'de (World Economic Forum, 2016) banka büyüklükleri ve türlerine göre listelenmiştir.

**Tablo 2.1:** Finansal hizmetlerdeki kimlik yönetimi kaynaklı sorunlar.

| İş Problemi | Perakende/küçük - orta ölçekli bankacılık | Kurumsal bankacılık ve yatırım bankacılığı |
|---|---|---|
| *Verimsiz ve yüksek maliyetli müşteri kabul işlemleri* | ✓ | ✓ |
| *Verimsiz, yüksek maliyetli ve etkin olmayan müşterini tanı ve durum tespiti süreçleri* | ✓ | ✓ |
| *Yüksek oranda manuel ve zaman alan uyumluluk işlemleri* | ✓ | ✓ |
| *Tüzel kişiler hakkında bilgi toplama ve toplam riski belirleme zorluğu* | ✓ | ✓ |
| *Bireysel kimliği (örneğin şirket yöneticileri) kurumsal kimlikle ilişkilendirme zorluğu* | ✓ | ✓ |
| *Tüm işlem ortaklarını tanımlama zorluğu (örneğin, ticari ilişkilerde üçüncü taraflar)* | ✓ | ✓ |
| *Veri işleme ve gizlilik konusundaki yasal standartlara uymakta zorluk* | ✓ | ✓ |
| *Müşterinin birden fazla görünümünün olması* | ✓ | ✓ |
| *Etkili/uygun ürün ve hizmetler sağlamada zorluk* | ✓ | |
| *Yeni müşterilerin finansal geçmişlerinin takibinin zorluğu* | ✓ | |
| *Yüksek dolandırıcılık oranları* | ✓ | |
| *Varlık mülkiyeti ve kaynağını takip etmede zorluk* | | ✓ |
| *Varlık izleme ve tespit etmede zorluk* | | ✓ |

Finansal hizmetler sektöründeki kimlik sorunlarının aşılabilmesi için dijital kimliklerin kullanılabileceği uygulamaların hayata geçirilmesi gerekmektedir. Dijital kimlik sisteminde, kimlik dijital kayıtlardan oluşmakta olup kullanıcı bunları kontrol edebilmektedir. Kimlik kanıtı, standartlaştırılmış dijital formatta varlıklar arasında paylaşılabilmektedir.

Dijital bilgi zarar verilmesinden, bozulmaktan, kaybolmaktan ve çalınmaktan son teknoloji doğrulama ve güvenlik protokolleriyle korunabilmektedir. Kullanıcı iznine bağlı olarak özel ve güvenli yollarla paylaşılması mümkündür. Böylece bankaların ve diğer finans kuruluşlarının, müşterilerini daha iyi tanıması ve onlara daha iyi hizmet etmesi mümkün olabilecektir.

### 2.4.2. Dijital Kimlik Yönetim Sistemleri

Bir kimlik yönetim sistemi, teknolojilerin, politikaların ve iş süreçlerinin birleşiminden oluşmaktadır. Dijital kimlik yönetim sisteminin öğeleri; kullanıcı, kimlik sağlayıcı ve servis sağlayıcıdır. Kullanıcı dijital bir kimliğe sahiptir ve bir servis sağlayıcı tarafından sağlanan kaynaklara erişmek için bunu kullanmaktadır. Kimlik sağlayıcının rolü, kullanıcılarının dijital kimliğini yönetmek ve kullanıcılarının kimliğini doğrulamaktır.

Dijital kimlik yönetim sistemi modelleri, merkezi kimlik, birleştirilmiş kimlik, kullanıcı merkezli kimlik ve kendine egemen kimlik olmak üzere dört aşamada ilerlemekte olup Şekil 2.4'te dijital kimlik yönetimi sistem modellerinin gelişimine yer verilmektedir.


**Şekil 2.4:** Dijital kimlik yönetim sistemi modellerinin gelişimi (Segovia Domingo & Enríquez, 2018).[6]

Blok zincir, bir dijital kimlik sistemi olarak benimsenme potansiyeline sahiptir. Blok zincir üzerinde bir kimlik yaratılarak, kişilerin kimliklerini yönetmelerini ve kişisel bilgilerinin kiminle paylaşılacağını ve nasıl erişileceğini kontrol etmelerini kolaylaştıracağı üzerinde durulmaktadır. Bu yaklaşım kendine egemen kimlik olarak adlandırılmaktadır.

Kendine egemen kimlik, insanların ve kuruluşların kendi kimlik verilerini kendi cihazlarında saklayabilmeleri ve kimlik verilerinin merkezi bir veritabanına dayanmaksızın onu doğrulaması gerekenlere etkili bir şekilde sunabilmeleri anlamına gelmektedir.

Kendine egemen kimlik, kullanıcının haklarını destekleyen ve kullanıcı odaklı bir yaklaşımdır. Bireylerin kimlikleri ve verileri üzerinde tam kontrol ve özerkliğe sahip olmalarını önermekte olup kriptograf Christopher Allen tarafından on ilke ile açıklanmıştır (Allen, 2016):

[6] (Segovia Domingo & Enríquez, 2018)'den alınarak tekrar çizilmiştir.

1. Varoluş: Kullanıcılar bağımsız bir mevcudiyete sahip olmalı ve mevcut kişisel kimliğinin bir uzantısı olmalıdır. Dijital formdan ibaret bir mevcudiyet olmamalıdır.

2. Kontrol: Kullanıcılar, kimlikleri üzerinde kontrol sahibi olmalı ve kimliklerin nasıl kullanıldığı ve verilerin nasıl açıklandığı konusunda nihai otorite olmalıdır.

3. Erişim: Kullanıcılar kendi verilerine kolayca erişebilmelidir.

4. Şeffaflık: Verileri yöneten sistemler ve onu analiz eden algoritmalar şeffaf ve açık olmalıdır.

5. Kalıcılık: Kimlikler, kullanıcının takdirine bağlı olarak, uzun ömürlü veya kalıcı olma becerisine sahip olmalıdır.

6. Taşınabilirlik: Kimlikler, güvenilir olsalar dahi tek bir üçüncü taraf varlık tarafından tutulmamalıdır ve kimliğe ilişkin bilgiler ve hizmetler taşınabilir olmalıdır.

7. Birlikte Çalışabilirlik: Kimlikler, sistemler, şirketler arasında ve uluslararası alanda kontrol kaybına sebep olmaksızın çalışma yeteneğine sahip olmalıdır.

8. Rıza: Kullanıcı verilerinin paylaşımı, kullanıcının açık rızası ve bilgisi ile yapılmalıdır.

9. Minimalizasyon: Açıklanan veya paylaşılan veriler işlemin gerçekleştirilmesi için gerekli olan asgari düzeye indirilmelidir.

10. Koruma: Kullanıcının hakları sistemin odağı olmalı ve kullanılan algoritmalar bağımsız ve merkezsiz olmalıdır.

### 2.4.3. KYC: Müşterini Tanı

KYC yani “Müşterini Tanı” bankaların ve diğer finans kuruluşların müşterilerinin kimliklerini doğruladığı süreçtir. Amacı, müşterilerden kaynaklanan riskleri tanımlamak, anlamak ve azaltmaktır. Bu süreç daha çok kara para aklamayı önleme (AML) düzenlemeleri ve terörün finansmanının engellenmesi çalışmaları ile ilgilidir ve suç faaliyeti ile sahteciliğin azaltılması amacıyla uygulanmaktadır. Müşterilerin doğru bir şekilde tanımlanması yasalar tarafından zorunlu tutulmakta ve bu konuda yapılan ihmaller finans kuruluşlarının ağır cezalar alması ile sonuçlanmaktadır.

EY Türkiye'nin Fintech Dönüşümü raporunda (EY Türkiye, 2018), finansal sektöre katılım için ülke çapındaki altyapının güvenli hale getirilmesi ve bunun tüketicilerle iletişimde büyük önem arz ettiği, Fintech şirketleri ve mevcut finans kuruluşlarının, tüketicilerin finansal işlem bilgilerinin güvenli bir şekilde paylaşımını sağlayacak ortak altyapıları kurması, sıkı bir denetime tabi tutması ve tüketicinin verileri üzerinden yapılan işlemler hakkında bilgilendirilmesi için ortak geri bildirim mekanizmaları kurmaları gerektiği ifade edilmektedir.

KYC çalışmalarında karşılaşılan aşağıdaki zorluklar göz önüne alındığında KYC uygulamalarının değişmesinin gerekli olduğu düşünülmektedir.

**1. Müşteri Kayıt Maliyeti:** Thomson Reuters'ın 2017 yılı için yaptığı KYC çalışmasına göre, finans kuruluşları her yıl müşteri kaydı için ortalama 150 milyon dolar harcamaktadır ve bu maliyetin 2018 yılında %13 oranında artması beklenmektedir (Thomson Reuters, 2017).

**2. Müşteri Kayıt Süresi:** Yine aynı çalışmada, ortalama müşteri kayıt süresinin 2016 yılında 28 gün olduğu ve 2017 yılında ise 32 güne yükseldiği belirtilmiştir.

**3. Veri Güncelleme Maliyetleri:** Mali kurumların verilerini aralıklı olarak güncellemeleri gerekmektedir ki bu da maliyetleri daha da artırmaktadır.

**4. Müşteri Memnuniyetsizliği:** Zorlu süreç ve gereklilikler nedeniyle finans kuruluşları, müşterilerinin % 84'ünün KYC ile olumsuz bir deneyime sahip olduğunu bildirmekte ve bu müşterilerin % 12'sinin alternatif bankacılık ilişkileri aramasına neden olmaktadır.

**5. Teknolojiye Yatırım:** Yıllık müşteri kayıt maliyetlerinin dörtte birinden fazlası, süreci hızlandırmak ve genel müşteri deneyimini geliştirmek için teknolojinin iyileştirilmesine adanmıştır.

Son zamanlarda, bankaların ortak kullanabileceği, finansal tüketicilerin finansal işlemlerdeki tüm başvurularını dijital olarak yapabildiği ve bankalarla olan fiziksel evrak paylaşım ihtiyacının ortadan kaldıran e-KYC platformları üzerinde çalışılmaktadır. Bu platformlar sayesinde finansal hizmetlere olan talebin, işlem kolaylığı ve artan güvenlik ile birlikte artması beklenmektedir.

### 2.4.4. Kimlik Çerçeveleri

David Birch, "Kimlik: Yeni Para" isimli kitabında (Birch, 2016), bir dijital kimlik ile sahip olduğu özelliklerin birbirine dijital sertifikalar ile bağlı olacağı ve bu sertifikaların çeşitli işlemleri desteklemek için paylaşım döngüsü içine girebileceği bir model tanımlamıştır. Buna göre, Şekil 2.5'te görüldüğü gibi kimliğin her özelliği ilgili kurum veya kuruluş tarafından imzalanmaktadır. Örneğin bir kişinin yaşı bilinmek istenildiğinde, kişi yaş özelliğinin yer aldığı güvenli bir sertifika sunarsa bu bilginin güvenilir bir kaynaktan geldiği anlaşılıp doğrulama yapılması mümkün olacaktır. Tüm bu işlemler otomatik olarak gerçekleşmekte ve bu bilgiler 'vesika' (credential) olarak adlandırılmaktadır. Burada verilen örnekte vesikanın başlığı 18_YAŞINDAN_BÜYÜK_MÜ olacaktır.

Burada açıklanan vesika yapısına benzer bir şekilde kimliğin kendisi açıklanmadan sadece KYC doğrulamasının bankalar ve diğer finans kuruluşları arasında paylaşılacağı kendine egemen bir finansal kimlik oluşturulabileceği değerlendirilmektedir.

| Özellikler | İmzalar |
|---|---|
| ÇALIŞMA_İZNİ_VAR_MI | AVRUPA BİRLİĞİ İMZALADI |
| ÇALIŞIYOR_MU | CHYP İMZALADI |
| 18_YAŞINDAN_BÜYÜK_MÜ | BARCLAYS İMZALADI |
| İNGİLTEREDE_Mİ | VODAFONE İMZALADI |

**Şekil 2.5:** Kimlik - özellikler **(Birch, 2016)**.[7]

### 2.4.5. Blok Zincir İle KYC Uygulamaları

KYC uygulamalarını oluşturmak için blok zincir teknolojisinin kullanılması finansal hizmetlerin müşterilere ulaştırılması konusunda yenilikçi bir gelişme olarak görülmektedir.

[7] (Birch, 2016)'dan alınarak tekrar çizilmiştir.

Blok zincir üzerinde çalışan bir KYC uygulaması, aynı müşteri için farklı kuruluşlar tarafından, müşteri tanımlama ve doğrulama işleminin birkaç kez gerçekleştirilmesi yerine bir kez gerçekleştirilebildiği dağıtılmış bir altyapı sağlamaktadır.

KYC blok zincir üzerinden sağlanması oldukça karmaşık ve zor olan bir hizmettir. Bu konuda en iyi uygulamalar henüz oluşmamıştır. Ancak Fintech firmaları pek çok uygulama gerçekleştirmiştir. Konu üzerindeki araştırmalar ise devam etmektedir.

Bhaskaran ve diğ. (2018) çalışmalarında, blok zincir kullanarak KYC sürecinin bankalar ve müşteriler tarafından paylaşıldığı çift taraflı bir veri paylaşım modeli önermiştir. Açıklanan bu model Hyperledger Fabric üzerinde geliştirilen izinli bir blok zincir üzerinde çalışmaktadır.

Bir sonraki bölümde bu bölümde açıklanan kimlik çerçeveleri yaklaşımı kullanılarak kendine egemen kimlik ilkelerini sağlamayı hedefleyen bir blok zincir üzerinde dağıtılmış bir finansal kimliğin oluşturulması üzerinde durulmuştur.

# 3. MALZEME VE YÖNTEM

Blok zincirin, kişilerin kimliklerini hırsızlığa karşı koruyan ve hileli faaliyetleri büyük ölçüde azaltan bir platform oluşturmak için kullanılması mümkündür. Bu teknolojinin, bankaların ve diğer finans kuruluşlarının çeşitli sektörlerde karşılaşılan kimlik doğrulama ve mutabakat sorunlarını ele alan güçlü blok zincirler oluşturmasına yardımcı olabileceği ve böylece müşteriler ve kuruluşlar için zaman ve kaynak tasarrufu sağlayabileceği değerlendirilmektedir.

Kişisel verilerin blok zincirde tutulmasının bazı sakıncaları vardır. KYC uygulamaları geliştirilirken kişisel verilerin blok zincir üzerinde saklanmayacağı modeller üzerinde durulması daha doğru olacaktır. Kimlikte yer alan ham verileri depolamak yerine, yalnızca kullanıcı hakkındaki soruların cevaplarının bir blok zincirinde saklanması güvenliği artıracaktır. Bir önceki bölümde anlatılan kimlik çerçeveleri bu yöntemin temelini oluşturmaktadır. Bu bölümde, bir önceki bölümde açıklanan kendine egemen kimliğin KYC uygulamaları için nasıl oluşturulabileceği üzerinde durulmuştur.

## 3.1. ETHEREUM BLOK ZİNCİR PLATFORMU

Ethereum akıllı sözleşme temelli bir blok zincir platformudur. Akıllı sözleşmeler ise EVM'de yer alan bayt kodundan ibarettir. Akıllı sözleşmeler Solidity gibi yüksek seviyeli diller kullanılarak yazılıp blok zincire aktarılmaktadır. Kullanıcılar işlemlerini gerçekleştirirken akıllı sözleşmeyle etkileşim içine girmektedir. Bir işlem alındığında Ethereum düğümleri işlemin hedeflediği işlevin belirtilen sözleşmede karşılık geldiği fonksiyonu verilen argümanlarla yürütmektedir. Fonksiyonlar akıllı sözleşme kodu ile bir blok zincire yerleştirildiğinde, dijital olarak doğrulanabilir veri girişleri tarafından tetiklenerek belirli koşullar sağlandığında işlemler otomatik olarak gerçekleşmektedir.

Akıllı sözleşmeler, dijital kimlikler ile kullanılmaktadır. Akıllı sözleşmelerde, tarafların kimliği hesap adresleri ile belirlenmektedir. Hesapların yükümlülükleri ve hakları belirlenmekte ve akıllı sözleşme koduna uygun şekilde kodlanmaktadır. Kullanıcıların doğru bir şekilde tanımlanmaması veya akıllı sözleşme kodundaki bir hata sahtekarlığa yol açabilmektedir. Ethereum düğümleri işlemlerin blok zincire yazılması üzerinde anlaşmaya varmak üzere PoW mutabakat mekanizmasını kullanmaktadır. Her Ethereum işleminin gas fiyatı denen bir maliyeti vardır. Kullanıcı yapacağı her işlem için bir ödeme yapmak zorundadır.

Geleneksel finans kuruluşları için özellikle akıllı sözleşmelerle proglamlanabilirlik olanağı sağlayan ağlarda, blok zincir teknolojisi kullanılarak mevcut iş modellerinin geliştirilebilmesinin mümkün olacağı değerlendirilmektedir. Bununla birlikte, açık blok zincirler ile oluşturulan kimlik uygulamalarının finansal alandaki yasal düzenlemelerle çelişmesi mümkündür. Bu bölümde anlatılan çalışma ile bir yandan blok zincir tabanlı akıllı sözleşmelerden faydalanarak finans kuruluşlarının KYC ile ilgili düzenlemelere uyumunu sağlarken, diğer yandan kişisel verilerin korunması hakkındaki düzenlemelere uygun ve kullanıcıların gizliliğini koruyacak bir tasarımın Ethereum blok zincirinde nasıl geliştirilebileceğinin anlaşılması amaçlanmıştır.

## 3.2. BLOK ZİNCİR OLUŞTURULMASINDA KULLANILAN ALTYAPI

### 3.2.1. Web3 Framework

Web3.js (Ethereum Foundation), bir HTTP, WebSocket veya IPC bağlantısı kullanarak yerel veya uzak bir Ethereum düğümü ile etkileşime girilmesini sağlayan bir kütüphaneler koleksiyonudur. Web3.js kullanılarak Ethereum blok zinciri üzerinde işlemlerin gerçekleştirilmesi, Solidity akıllı sözleşme kodunun derlenmesi ve akıllı sözleşmelerdeki fonksiyonların çalıştırılması mümkündür. Bu tez için geliştirilen uygulamalarda Etehereum ile bağlantı kuracak arayüz olarak Web3.js kullanılmıştır. Web.js yerel bir Ethereum düğümüne bağlanabileceği gibi Ethereum'un test ağları olan Rinkeby, Ropsten ve Kovan'a ya da Ethereum'un ana ağı olan Mainnet'e bağlanabilmektedir.

### 3.2.2. Ganache CLI

Ganache CLI veya daha çok bilinen eski adıyla TestRPC, tam bir Ethereum düğümü ve yerel blok zinciri ağını simüle etmekte olup Ethereum uygulamalarının hızlı bir şekilde test edilmesi için kullanılmaktadır (Truffle Suite). Ganache CLI ile anahtarları düğüme kayıtlı olan belli sayıda hesap üretilmesi mümkündür. Ganache CLI, oluşturulan hesaplar için belli miktarda bakiye sağlamaktadır. Böylece işlemleri finanse etmek için ETH temin etme ihtiyacını ortadan kaldırmaktadır. Yerel bir ağ oluşturduğu için işlem bloklarını herhangi bir mutabakat algoritması kullanmadan anında işlemektedir. Bu tezdeki uygulamaların geliştirilmesinde sayılan özelliklerinden dolayı Ganache CLI kullanılmıştır.

### 3.2.3. İşlem İmzalama

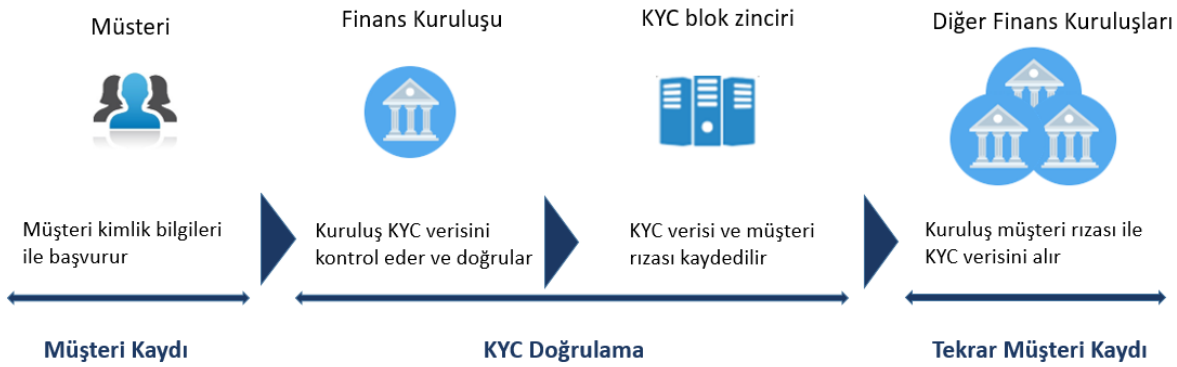
Metamask (Metamask), Ethereum hesap yönetimi için kullanılabilecek bir tarayıcı eklentisidir. Metamask Ethereum hesaplarına bağlı açık ve özel anahtarları tarayıcının yerel deposunda saklanmasına ve müşteri tarafında işlem imzalamaya olanak tanımaktadır. Bu tez için gerçekleştirilen uygulamaların test edilebilmesi için Ganache CLI ağında oluşturulmuş olan kullanıcı anahtarları Metamask eklentisine tanımlanarak işlem imzalama bu hesaplar tarafından Metamask üzerinden sağlanmıştır. Metamask'tan başka, ethereumjs-tx (EthereumJS) gibi paketler uygulamaya eklenerek de işlem imzalamaya imkan sağlanabilmektedir.

## 3.3. GERÇEKLEŞTİRİLEN UYGULAMALAR

Ethereum blok zinciri üzerinde KYC işlemlerinin yapılabilmesi için iki farklı yaklaşımla uygulama gerçekleştirilmiştir. Birinci modelde kuruluş tarafından müşteriden alınan veriler blok zincire aktarılarak işlemler blok zincir üzerinde yapılmaktadır. Bu modelin amacı kuruluşların KYC doğrulamasını yaptıkları müşteri bilgilerini diğer kuruluşlarla paylaşarak aynı müşteri için tekrar doğrulama yapılması gerekliliğini ortadan kaldırmak, böylece bu işlemleri tekrar tekrar yapmanın maliyetinden kaçınmaktır. İkinci modelde ise müşterinin kontrolünün artırılması, kişisel verilerin korunması hakkındaki düzenlemelere uyulması ve güvenliğin geliştirilmesi hususlarında birinci modelin sağlayamadıklarının da fonksiyonlara eklenmesi amaçlanarak kimlik verilerinin müşterinin finans kuruluşuna başvurması üzerine müşteriden alındıktan sonra blok zincir dışında müşterinin başvurusunu yaptığı kuruluşun kendi kaynaklarında saklandığı bir yapı kurulmuştur. İkinci modelde blok zincir üzerinde kişisel veriler saklanmamaktadır, ancak hem kuruluşların hem de müşterilerin yapılan işlemleri takip edebilmeleri için müşterilerin başvurularına ve kuruluşların yaptıkları KYC doğrulamalarına ilişkin işlemler kayıt altına alınmaktadır.

### 3.3.1. Birinci Model: Kimlik Verileri Blok Zincirde

Bu modelde, finans kuruluşu tarafından müşteriden alınan kimlik bilgileri blok zincire aktarılır ve doğrulama yapıldıktan sonra diğer kuruluşlar ile KYC bilgileri paylaşılır. Müşterinin tüm kimlik bilgileri blok zincire kaydedilir ve aynı müşterinin daha sonra farklı kuruluşlara başvurması üzerine tekrar doğrulama işlemi yapmaya ihtiyaç bırakmadan kimlik bilgileri diğer kuruluşlar tarafından müşterinin rızası ile görüntülenerek başvurunun onaylanabilmesini sağlanır. Şekil 3.1'de birinci modelin işleyişi gösterilmiştir.




**Şekil 3.1:** Birinci modelin işleyişi.

### *3.3.1.1. Sistem Mimarisi*

Önerdiğimiz model aşağıdaki öğelerden oluşur:

- Blok Zincir: Müşterinin kimlik bilgilerinin, bu bilgilerin görüntülenebilmesi için verdiği rızanın kaydedilmesi ve bütünlük kontrollerinin yapılması için kullanılmaktadır.
- Akıllı Sözleşme: Blok zincire veri yazılıp okunabilmesini sağlamak üzere Solidity programlama dili ile yazılan fonksiyonlardan oluşmaktadır.
- Kuruluş Portalı: Müşterinin verisinin blok zincire kaydedilmesi için kullanılmaktadır.
- Müşteri Portalı: Müşterinin verilerini kontrol edebilmesi ve bu verilerin kuruluşlar tarafından kullanılabilmesi için rıza vermesi amacıyla kullanılmaktadır.

**Blok Zincir**

Ağa dahil edilen kuruluşlar blok zincirin düğümlerini oluşturmaktadır. Uygulamanın gerçekleştirilmesi için Ethereum Ganache CLI ağı kullanılmıştır. Ganache CLI yerel bilgisayarda tek bir düğüm ve buna bağlı hesaplar oluşturmaktadır. Blok zincir teknolojisi, kimlik bilgilerinin kaydedilmesi ile rıza eylemleri için depolama ve alınan bilgilerin bütünlüğünü doğrulamak için gerekli bilgileri depolamak amacıyla kullanılır. Bu model için yazılan akıllı sözleşme ile blok zincir KYC bilgilerinin kaydedilmesi, doğrulanması ve diğer kuruluşlarla paylaşılmasını sağlamak üzere programlanmıştır.

**Kuruluş Portalı**

Müşteri tarafından sağlanan veriler kuruluş tarafından blok zincire kaydedilir. Bu kayıt aynı zamanda müşterinin rızasının alınması için de bir başvuru sayılır. Çünkü müşteri rızası olmadan kuruluş bu bilgileri kullanamaz. Farklı bir kuruluş aynı müşterinin verilerini görmek istediğinde de yine müşterinin rızasını almak zorundadır.

**Müşteri Portalı**

Müşteri portalı, müşterinin blok zincire kuruluşlar tarafından aktarılan verilerini görüntüleyebilmesi ve müşterinin rızasının kaydedilmesi için kullanılır.

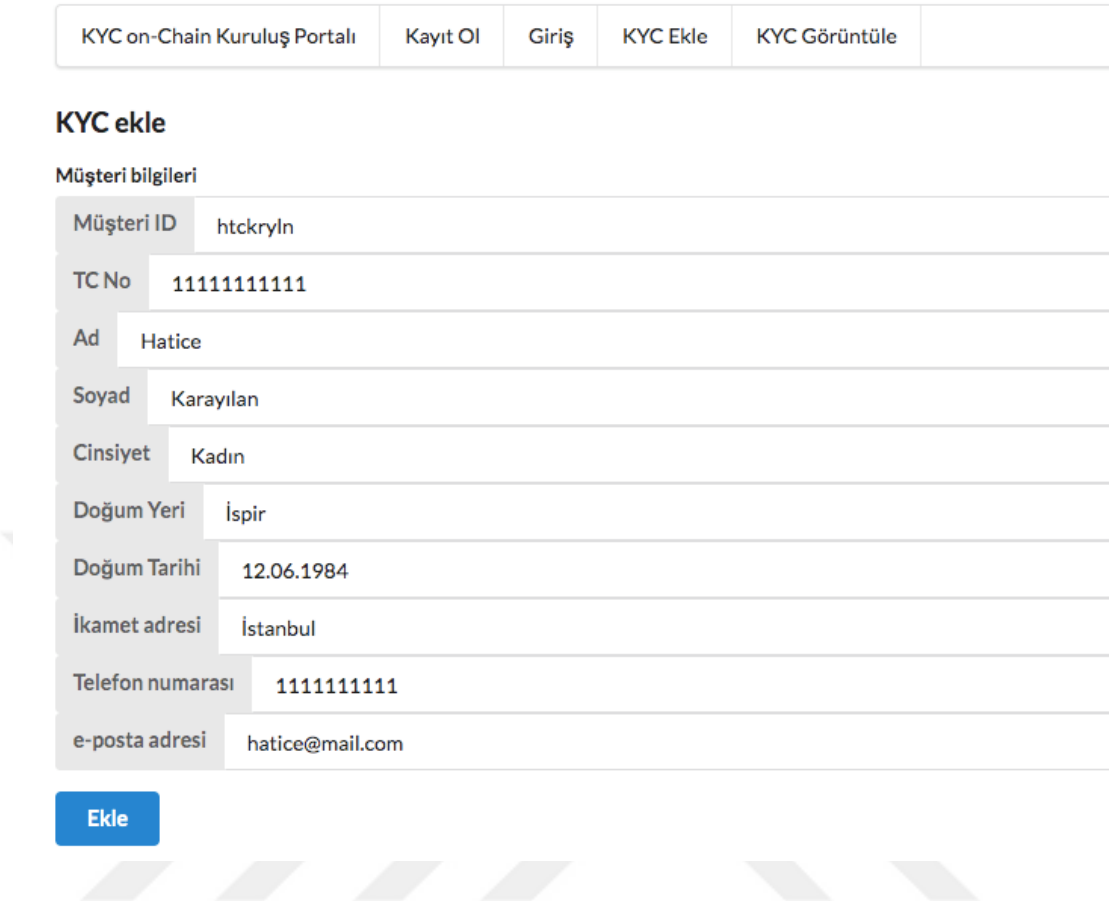
#### *3.3.1.2. Uygulamanın Fonksiyonları*

**KYC Doğrulaması**

1. Kuruluş portalı üzerinden müşterinin sağladığı kimlik bilgileri Şekil 3.2'de görülen KYC formu ile blok zincire kaydedilir.

2. Bu bilgiler kuruluş tarafından ancak müşteri blok zincir üzerinden rızasını verdiği takdirde kullanılabilir.

3. Farklı bir kuruluş daha önce blok zincirde doğrulanmış olan müşteri verilerini görüntülemek için müşteriye bir talepte bulunur.




**Şekil 3.2:** Kuruluş, kuruluş portalından KYC doğrulaması yaptığı müşterinin bilgilerini kaydeder.

**Müşteri Rızası**

1. Müşteri portalından müşteri, başvuruda bulunduğu organizasyon tarafından blok zincire kaydedilen kimlik verilerini kontrol edebilir.

2. Blok zincirde doğrulanmış olarak yer alan kimlik verilerini görüntülemek isteyen kuruluşların talepleri müşteri tarafından Şekil 3.3'te görüldüğü şekilde kabul edilebilir veya reddedilebilir.


**Şekil 3.3:** Müşteri, müşteri portalında doğrulanmış KYC bilgilerini görüntülemek isteyen kuruluşlar için açık rıza verir.

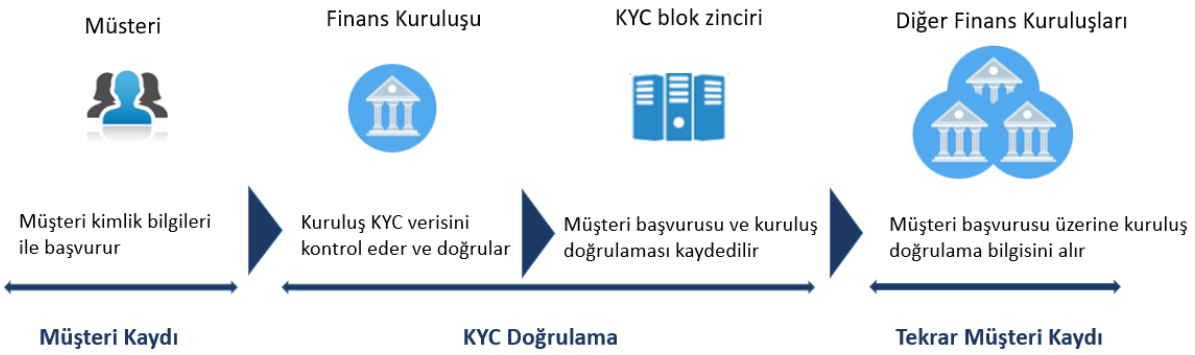
Bu uygulamada müşteri ve kuruluşlar arasındaki bütün bilgi alışverişi blok zincir teknolojisi ile gerçekleştirilmektedir.

### 3.3.2. İkinci Model: Kimlik Verileri Blok Zincir Dışında

Bu model uygulanırken özellikle, Kişisel Verilerin Korunması Kanunu'na (Kişisel Verilerin Korunması Kanunu, 2016) göre aşağıda sayılan gerekliliklerin sağlaması amaçlanmıştır:

- Bir kişinin kendisiyle ilgili bütün kişisel veriler hakkında bilgi edinebilmesinin sağlanması
- Bu verilerin belirlenerek kişiye sunulabilmesi
- Kişinin isteğine bağlı olarak verinin değiştirilebilmesi ya da silinebilmesi

Müşterinin bizzat başvurması ile iki taraf arasında KYC bilgilerinin onay bilgisinin paylaşılacağı bir yapı kurulmuştur. Müşterinin bir kuruluşa yaptığı başvuru ve bu başvuru sonucunda kuruluş tarafından yapılan doğrulama blok zincire kaydedilir ve bu bilgi müşterinin daha sonra yapacağı başvurularda tekrar doğrulama işlemi yapmaya ihtiyaç bırakmadan diğer kuruluşlar tarafından KYC doğrulamasının kabul edilmesini sağlar. İkinci modelin işleyişi Şekil 3.4'te açıklanmıştır.




**Şekil 3.4:** İkinci modelin işleyişi.

KYC verilerinin, onaylanmış verilerin sahibi olan müşteriden alıcı olan kuruluşa devredilmesi zincir dışında gerçekleşmektedir. Veri aktarımı işleminin kendisi ve müşteri tarafından verilen kimlik bilgilerinin SHA-256 özet fonksiyonuyla alınmış bir özeti blok zincire kaydedilmektedir. Amaç, kimlik doğrulama işlemlerinden kaynaklanan doğrulanmış bilgiler ile müşterinin aynı verilerle farklı kuruluşlara başvurması durumunda özet bilgilerinin karşılaştırılarak doğrulama yapıldığından emin olunması ve bu durumda tekrar KYC doğrulaması yapmak mecburiyetinden kaçınılmasıdır.

#### *3.3.2.1. Sistem Mimarisi*

Önerdiğimiz ikinci model aşağıdaki öğelerden oluşur:

- Blok Zincir: Müşteri başvurusu ve kuruluş doğrulaması işlemlerinin kaydedilmesi ile başvurular arasındaki bütünlük kontrollerinin yapılması için kullanılmaktadır.
- Akıllı Sözleşme: Blok zincire veri yazılıp okunabilmesini sağlamak üzere Solidity programlama dili ile yazılan fonksiyonlardan oluşmaktadır.
- Kuruluş API'ları: Uygulama üzerinden müşterinin kimlik bilgilerinin müşterinin başvuruda bulunduğu kuruluşa aktarılması için kullanılmaktadır. Veritabanı olarak bir ilişkisel veritabanı yönetim sistemi olan MySQL seçilmiştir.
- Müşteri Portalı: Müşterinin kendi kimlik verilerini kaydedip istediği kuruluşun müşterisi olabilmek için başvuru yapabilmesi için kullanılmaktadır.
- Kuruluş Portalı: Müşterinin verilerinin API'lar üzerinden alınarak görüntülenip buna göre doğrulanması ve blok zincire onay bilgisinin kaydedilmesi amacıyla kullanılmaktadır.

**Blok Zincir**

Ağa dahil edilen kuruluşlar blok zincirin düğümlerini oluşturmaktadır. Uygulamanın gerçekleştirilmesi için Ethereum Ganache CLI ağı kullanılmıştır. Ganache CLI yerel bilgisayarda tek bir düğüm ve buna bağlı hesaplar oluşturmaktadır. Blok zincir teknolojisi, müşterinin KYC doğrulamasının kaydedilmesi ve doğrulanan KYC verilerinin diğer kuruluşlar tarafından paylaşılabilmesi için müşterinin verdiği rızanın saklanması için kullanılmaktadır. Bu model için yazılan akıllı sözleşme ile blok zincir KYC bilgilerinin özet değerinin kaydedilmesi, doğrulanması ve diğer kuruluşlarla paylaşılmasını sağlamak üzere programlanmıştır.

**Kuruluş API'ları**

Kuruluş API'lar müşterilerin kimlik bilgilerinin aktarılabilmesi için kuruluşların arka uç sistemlerinde konuşlanan kendi veritabanlarına bağlanmaktadır. Böylece, istemci uygulaması, kimlik bilgilerinin depolandığı kuruluşun sunucusuna bağlanarak müşteri verilerini veritabanlarına yazıp okuyabilmektedir. Müşteri tarafından yapılan başvuruları kontrol etmek ve KYC formundan üretilmiş olan özet değeri blok zincirde kaydedilen özet değerlerle karşılaştırabilmek için API'lar blok zincir ile bağlantı kurmaktadır.

**Müşteri Portalı**

Müşteri portalı blok zincir ile müşteri başvurusunun kaydedilmesi için iletişim kurmaktadır. Ayrıca API'lar üzerinden kuruluşun arka uç sistemlerine bağlantı kurulmaktadır. Kimlik bilgileri birden fazla kuruluşa aktarıldığında, birden fazla API bağlantısı yapılmaktadır.

**Kuruluş Portalı**

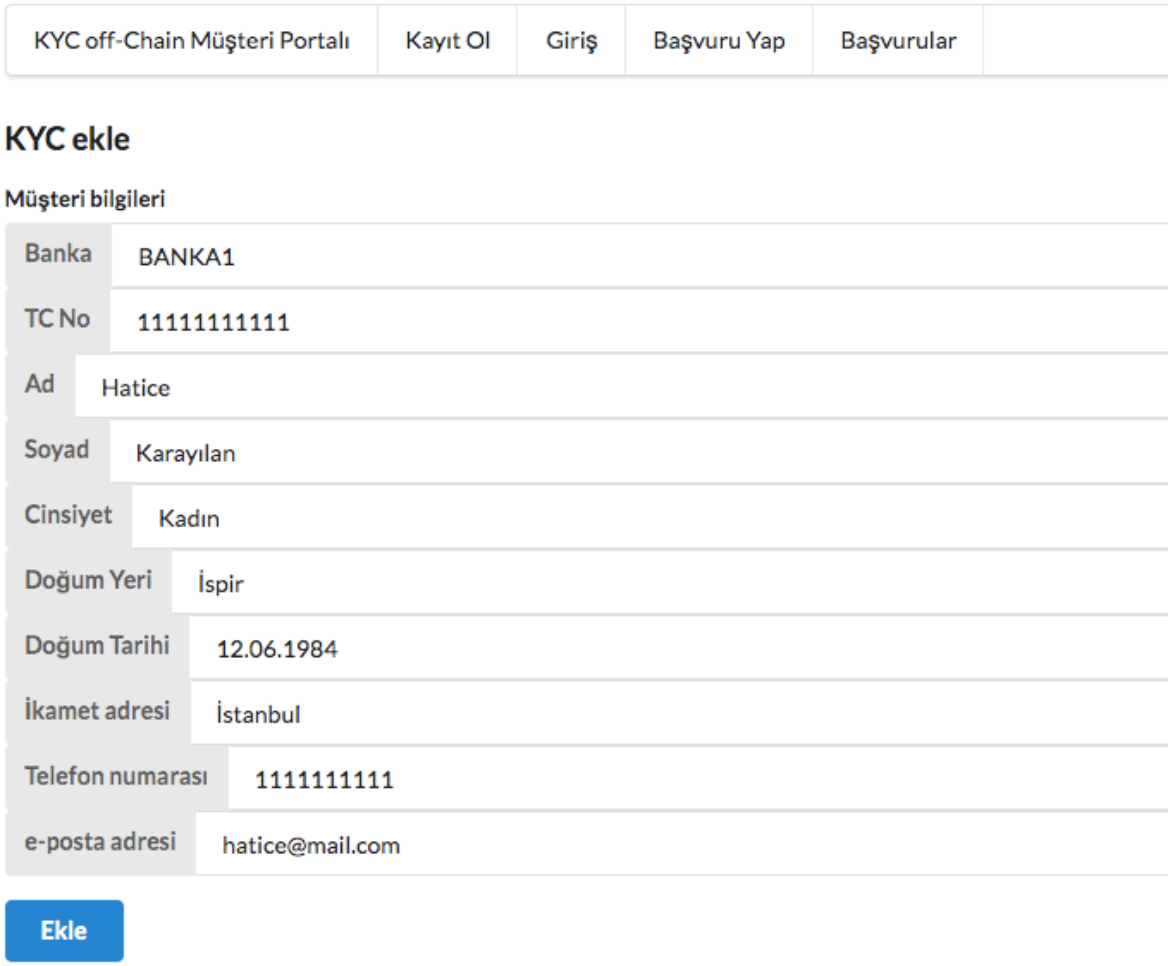
Müşteri tarafından kuruluşa başvuru yapıldığında bir KYC formu doldurulur ve bu formdaki kimlik bilgileri API'lar üzerinden kuruluş veritabanına aktarılır. Kuruluş bu bilgileri kuruluş portalından görüntüleyip KYC doğrulamasını yapar. Farklı bir kuruluş aynı müşterinin verilerini görmek istediğinde de yine bu müşterinin başvurusu üzerine aldığı KYC formunu portaldan eriştiği müşteriye ait doğrulanmış KYC form özetiyle karşılaştırabilir.

### *3.3.2.2. Uygulamanın Fonksiyonları*

**Müşteri Kaydı**

1. Müşteri, müşteri portalı üzerinden kullanıcı oluşturup giriş yapar ve başvurduğu kuruluşu seçerek kimlik bilgilerini Şekil 3.5'te görülen KYC formunu doldurarak kaydeder.

2. Kimlik bilgileri başvuruda bulunulan kuruluşun API'ı üzerinden kuruluşa iletilir. Aynı zamanda kimlik bilgilerinin SHA-256 algoritması ile özeti alınarak blok zincirde bu özet değeriyle birlikte müşteri için bir kayıt oluşturulur.




**Şekil 3.5:** Müşteri, müşteri portalındaki KYC formundan kimlik bilgilerini girerek seçtiği kuruluşa başvurur.

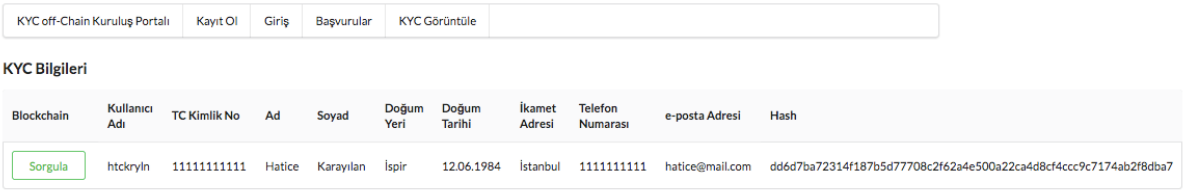
**KYC Doğrulaması**

1. Kuruluş portalında bu kuruluş için başvuru yapan müşterilerin bilgileri API üzerinden alınır.

2. Doldurulan formun özet değeriyle daha önce başka bir kuruluşun blok zincir üzerinde doğrulama gerçekleştirip gerçekleştirmediği Şekil 3.6'da yer alan modül üzerinden kontrol edilir.

3. Eğer başvuru yapılan formun özet değeriyle blok zincirde doğrulanmış bir kayıt bulunuyorsa söz konusu kimlik verilerinin daha önce doğrulandığı anlaşıldığından tekrar KYC doğrulama

işlemleri yapılmaz müşteri doğrudan kabul edilir. Eğer başvuru yapılan form verilerinin daha önce doğrulanmadığı görülürse kuruluş tarafından KYC doğrulama işlemleri yapılır ve işlemler tamamlandıktan sonra blok zincire doğrulama yapıldığı bilgisi kaydedilir.




**Şekil 3.6:** Kuruluş, kuruluş portalından müşterinin bilgilerini inceleyerek doğrulama yapar.

Bu modelde blok zincir teknolojisi sadece merkezi olmayan başvuru ve doğrulama bilgisinin alışverişi için kullanılmaktadır. KYC bilgileri, kuruluşlarda merkezi olarak depolanmaktadır. Müşteri tarafından kimlik verilerinin organizasyona aktarılması için API'lar kullanılırken, blok zincir ise doğrulama bilgisinin kimlik bilgilerinin özet değeriyle birlikte kaydedilmesi için kullanılmaktadır.

### 3.3.3. Verileri Blok Zincir Dışında Tutmanın Avantajları

İki model geliştirilirken hangi verilerin blok zincirde hangi verilerin blok zincir dışında tutulması gerektiğine yönelik analiz çalışması yapılmıştır. İkinci modelde müşteriye ait tüm kimlik verilerinin blok zincir dışında tutulmasının etkili bir çözüm olacağı üzerinde durulmuştur. Bu çözümün, kişisel veriler hakkındaki düzenlemelere uyumu sağlamasıyla birlikte blok zincirde saklanması gereken verileri azaltarak performansı da artıracağı öngörülmektedir. Kimlik verilerini blok zincir dışında, bir ilişkisel veritabanında saklayarak blok zincirin performansı artırılacak ve gelecekte depolama yükü oluşmasının önüne geçilecektir.

# 4. BULGULAR

Bu bölümde, önceki bölümde açıklanan iki KYC modeli kişisel veriler hakkındaki düzenlemelere uyum, performans ve güvenlik bakımından karşılaştırılmıştır.

## 4.1. KİŞİSEL VERİLERİN KORUNMASI DÜZENLEMELERİNE UYUM

Bir KYC uygulaması kimlik bilgileri içermesi sebebiyle kişisel veriler hakkındaki yasalara ve düzenlemelere uyumlu olarak tasarlanmak zorundadır. Kişisel verileri kaydeden blok zincir çözümlerinde, paylaşılması gereken veri miktarını en aza indirmek, hem kimlik sahibi hem de kimlik doğrulayıcı için daha güvenli olacaktır. Kimlik sahibinin, gereksiz veya hassas olabilecek verileri paylaşmaması ve kimlik doğrulayıcının da bunları blok zincir üzerinde saklamaması en doğrusudur. Böylece kişisel verileri koruma düzenlemelerinin gerekliliklerine uyum sağlanması kolaylaşacaktır.

Uygulanan birinci modelde müşterilerin verileri blok zincir üzerinde tutulmakta olup müşterinin rızası olması koşuluyla diğer kuruluşlar tarafından görüntülenebilmektedir. Bu özelliği sayesinde kişisel verilerin korunması hakkındaki düzenlemelerin açık rıza şartını yerine getirmiş olmaktadır. Ancak blok zincirin değiştirilemez ve silinemez olması sebebiyle müşterinin bu yöndeki taleplerinin karşılanması mümkün olamayacaktır veya bu talepleri karşılayabilmek için blok zincir, üzerinde belirlenen belirli kurallara göre sürekli yeni bir zincir oluşturularak değiştirilecektir.

Uygulanan ikinci model blok zincirde kişisel veri tutulmaması sayesinde kişisel veriler hakkındaki düzenlemelere uyumlu olacaktır. Müşterilerin verilerinin ancak müşterinin başvurusu ile ilgili kuruluşun kendi kaynaklarında tutulması sayesinde kişisel veriler hakkındaki düzenlemelere uyum kuruluşun kendi sorumluluğunda olacak ve müşterinin verileri hakkında bilgi alma ve bunların silinmesi talepleri karşılanabilecektir.

Aşağıdaki tabloda, kimlik verileri içeren sistemlerin Kişisel Verileri Koruma Kanunu'nun gereklerini yerine getirebilmesi için sağlaması gereken kriterler ile geliştirilen modellerin bu kriterleri karşılama durumları değerlendirilmektedir.

**Tablo 4.1:** Kişisel Verileri Koruma Kanunu'na uyum.

| Kriter | Karşılıyor mu? | |
|---|---|---|
| | **1. Model: Kimlik verileri blok zincirde** | **2. Model: Kimlik verileri blok zincir dışında** |
| Bir kişinin kendisiyle ilgili bütün kişisel veriler hakkında bilgi edinebilmesinin sağlanması | Evet | Evet |
| Kişisel verilerin belirlenerek kişiye sunulabilmesi | Evet | Evet |
| Kişinin isteğine bağlı olarak verilerinin değiştirilebilmesi ya da silinebilmesi | Hayır | Evet |
| Diğer kuruluşlarla veri paylaşımının ancak kişinin açık rızası alınarak gerçekleştirilebilmesi | Evet | Evet |

## 4.2. PERFORMANS DEĞERLENDİRMESİ

Modeli geliştirilen iki uygulama Mac OS işletim sistemine sahip, Intel Core i5 1.8 Ghz çift çekirdekli işlemcisi, 4 GB hafızası ve 128 GB SSD diski olan bir bilgisayar üzerinde test edilmiştir. Blok zincire yazma işlemi gerektiren fonksiyonlarda işlem imzalama için Metamask eklentisi kullanılması sırasında hesap anahtarları açılan bir Metamask penceresi üzerinden girilmektedir. Bu durum performans ölçülmesinde doğru olmayan sonuçlar oluşmasına sebep olabileceği için performans testleri sırasında hesap anahtarları uygulamaların kaynak koduna eklenmiş ve Ethereumjs-tx kütüphanesinden faydalanılarak işlem imzalama gerçekleştirilmiştir. İkinci modelde kimlik verilerinin kaydedileceği ilişkisel veritabanı olarak ise MySQL tercih edilmiştir.

Birinci modelin kimlik verilerini blok zincire yazma ve okuma; ikinci modelin ise kimlik verilerini MySQL veritabanına, özet değerini ise blok zincire yazma ve okuma fonksiyonları uygulama üzerinden test edilerek iki model için de alınan sonuçların ortalaması milisaniye cinsinden aşağıdaki tabloda sunulmuştur. Yazma işlemleri sırasında gas fiyatı olarak 10 Gwei ve gas limiti olarak 300000 belirlenmiştir. Testler için kullanılan blok zincir ağı önceki bölümde

açıklanan Ganache CLI ağıdır. Bu ağda tek bir düğüm üzerinden işlemler gerçekleştirilmekte olup, herhangi bir mutabakat işlemi olmaksızın veriler blok zincire anlık olarak yazılmaktadır. Tablo 4.2 , 4.3 ve 4.4'te yer alan veriler yazma ve okuma fonksiyonları ile yazılıp okunarak işlem süresi ölçülmüştür. Tablo 4.2'de görüldüğü üzere birinci modelin müşteri veri yapısında yedi değişken bytes32 veri tipinde tanımlanmıştır. Ethereum blok zincirinde Solidity dili ile yazılan akıllı sözleşmelerde bir fonksiyona parametre olarak verilebilecek veri boyutu sınırlıdır. Bu sebeple, bu sorunu aşmak için bu yedi alan string yerine bytes32 veri tipinde tanımlanmıştır. Bu durum, Ethereum blok zincirinin yüksek hacimde veri saklanmasına uygun olarak tasarlanmadığını göstermektedir. Bunun sonucunda, verilerin özet değerinin blok zincirde saklandığı ikinci modelin Ethereum blok zinciri yapısına daha uygun olduğu anlaşılmaktadır.

**Tablo 4.2:** Birinci modelin blok zincir akıllı sözleşmesindeki müşteri veri yapısı.

| Değişken | Veri Tipi |
|---|---|
| id | string |
| tcno | uint |
| ad | string |
| soyad | string |
| cinsiyet | bytes32 |
| dogumy | bytes32 |
| dogumt | bytes32 |
| ikamet | bytes32 |
| telno | bytes32 |
| eposta | bytes32 |
| kurulus | bytes32 |

**Tablo 4.3:** İkinci modelin blok zincir akıllı sözleşmesindeki müşteri veri yapısı.

| Değişken | Veri Tipi |
|---|---|
| id | string |
| kycHash | string |
| kurulus | string |
| kycOnay | string |

**Tablo 4.4:** İkinci modelin MySQL veritabanındaki müşteri tablosuna ait alanlar.

| Değişken | Veri Tipi |
|---|---|
| kyc_id | varchar(45) |
| kyc_tcno | varchar(11) |
| kyc_ad | varchar(45) |
| kyc_soyad | varchar(45) |
| kyc_cinsiyet | varchar(45) |
| kyc_dogumy | varchar(45) |
| kyc_dogumt | varchar(45) |
| kyc_ikamet | varchar(120) |
| kyc_telno | varchar(45) |
| kyc_eposta | varchar(45) |
| kyc_hash | varchar(120) |

Bu uygulamada Ganache CLI ağı kullanılması sebebiyle işlem süresinin oldukça kısa olduğu, MySQL ile yakın performanslar oluştuğu anlaşılmaktadır. Gelecek çalışmalarda yapılacak testlerde, daha doğru sonuçlar alabilmek için bu araç kullanılmadan birden fazla düğümden oluşan özel blok zincir ağları kullanılmalıdır. Ayrıca, (Chen ve diğ., 2018) MySQL veritabanı ile özel Ethereum blok zincirinin performanslarını karşılaştırdıkları çalışmalarında MySQL veritabanının daha yüksek performans gösterdiği sonucuna ulaşmışlardır. Bu tez kapsamında, test edilen iki model için kaydedilen verilerin boyutları sınırlıdır. Bundan sonra yapılacak çalışmalarda, MySQL veritabanı ile blok zincirin performans değerlendirmesinin yüksek hacimli verilerle gerçekleştirilmesinin yerinde olacağı değerlendirilmektedir.

**Tablo 4.5:** İki modelin Ganache CLI blok zinciri ve MySQL veritabanındaki performanslarının karşılaştırması.

| Model | Fonksiyon | İşlem Süresi (ms) |
|---|---|---|
| Kimlik verileri blok zincirde | Kimlik verilerini blok zincire yazma | 0,739 |
| | Kimlik verilerini blok zincirden okuma | 0,807 |
| Kimlik verileri blok zincir dışında | Kimlik verilerinin özet değerini blok zincire yazma | 0,522 |
| | Kimlik verilerinin özet değerini blok zincirden okuma | 0,710 |
| | Kimlik verilerini MySQL veritabanına yazma | 1,051 |
| | Kimlik verilerini MySQL veritabanından okuma | 0,404 |

Ganache CLI tek bir düğümden oluşması ve mutabakat mekanizması olmaksızın çalışmasıyla tasarladığımız konsorsiyum blok zincirine uygundur. Bunun yanında, tasarladığımız uygulamaların açık bir Ethereum blok zincirinde çalışması durumunda elde edilecek

performansı ölçmek için Ethereum'un Rinkeby test ağı üzerinde aynı testler tekrarlanmıştır. Aşağıdaki tabloda alınan sonuçlar yer almaktadır.

**Tablo 4.6:** İki modelin Ganache CLI ve Rinkeby blok zincirleri üzerindeki performanslarının karşılaştırması.

| Model | Fonksiyon | Blok Zincir | İşlem Süresi (ms) |
|---|---|---|---|
| Kimlik verileri blok zincirde | Kimlik verilerini blok zincire yazma | Ganache CLI | 0,739 |
| | Kimlik verilerini blok zincirden okuma | Ganache CLI | 0,807 |
| | Kimlik verilerini blok zincire yazma | Rinkeby | 25554,310 |
| | Kimlik verilerini blok zincirden okuma | Rinkeby | 25,827 |
| Kimlik verileri blok zincir dışında | Kimlik verilerinin özet değerini blok zincire yazma | Ganache CLI | 0,522 |
| | Kimlik verilerinin özet değerini blok zincirden okuma | Ganache CLI | 0,710 |
| | Kimlik verilerinin özet değerini blok zincire yazma | Rinkeby | 27601,393 |
| | Kimlik verilerinin özet değerini blok zincirden okuma | Rinkeby | 24,827 |

Ethereum'un test ağlarından birisi olan Rinkeby herkese açıktır ve PoA (Proof of Authority) mutabakat mekanizmasını kullanmaktadır. Rinkeby ağına uygulama üzerinden Infura API'ı[8] ile bağlantı sağlanmıştır. Tablo 4.6'daki sonuçlardan da görülebileceği üzere Rinkeby test ağında blok zincire yazma işlem süresi birinci model için 25,55 ikinci model için ise 27,6 saniye gibi uzun sürelerdir. Ganache CLI ağında alınan sonuçlar ile Rinkeby ağında alınan sonuçlar karşılaştırıldığında özel bir blok zincir kullanmanın açık bir blok zincire olan avantajları açıkça görülebilmektedir.

## 4.3. GÜVENLİK DEĞERLENDİRMESİ

Bir önceki bölümde bankaların ve diğer finans kuruluşlarının düğümleri oluşturduğu blok zincir üzerinde çalışan iki ayrı model açıklanmıştır. Bu iki model de Ethereum test ağında test edilmiş olmakla birlikte düğümlerin yalnızca finans kuruluşlarından oluşması sebebiyle izinli ve konsorsiyum blok zincirlere birer örnektir.

Kimlik verilerinin tüm blok zincir düğümlerine kopyalandığı blok zincirlerde güvenlik riski artmaktadır. Her düğümün güvenlik uygulamalarının aynı seviyede olmaması sebebiyle, bu durumun saldırganların verileri çalmasını kolaylaştırma ihtimali vardır. Bu sebeple kimlik

[8] https://infura.io/

bilgilerinin blok zincirde saklanmadığı ikinci modelin birinci modele göre daha güvenli olduğu değerlendirilmektedir. Ancak blok zincire dahil olan her kuruluşun kendi müşterilerinin verilerini kendi veritabanlarında saklaması gerekeceğinden kendi alt yapılarının güvenliğinin de sağlanması gerekmektedir ve bu her kuruluşun kendi sorumluluğunda olacaktır. Bu bölümde, tasarladığımız iki modelin bilinen bazı blok zincir saldırılarına dayanıklılıkları değerlendirilmiştir.

### 4.3.1. Sybil Atak

Sybil saldırısı ile bir madenci ağda birden fazla sanal düğüm yaratmakta olup bu düğümler ağda hatalı bir işlem için olumlu oylama gibi yanlış bilgiler enjekte ederek seçim sürecini bozabilmektedir (Conti ve diğ., 2018). Özel veya konsorsiyum gibi izinli blok zincirlerde sadece belli sayıdaki bilinen katılımcılar blok zincirin tümüne sahiptir (Walport, 2016). Katılımcılar bilindiğinden, bir Sybil saldırısı riski yoktur, bu nedenle mutabakat mekanizması için oy birliği kullanılmaktadır ve bu sayede, kapalı blok zincirler açık blok zincirlerden çok daha yüksek bir performansa sahiptir (Ali ve diğ., 2019).

Tasarladığımız iki modelde de blokların oluşturulması konusunda fikir birliğine varmak oldukça basittir ve karmaşık işlemler gerektirmez. Yapılan KYC incelemesi neticesinde müşterinin kimlik doğrulaması yapılmakta, yasal düzenlemelere aykırı bir durum bulunmuyorsa müşteri kuruluş tarafından kabul edilmekte ve blok zincire bu bilgi kaydedilmektedir. Düğümler yasal düzenlemelere tabi güvenilir finans kuruluşlarından oluşmaktadır. Bir finans kuruluşunun blok zincirde yanlış bilgiler yayması ihtimali oldukça düşüktür. Böyle bir durumda tabi olduğu düzenlemeler gereği finans kuruluşunun ağır cezalar alması söz konusu olacaktır.

### 4.3.2. %51 Atağı

Kötü niyetli bir düğüm, blok zincir ağın yüzde 51'ini kontrol ederse, bu durumun işlemlerin olması gerektiği gibi doğrulanamaması ve sonuç olarak blok zincire yanlış bilgi eklenmesi ile sonuçlanabileceği düşünülmektedir. PoW mutabakat mekanizmasını kullanan blok zincirler, kullanıcının ağdaki işlem gücünün %51'ini kontrol ettiği senaryolarda savunmasızdır (Ali, ve diğerleri, 2019). Ethereum blok zincirinin de kullandığı konsensüs algoritmasının PoW olduğu değerlendirildiğinde Ethereum'un bu riski taşıdığını söylemek mümkündür, diğer yandan Ethereum'un PoS konsensüs algoritmasını kullanması üzerine çalışmalar yapılmaktadır.

Bu tez için geliştirilen modellerde ise katılımcılar belirlidir. Ağdaki katılımcıların biri veya birkaçının blok zincirin kontrolünü ele geçirmesi ve yanlış yönlendirmesine karşı kuruluşlar arasında kurulacak konsorsiyum ile önlem alınacağı varsayılmıştır. Tasarladığımız modeller kapalı ve konsorsiyum blok zincirler olduğundan mutabakat mekanizması kullanılmayacağı varsayılmıştır. Böyle bir atak oluşması durumunda ise bunun tespit edilmesi, önlem alınması ve yapılan hatalı işlemlerin geriye alınması açık blok zincirlere göre çok daha kolay olacaktır.

### 4.3.3. Tutulma Atağı

Tutulma atağı, saldırganın kurbanın tüm gelen ve giden bağlantılarını kontrol ederek kurbanı ağdaki diğer katılımcılardan ayırması ile gerçekleşmektedir. Daha sonra, saldırgan, kurbanın blok zincire ilişkin görüşünü değiştirebilmekte veya kurbanın blok zincirinin eski görünümlerinde gereksiz bilgi işlem gücü harcamasına sebep olabilmektedir (Li ve diğ., 2017). Ayrıca, saldırgan kendi kötü niyetli işlemlerini yürütmek için kurbanın bilgi işlem gücünden bu yolla yararlanabilmektedir. Tutulma atağı, ağdaki katılımcılardan kaynaklanabilecek bir atak olarak değerlendirilmektedir ve özellikle açık blok zincirler bu ataktan etkilenmektedir. Belirli katılımcıları olan özel bir blok zincirde bu aktiviteleri gerçekleştiren saldırganın tespit edilmesi oldukça kolaylaşacaktır.

Bu atak ve bu bölümde ele alınan diğer ataklar açık blok zincirlerde önemli sorunlara yol açmaktadır. Ancak belli kurallara uygun çalışan, yasal düzenlemelere tabi güvenilir katılımcılardan oluşan özel blok zincirlerde bu atakların gerçekleştirilmesi ihtimali oldukça düşük olmakla birlikte tespit edilmesi açık blok zincirlere göre çok daha kolay olacaktır. Tasarladığımız modeller değerlendirildiğinde kişisel verilerin veya bunlarla ilişkilendirilebilecek özet değerleri de olsa herhangi bir bilginin korunması için bu modellerin kapalı ve özel blok zincirler üzerinde çalışmasının gerekli olduğu anlaşılmaktadır.

# 5. TARTIŞMA VE SONUÇ

Son yıllarda, teknolojinin gelişimi finansal hizmetler sektörünü de etkilemektedir. Fintech, gelişen bilişim teknolojilerinden faydalanarak, finans kuruluşlarına ve müşterilerine, özel yazılımlar ile finansal operasyonlarını, süreçlerini ve yaşamlarını daha iyi yönetmelerine yardımcı olmak için kullanılmaktadır. Fintech için kullanılmaya başlanan yeni teknolojilerden birisi de blok zincirdir.

Blok zincirin oluşturulmasının temelinde aracı bir kuruma olan ihtiyacı ortadan kaldırarak aynı ağ üzerindeki eşlerin para aktarımını özgür bir şekilde yapabilmesi fikri yatmaktadır. Blok zincir platformlarının, güvenlik ve değişmezlik göz önünde bulundurularak tasarlanmış merkezi olmayan veritabanları sağlamaları sayesinde geleneksel veritabanları üzerinde avantajları vardır. Geleneksel veritabanları da aynı şeyleri sağlayabilir, ancak bu güvenlik özelliklerine sahip dağıtılmış sistemleri kurma maliyetleri blok zincire göre daha fazladır. Blok zincir teknolojisi birçok uygulamada büyük avantajlara sahip olsa da, her şeye uygun bir çözüm olduğunun savunulması mümkün değildir. Bir blok zincir uygulaması gerçekleştirilirken çözüm oluşturulan iş için dağıtılmış bir veri yapısına gerçekten ihtiyaç duyulup duyulmadığının araştırılması gerekmektedir.

Blok zincir teknolojisinin kullanılabileceği alanlardan birisi olarak kimlik yönetimi öne çıkmaktadır. Ancak bu alan blok zincir uygulamalarının gerçekleştirilebileceği en karmaşık alanlardan biri olarak görülmektedir. Kimlik yönetimi, finansal hizmetler vermek üzere KYC gereklerinin sağlanması, dolandırıcılıkla mücadele edilmesi ve güvenilir kredi geçmişlerinin geliştirilmesi alanlarında sağladıkları ile finansal hizmetler sektöründe önemli bir çözümdür. Kimlik yönetimi sistemleri AML normlarına uygun yasal bir yapı oluşturmalı, eşsiz bir kimlik sağlamalı, e-KYC ile uyumlu olacak şekilde dijital altyapı üzerine kurulmalı ve nüfusun tamamına yayılabilmesi için maliyet etkin olmalıdır.

Blok zincir teknolojisi, verilerin bir aracı kurum olmaksızın bir ağdaki varlıklar arasında doğrudan güvenilir bir şekilde paylaşılmasına imkan tanıması sayesinde, finansal hizmetler için düşük maliyetli, kullanım kolaylığı olan güvenli uygulamalar geliştirilmesine yardımcı olmaktadır. Özellikle bankaların ve diğer finans kuruluşlarının müşteri kaydını KYC düzenlemelerine uygun olarak gerçekleştirmek için harcadıkları zaman, maliyetin yüksekliği

ve karşılaşılan zorluklar göz önüne alındığında, blok zincir temelli sistemlerin bu alanda önemli gelişmeler yaşanmasına olanak tanıyacağı değerlendirilmektedir.

Blok zincir ile dijital kimlik sistemleri tasarlanırken özellikle göz önünde bulundurulması gereken bazı hususlar vardır. Birincisi, kimlik verilerinin tüm düğümlere kopyalanması güvenlik riskini artıracaktır. Blok zincire sahip olan her kuruluşun güvenlik uygulamaları aynı seviyede olamayacağı için, bunun saldırganların verileri çalmasını kolaylaştıracağı düşünülmektedir. Verilerin açık bir blok zincirde tutulması durumunda ise blok zincirin silinemez olması sebebiyle veri sahibinin verilerini asla tamamen yok edemeyecek olması kişisel verilerin korunması hakkındaki yasa ve düzenlemelere aykırılık oluşturacaktır.

Blok zincir teknolojisi gelişmiş güvenlik özellikleri ile tasarlansa da her şeyin otomatik olarak doğrulanmasını sağlaması söz konusu değildir. Nihayetinde, herhangi bir bilginin doğruluğu ve gerçekliği, kişisel bilgilerini blok zincire kaydeden bireylere ve blok zincirde tutulan verilerin doğruluğunu denetleme ve onaylama becerisine ve yetkisine sahip olan kuruluşlara ait olacaktır.

Dijital kimlik sistemlerinde özellikle kullanıcının kimlik bilgilerinin korunması önemlidir. Bu sebeple bu tezde, kimlik bilgilerinin güvenliğinin sağlanması amacıyla bu bilgilerin doğrudan blok zincirde tutulmadığı ancak bu verilerin özetlerinin ve kullanıcının kimliğine yöneltilmiş soruların cevaplarının saklandığı ve bunların diğer taraflarla paylaşıldığı bir uygulama gerçekleştirilmiş ve bu verilerin açıkça blok zincirde tutulduğu diğer bir uygulama ile kıyaslanmıştır. Gerçekleştirilen uygulamalar ile bir kez doğrulanmış kimlik verileri için onay bilgisi saklanarak kimlik doğrulaması yapmak isteyen diğer taraflarla da paylaşılabileceği ve bunun da finans kuruluşlarını tekrar doğrulama işlemi yapmaktan kurtaracağı gösterilmiştir. Böylece finans kuruluşlarının KYC işlemlerini daha etkin ve verimli bir şekilde gerçekleştirmesinin de sağlanmış olacağı düşünülmektedir.

Uygulanan modeller kişisel verilerin korunması hakkındaki düzenlemelere uyum, performans ve güvenlik açısından kıyaslandığında kimlik bilgilerinin blok zincir dışında tutulduğu ikinci modelin KYC işlemlerini gerçekleştirmek için daha doğru bir yaklaşım olduğu değerlendirilmiştir.

Uygulaması gerçekleştirilen ikinci modelde kullanılan özet fonksiyonlar tek yönlü olmakla beraber saldırganların fonksiyon çıktısından girdisini tahmin etmeleri mümkün olabileceğinden

potansiyel tehlike oluşturabileceği değerlendirilmektedir. Bu sebeple KYC uygulamalarının açık blok zincirler üzerinde geliştirilmesinin güvenlik açıklarına sebep olabileceği göz önüne alınmalıdır. Tez kapsamında değerlendirilen bazı saldırı türlerinin ise özellikle açık blok zincirleri hedef aldığı görülmüştür. KYC işlemi için gerekli olan kimlik verilerinin hassasiyeti göz önüne alındığında KYC uygulamalarının izne tabi özel veya konsorsiyum blok zincirler üzerinde gerçekleştirilmesinin ve bu blok zincirler üzerinde saklanan verilerin ise sadece doğrulama verileri olmasının uygun olacağı değerlendirilmektedir.

Ganache CLI ağı ve MySQL veritabanının verileri yazma ve okumadaki performansları karşılaştırıldığında özel bir blok zincirin de bir ilişkisel veritabanı gibi yüksek hızlara ulaştığı görülmektedir. Ancak bu tez kapsamında sınırlı bir veri setiyle testler gerçekleştirilmiştir. Bundan sonraki çalışmalarda ilişkisel bir veritabanı ile blok zincirlerin performanslarının yüksek hacimdeki verilerle test edilerek karşılaştırılmasının faydalı olabileceği düşünülmektedir. Diğer yandan, gerçekleştirilen testlerde Solidity'nin veri sınırlandırmasının Ethereum'un blok zincire yazılıp okunabilecek verilerin boyutunu sınırlandırdığı görülmektedir. Her ne kadar bu sınırlandırmayı aşmanın yolları olsa da Ethereum'un yüksek hacimli veri depolamaya uygun tasarlanmadığı anlaşılmaktadır. Gerçek hayattaki uygulamalarında KYC sistemlerinin kimlik bilgileri dışında bu bilgilerin yer aldığı resmi dokümanların elektronik kopyalarının da kaydedileceği şekilde tasarlanması gerektiği değerlendirildiğinde blok zincir dışında bir veri deposunun kullanılması kaçınılmazdır.

Kimlik bilgilerini blok zincirin dışında bir ilişkisel veritabanında saklamak performansı artırarak zamanla oluşacak depolama yükünden blok zinciri kurtaracaktır. Ancak böyle bir veri depolama sistemi, güvenli erişim kontrolünü ve veri gizliliğini sağlayacak şekilde tasarlanmalıdır.

# KAYNAKLAR

Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2019). Applications of Blockchains in the Internet of Things: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials, Vol. 21, No. 2*.

Allen, C. (2016). *The Path of Self Sovereign Identity*. https://www.coindesk.com/path-self-sovereign-identity/, [Ziyaret Tarihi: 30.05.2019].

Belin, O. (2018). *The Difference Between Blockchain & Distributed Ledger Technology*. https://tradeix.com/distributed-ledger-technology/, [Ziyaret Tarihi: 22.11.2018].

Bhaskaran, K., Ilfrich, P., Liffman, D., Vecchiola, C., Jayachandran, P., Kumar, A., . . . Teo, E. G. (2018). Double-Blind Consent-Driven Data Sharing on Blockchain. *2018 IEEE International Conference on Cloud Engineering.*

Birch, D. (2016). *Kimlik: Yeni Para (Orijinal adı: Identity is the New Money, Orijinal yayın tarihi: 2014).* Kapital Medya Hizmetleri A.Ş.

Chen, S., Zhang, J., Shi, R., Yan, J., & Ke, Q. (2018). A Comparative Testing on Performance of Blockchain and Relational Database: Foundation for Applying Smart Technology into Current Business Systems. *Springer, Cham, Lecture Notes in Computer Science, vol 10921*.

Cheng, E. (2018). *Japanese cryptocurrency exchange loses more than $500 million to hackers*. https://www.cnbc.com/2018/01/26/japanese-cryptocurrency-exchange-loses-more-than-500-million-to-hackers.html, [Ziyaret Tarihi: 25.11.2018].

Conti, M., Kumar, S., Lal, C., & Ruj, S. (2018). A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials Vol., 20, No. 4*.

Daryna, P. (2018). *6 Promising Use Cases of Blockchain in FinTech*. https://rubygarage.org/blog/blockchain-use-cases-in-fintech, [Ziyaret Tarihi: 23.11.2018].

Deloitte. (2017). *5 blockchain technology use cases in financial services*. blog.deloitte.com: http://blog.deloitte.com.ng/5-blockchain-use-cases-in-financial-services/, [Ziyaret Tarihi: 23.11.2018].

Deloitte LLP. (2016). *Blockchain Enigma Paradox Opportunity.* https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf, [Ziyaret Tarihi: 12.10.2018].

Deloitte Türkiye. (2017). *Türkiye Fintech Ekosistemi.* https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/finance/turkiye-fintech-ekosistemi.pdf, [Ziyaret Tarihi: 12.10.2018].

Ethereum Foundation. (tarih yok). *web3.js - Ethereum JavaScript API.* https://github.com/ethereum/web3.js/, [Ziyaret Tarihi: 11.03.2019].

EthereumJS. (tarih yok). *A simple module for creating, manipulating and signing ethereum transactions.* https://github.com/ethereumjs/ethereumjs-tx, [Ziyaret Tarihi: 11.03.2019].

EY Türkiye. (2018). *EY Türkiye Fintech Dönüşümü Raporu.* https://www.ey.com/Publication/vwLUAssets/Fintech_Donusumu_Raporu/%24FILE/EY_Turkiye_Fintech_Donusumu_raporu.pdf, [Ziyaret Tarihi: 02.12.2018].

Eyal, I., & Sirer, E. G. (2018). *Majority is not Enough: Bitcoin Mining is Vulnerable.* https://www.cs.cornell.edu/~ie53/publications/btcProcFC.pdf, [Ziyaret Tarihi: 15.11.2018].

Fintechnews Singapore. (2018). *The Evolution of eKYC and Digital Identity in The Age of Blockchain.* http://fintechnews.sg/20937/blockchain/xenchain-digital-identity-kyc/, [Ziyaret Tarihi: 30.11.2018].

FSB. (2017). *Financial Stability Implications from FinTech Supervisory and Regulatory Issues that Merit Authorities' Attention.* http://www.fsb.org/wp-content/uploads/R270617.pdf, [Ziyaret Tarihi: 02.12.2018].

Hileman, G., & Rauchs, M. (2017). *Global Blockchain Benchmarking Study*. ey.com: https://www.ey.com/Publication/vwLUAssets/ey-global-blockchain-benchmarking-study-2017/$File/ey-global-blockchain-benchmarking-study-2017.pdf, [Ziyaret Tarihi: 05.05.2019].

*How does Bitcoin work?* (2018). https://bitcoin.org/en/how-it-works, [Ziyaret Tarihi: 10.10.2018].

*How secure is blockchain really?* (2018). https://www.technologyreview.com/s/610836/how-secure-is-blockchain-really/, [Ziyaret Tarihi: 05.12.2018].

*Kişisel Verilerin Korunması Kanunu.* (2016). https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf, [Ziyaret Tarihi: 05.05.2019].

Li, X., Jianga, P., Chenb, T., Luoa, X., & Wen, Q. (2017). A Survey on the Security of Blockchain Systems. *Future Generation Computer Systems*.

Metamask. (tarih yok). *METAMASK*. metamask.io: https://metamask.io/, [Ziyaret Tarihi: 11.03.2019].

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, [Ziyaret Tarihi: 25.11.2018].

Pinto, R. (2018). *How Blockchain Can Solve Identity Management Problems*. https://www.forbes.com/sites/forbestechcouncil/2018/07/27/how-blockchain-can-solve-identity-management-problems/#795ece8e13f5, [Ziyaret Tarihi: 10.10.2018].

Segovia Domingo, A., & Enríquez, Á. (2018). *Digital Identity: The Current State of Affairs.* https://www.bbvaresearch.com/wp-content/uploads/2018/02/Digital-Identity_the-current-state-of-affairs.pdf, [Ziyaret Tarihi: 01.10.2018].

Siegel, D. (2016). *Understanding The DAO Attack*. https://www.coindesk.com/understanding-dao-hack-journalists, [Ziyaret Tarihi: 15.05.2019].

The Economist. (2015). *The great chain of being sure about things*. https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things, [Ziyaret Tarihi: 01.12.2018].

The Economist. (2016). *Hype springs eternal*. https://www.economist.com/finance-and-economics/2016/03/19/hype-springs-eternal, [Ziyaret Tarihi: 01.12.2018].

The World Bank. (2018). *Blockchain & Distributed Ledger Technology (DLT)*. worldbank.org: https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt, [Ziyaret Tarihi: 22.11.2018].

Thomson Reuters. (2017). *Thomson Reuters 2017 Global KYC Surveys Attest to Even Greater Compliance Pain Points.* thomsonreuters.com: https://www.thomsonreuters.com/en/press-releases/2017/october/thomson-reuters-2017-global-kyc-surveys-attest-to-even-greater-compliance-pain-points.html, [Ziyaret Tarihi: 03.12.2018].

*Top Three Blockchain Platforms You Must Know About*. (2018). https://dzone.com/articles/best-3-blockchain-platforms-you-must-know-about, [Ziyaret Tarihi: 15.11.2018].

Toronto Centre. (2017). *FinTech, RegTech and SupTech: What They Mean for Financial Supervision.* https://res.torontocentre.org/guidedocs/FinTech RegTech and SupTech - What They Mean for Financial Supervision.pdf, [Ziyaret Tarihi: 31.10.2018].

Truffle Suite. (tarih yok). *Fast Ethereum RPC client for testing and development.* github.com: https://github.com/trufflesuite/ganache-cli, [Ziyaret Tarihi: 11.03.2019].

Usta, A., & Doğantekin, S. (2018). *Blockchain 101 v2.* BKM.

Walport, M. (2016). *Distributed Ledger Technology: beyond block chain.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf, [Ziyaret Tarihi: 08.06.2019].

Wang, L., Shen, X., Li, J., Shao, J., & Yang, Y. (2019). Cryptographic primitives in blockchains. *Journal of Network and Computer Applications*.

William, J. (2016). *Financial Technology.* CreateSpace Publishing.

World Economic Forum. (2016). *A Blueprint for Digital Identity -The Role of Financial Institutions in Building Digital Identity*. http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf, [Ziyaret Tarihi: 30.11.2018].

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain Technology Overview*. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf, [Ziyaret Tarihi: 04.12.2018].

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain Challenges and Opportunities: A Survey. *Int. J. Web and Grid Services, Vol. 14, No. 4*.

# ÖZGEÇMİŞ

| Kişisel Bilgiler | |
|---|---|
| Adı Soyadı | Hatice KARAYILAN |
| Doğum Yeri | İspir / Erzurum |
| Doğum Tarihi | 12.06.1984 |
| Uyruğu | ☑ T.C. ❒ Diğer: |
| Telefon | 05326248200 |
| E-Posta Adresi | karayilanhb@gmail.com |
| Web Adresi | |

| Eğitim Bilgileri<br>Lisans | |
|---|---|
| Üniversite | İstanbul Üniversitesi |
| Fakülte | Mühendislik Fakültesi |
| Bölümü | Bilgisayar Mühendisliği |
| Mezuniyet Yılı | 2006 |

| Yüksek Lisans | |
|---|---|
| Üniversite | İstanbul Üniversitesi-Cerrahpaşa |
| Enstitü Adı | Lisansüstü Eğitim Enstitüsü |
| Anabilim Dalı | Bilgisayar Mühendisliği Anabilim Dalı |
| Programı | Bilgisayar Mühendisliği |

| Makale ve Bildiriler |
|---|