T.C.
ERCİYES ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI

ELEKTRONİK ÖDEMELERDE BLOK ZİNCİRİ SİSTEMATİĞİ VE UYGULAMALARI

Hazırlayan
İmparator S. KARAKÖSE

Danışman
Doç. Dr. Veli AKEL

Yüksek Lisans Tezi

Eylül 2017
KAYSERİ

T.C.
ERCİYES ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI

ELEKTRONİK ÖDEMELERDE BLOK ZİNCİRİ SİSTEMATİĞİ VE UYGULAMALARI

(Yüksek Lisans Tezi)

Hazırlayan
İmparator S. KARAKÖSE

Danışman
Doç. Dr. Veli AKEL

Eylül 2017
KAYSERİ

BİLİMSEL ETİĞE UYGUNLUK

Bu çalışmadaki tüm bilgilerin, akademik ve etik kurallara uygun bir şekilde elde edildiğini beyan ederim. Aynı zamanda bu kural ve davranışların gerektirdiği gibi, bu çalışmanın özünde olmayan tüm materyal ve sonuçları tam olarak aktardığımı ve referans gösterdiğimi belirtirim.

İmparator S. KARAKÖSE

YÖNERGEYE UYGUNLUK

"**Elektronik Ödemelerde Blok Zinciri Sistematiği ve Uygulamaları**" adlı Yüksek Lisans tezi, Erciyes Üniversitesi Lisansüstü Tez Önerisi ve Tez Yazma Yönergesine uygun olarak hazırlanmıştır.

Hazırlayan
İmparator S. KARAKÖSE

Danışman
Doç. Dr. Veli AKEL

İşletme Anabilim Dalı Başkanı
Prof. Dr. A. Asuman AKDOĞAN

KABUL ONAY SAYFASI

Doç. Dr. Veli AKEL danışmanlığında İmparator KARAKÖSE tarafından hazırlanan "Elektronik Ödemelerde Blok Zinciri Sistematiği ve Uygulamaları" adlı bu çalışma jürimiz tarafından Erciyes Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalında **Yüksek Lisans** tezi olarak kabul edilmiştir.

03/09/2017

JÜRİ:

Danışman : Doç. Dr. Veli AKEL .....

Üye : Prof. Dr. Erk HACIHASANOĞLU .....

Üye : Prof. Dr. Levent ÇITAK .....

ONAY:

Bu tezin kabulü Enstitü Yönetim Kurulunun 27/10/2017 tarih ve 34 sayılı kararı ile onaylanmıştır.

27/10/2017

Prof. Dr. Celalettin CELİK

Enstitü Müdürü

ELEKTRONİK ÖDEMELERDE
BLOK ZİNCİRİ SİSTEMATİĞİ VE UYGULAMALARI

İmparator S. KARAKÖSE

Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Eylül 2017

Danışman: Doç. Dr. Veli AKEL

ÖZET

Elektronik ödemeler, merkezi yapılar ile yakından ilişkili ve bağlıdır. Bu, elektronik ödemelerin kullanımı ve koordineli çalışmaları için düzenleyiciler tarafından beklenen bir gerekliliktir. Elektronik ödemeler bir merkeze bağlı olmaksızın en çok blok zinciri teknolojisi kullanılarak gerçekleştirilmektedir. Bu tez, blok zinciri teknolojisinin elektronik ödemeler alanındaki fonksiyonu ve etkisi hakkında genel bir bakış sunmaktadır. Blok zinciri, işlemlerin kaydedilmesi ve varlıkların bir ağda izlenme sürecini kolaylaştıran, paylaşılan ve dağıtık bir kayıt şeklidir. Blok zinciri sistemi, A'dan B'ye herhangi bir aracı olmaksızın kripto para transferi sağlamasının yanında birçok farklı imkanlar da sunmaktadır. Blok zinciri sistemi, tek bir noktadan işlemlerin yapılmasına imkan verirken, işlem masrafları ve süre açısından da önemli tasarruflar sağlamaktadır. İşte bu çalışmada geleneksel ekonomik yapıyı belirli alanlarda değiştirebilecek bir sistem olan blok zinciri sistematiği tanıtılmaya çalışılmıştır. Blok zinciri teknolojisinin altında yatan temel kavramlar ve kripto paraların arkasındaki dağıtık yapı açıklanmakta olup, sistemin finansal uygulama alanları üzerinde odaklanılmıştır. Ayrıca blok zinciri gelişimi ve kullanımı ile ortaya çıkan yeni durumlar da değerlendirilmiştir. Bu tez, blok zinciri teknolojisinin finansal sektörü özellikle elektronik ödemeler alanında nasıl etkilediğini incelemek amacıyla, teorik bir çerçeve ve terminolojinin oluşturulmaya çalışıldığı tanıtıcı niteliğe sahip bir çalışma olarak değerlendirilmelidir.

Anahtar Kelimeler; Blok Zinciri, Kripto/Sanal/Dijital Para, Elektronik Para, Dağıtımlı/Dağıtık Hesap/Kayıt/İşlem Teknolojisi, Elektronik Ödeme, Bitcoin, Ethereum, Hyperledger, Eşten Eşe Mutabakat, Kriptografi.

THE BLOCKCHAIN SYSTEMATICS AND APPLICATIONS IN ELECTRONIC PAYMENTS

İmparator S. KARAKÖSE

Erciyes University Institute for Social Sciences, M.Sc. Thesis, September 2017

Advisor: Assoc. Prof. Veli AKEL

ABSTRACT

Electronic payments are closely related and connected to central institutions. This is an expected requirement by regulators for the use of electronic payments and for coordinated work. Regardless of a center, electronic payments are operated by mostly using blockchain technology. This thesis provides an overview of the functions and effects of blockchain technology in field of electronic payments. Blockchain is a shared distributed form of recording that facilitates the process of recording transactions and monitoring assets in a network. The system has not a center, it provides crypto money transfer from A to B without a third party and many other possibilities. While the block chain system can be operated from a point where it is used, it significantly economizes the duration and operation costs. The system which is explained with blockchain that can innovate traditional economic structure in specific areas. This thesis focuses on explaining its financial application areas, conceptualizing blockchain technology and its distributed computing technology behind the cryptocurrency. It also assesses situations that arise with the development and use of blockchain. This thesis is based on literature review, attempted to establish a theoretical framework and terminology to examine how blockchain technology affects the financial sector, especially in field of electronic payments.

Keywords; Blockchain, Crypto / Virtual / Digital Currency, Electronic Money, Distributed Ledger Technology, Electronic Payment, Bitcoin, Ethereum, Hyperledger, Peer to Peer Consensus, Cryptography.

İÇİNDEKİLER

Sayfa

KISALTMALAR

API : Uygulama Programlama Arayüzü: Application Programming Interface

ASIC :Uygulamaya Özgü Bütünleşik Devre: Application Specific Integrated Circuit

BDDK : Bankacılık Düzenleme ve Denetleme Kurumu

BIS : Uluslararası Ödemeler Bankası: Bank for International Settlements

BKM : Bankalararası Kart Merkezi A.Ş.

BCH : Bitcoin Cash

BTC : Bitcoin

BTOM : Bankalararası Takas Odaları Merkezi

CHIPS : Bankalararası Kliring Odası Ödeme Sistemi: Clearing House Interbank Payments System

CPU : Merkezi İşlem Birimi: Central Processing Unit

ECB : Avrupa Merkez Bankası: European Central Bank

ETC : Ethereum Classic

ETH : Ethereum

FPGA : Alanda Programlanabilir Kapı Dizileri: Field Programmable Gate Array

GPU : Grafik İşleme Birimi: Graphics Processing Unit

GÖSAŞ : Garanti Ödeme Sistemleri A.Ş.

DAO : Ademi Merkezi Otonom Organizasyon: Decentralized Autonomous Organization

DLT : Dağıtık Kayıt Teknolojisi: Distributed Ledger Technology

DSA : Dijital İmza Algoritması: Digital Signature Algorithm

DTCC : ABD Mevduat Muhafaza ve Takas Şirketi: Depository Trust & Clearing Corporation

EFT : Elektronik Fon Transferi: Electronic Funds Transfer

EMKT : Elektronik Menkul Kıymet Transfer Sistemi

EPC : Avrupa Ödemeler Konseyi: European Payments Council

FINTECH : Finansal Teknoloji: Financial Technology

FSB : Finansal İstikrar Kurulu: Financial Stability Board

IACR : Uluslararası Kriptolojik Araştırmalar Birliği: International Association for Cryptologic Research

ICO : "Coin / Sikke" Halka Arzı: Initial Coin Offering

IETF : İnternet Mühendisliği Görev Grubu: Internet Engineering Task Force

ICANN : İnternet Tahsisli Sayılar ve İsimler Kurumu: Internet Corporation for Assigned Names and Numbers

IoT : Nesnelerin İnterneti: Internet of Things

IP : İnternet Protokolü: Internet Protocol

IPO : Halka açılma: Initial Public Offering

MBKP : Merkez Bankası Kripto Paraları: Central Bank Cryptocurrencies

MKK : Merkezi Kayıt Kuruluşu A.Ş.

MPTS : Mastercard Payment Transaction Services Turkey Bilişim Hiz. A.Ş.

NIST : Ulusal Standartlar ve Teknoloji Enstitüsü: National Institute of Standards and Technology

P2P : Eşten eşe: Peer to Peer

PBFT : Pratik Bizans Hata Toleransı: Practical Byzantine Fault Tolerance

PoA : Otorite Kanıtlaması: Proof of Authority

PoS : Pay Kanıtlaması: Proof of Work

PoW : İş Kanıtlaması: Proof of Work

RTGS : Gerçek Zamanlı Mutabakat: Real Time Gross Settlement System

SDR : Özel Çekme Hakki: Special Drawing Right

SegWit : Segregasyonlu Tanık: Segregated Witness

SHA : Güvenli Hash Algoritması: Secure Hash Algorithm

SWIFT : Dünya Bankalararası Finansal İletişim Kuruluşu: Society for Worldwide Interbank Financial Telecommunication

TCMB : Türkiye Cumhuriyet Merkez Bankası

WEF : Dünya Ekonomik Formu: World Economic Forum

ŞEKİLLER LİSTESİ

Sayfa

GİRİŞ

Finans alanındaki teknolojik gelişmeler, finans dünyasının sürekli gelişen ve değişen yapısı için büyük önem taşımaktadır. Finansal teknolojiler, değişen talepler için önemli ve etkin roller üstlenmektedir. Düzenleyici otoriteler, bu hızlı değişimler karşısında dikkatli bir şekilde verimlilik ve istikrar dengesini gözeterek finansal piyasaları düzenlemek istemektedir. Günümüzde finansal teknolojilerinin adaptasyonu çok hızlı gerçekleşebilmektedir. Finansal teknolojilerin uluslararası finans piyasalarını etkileyebilme süresi gittikçe azalmaktadır. Bu nedenle finans alanındaki teknolojik gelişmelere duyarlı olabilmek amacıyla, bazı durumlarda otoriteler, uluslararası işbirliklerini ve para sistemlerini araç olarak kullanmaktadır. Bu bağlamda elektronik ödemeler, modern ödeme anlayışında hayati bir önem taşımaktadır. Genel anlamda finansal hizmetler, elektronik ödemelerden ve farklı finansal işlemlerden doğacak tüm finansal ihtiyaçların karşılanması amaçlamaktadır. Finansal teknolojiler ise finansal hizmetler alanında kullanılan modern teknolojilerin tamamından oluşmaktadır. Finansal teknolojiler, finansal hizmetlerinin biçimlendiricisi olarak, ayrıca finansal hizmetlerin dijitalleşmesini de sağlamaktadır.

Finansal hizmetlerdeki güven, maliyet ve birçok farklı açıdan gelecek kaygılarının artmasıyla birlikte finansal teknolojiler terimi daha da değer kazanmaktadır. Blok zinciri (Blockchain) teknolojisi işlemlerin daha ekonomik bir şekilde gerçekleştirilebilmesini sağlamaktadır. Blok zinciri teknolojisi birçok farklı alanda kullanılacağı gibi en yaygın olarak finansal hizmetler alanında kullanılmaktadır. Blok zincirinin kullanıldığı en popüler örnek kripto para yapılarıdır ve yasal durumu otoritelere göre farklılık göstermektedir. Blok zinciri teknolojisi ve dağıtık kayıt teknolojisi (DLT[1], Distributed Ledger Technology) literatürde genellikle birbirinin yerine kullanılmaktadır. Blok zinciri teknolojisi, dağıtık bir sistem olarak dağıtık kayıt oluşturma yöntemidir. Blok

[1] DLT; (Distributed Ledger Technology) dağıtımlı/dağıtık bir kayıt/hesap teknolojisidir. Ledger, finans literatüründe "hesap" için kullanılan ortak bir terim olup, ayrıca defter-i kebir, hesap defteri, işlem kayıtlarının kopyası gibi anlamlarda da kullanılmaktadır.

zinciri, elektronik ödemelerde uzlaşma için bir aracıya ihtiyaç duymamaktadır. Sistemi kullanan herkes işlemlerin sahibi ve takipçisi konumunda olabilmektedir. Araştırma, ödemelerde blok zincir teknolojisi ile eşten eşe [2] ödemelerdeki değişiklikleri açıklamaktadır. Blok zinciri ile dağıtık ya da ademi merkezi[3] otonom organizasyon (DAO, Decentralized Autonomous Organization) yapısına sahip birçok alanda kullanılabilecek uygulamalar geliştirilebilmektedir. DLT'lerin, iş hacmi ve kaynakların kullanımı üzerindeki etkisi, uygulamaya göre değişiklik göstermektedir.

Klasik para birimi kavramının dışına çıkan blok zincirine dayanabilen para birimleri, sıklıkla kripto para, dijital para veya sanal para birimleri olarak adlandırılmaktadır. Bu tezde, elektronik ödemeler alanında blok zinciri sistematiğinin karakterize ettiği işlemler değerlendirilmektedir. Bu amaçla ilk olarak para ve elektronik ödeme sistemleri hakkında bilgi verildikten sonra, blok zincir sistematiği tanıtılmış olup bu teknolojinin ödeme işlemlerindeki işleyiş yapısı üzerinde durulmuştur. Son bölümde ise blok zincirinin finans alanında kullanımına ilişkin uygulamalar hakkında bilgi verilmiştir. Böylece blok zincirinin fonksiyonlarını değerlendirmek ve tanıtmak üzere hazırlanan bu tezin literatüre katkı sağlayacağı değerlendirilmektedir.

[2] Eşten eşe; (P2P, Peer-to-Peer) işler arası veri paylaşımı sağlayan dağıtık bir uygulama mimarisidir.
[3] Ademi merkezi; Merkezsiz, merkezi olmayan.

BİRİNCİ BÖLÜM

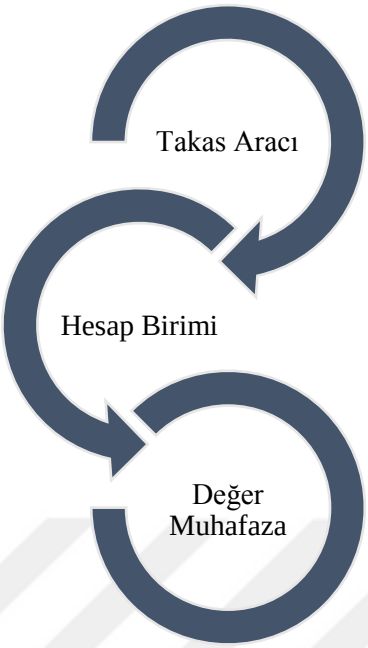
PARA VE ELEKTRONİK ÖDEME SİSTEMLERİ

Para kavramı uzun zamandır farklı yönleri ile tartışılmaktadır. Bu tartışmalara ek olarak yeni para yapıları eklenmektedir. Para yapıları, modern ekonomilerdeki en önemli ekonomik değerlerden biridir. Para, yazında oldukça farklı biçimlerde tanımlanmıştır. Finansal yeniliklerle gündeme gelen birçok para yapıları, ekonomik ya da hukuksal terimler yerine günümüzde daha çok teknolojik kavramlarla açıklanmaktadır.

Paranın çok hızlı bir şekilde geçirdiği niteliksel ve niceliksel değişim süreci, sabit ve değişmeyen bir para tanımının yapılabilmesinin önüne geçmektedir. Ekonomik kullanımlar ve alışkanlıklar sürekli değişiklik gösterdiğinden dolayı paranın kesin bir tanımını da yapmak mümkün olmamaktadır. Ekonomistler arasında paranın nasıl tanımlanacağı konusunda bir görüş birliği de bulunmamaktadır. Bununla birlikte, 19. yüzyılda önce altın ve gümüş daha sonra ise banknot ve çeke bağlı vadesiz mevduat, para tanımı kapsamına girmiştir. Günümüzde para tamının içine bazı aktifler de alınmaktadır. Bunların arasında ticari bankaların vadeli mevduatları, tasarruf sandıklarının mevduatları (banka olmayan mali aracı) sayılabilmektedir (Parasız, 2005: 12-13). Bununla birlikte para, her gecen gün daha da kaydileşmektedir.

Literatürde para, biçimine bakılmaksızın geleneksel olarak üç farklı işlev ile ilişkilendirilmektedir:

- **Takas aracı:** Para, takas sisteminin verdiği rahatsızlıktan kaçınmak için ticarette aracı olarak kullanılır, diğer bir deyişle işlemde yer alan iki taraf arasında bir araya gelme ihtiyacını karşılamaktadır.
- **Hesap birimi:** Para, malların, hizmetlerin, varlıkların ve yükümlülüklerin değer ve maliyetlerinin ölçümü için standart bir sayısal birim görevi görmektedir.
- **Değer muhafaza:** Para saklanabilmekte ve gelecekte kullanılabilmektedir.



Şekil 1.1. Ekonomik Literatürde Paranın Fonksiyonları

Kaynak: Yazar tarafından hazırlanmıştır

Para, ticarette standart bir ölçü ve ortak birim görevi görmektedir. Fiyat teklifi ve pazarlık için bir temel oluşturmaktadır. Para, etkin çalışan muhasebe sistemlerinin gerçekleştirilebilmesi ve geliştirilmesi için gereklidir. Paranın işlevleri kullanım amacına göre değişiklik gösterebilmektedir.

Para biriminin hukuki kavramı, düzenleyicinin gücü ile ilişkilidir. Banknot ve madeni paraların merkezi olarak ihracı için yasal bir çerçeve oluşturabilmesi, paranın hukuki çerçevesi, devletin finansal piyasaları düzenleme gücüne dayanmaktadır (IMF, 2016: 16).

1.1. Finansal Teknolojiler ve Uluslararası Para Sisteminin Gelişimi

Finansal teknolojiler, günümüzde sıklıkla finansal hizmetler ve bilgi teknolojilerinin birleşimi olarak görülmektedir ve bu birleşim uzun bir geçmişe sahiptir. 19. yüzyıl sonlarında finans ve teknoloji birleşerek, finansal küreselleşmenin ilk adımını oluşturmuştur. Paranın, kripto paraya doğru olan yolculuğunu daha anlaşılır bir hale getirebilmek amacıyla, *Finansal teknolojiler 1.0 (1838-1966)*, *Finansal teknolojiler 2.0 (1967-2008*), Finansal teknolojiler 3.0 (2008'den bugüne) olmak üzere finansal teknoloji

alanında ki bazı önemli gelişmeler üç ana baslık altında toplanmıştır (Arner, 2016, Zimmerman, 2016, Kuzu, 2003: 52). Aşağıda, finansal teknolojiler alanında yaşanan önemli gelişmelerin hangileri olduğu konusunda kısa açıklamalarda bulunulmuştur.

Finansal Teknolojiler 1.0 (1838-1966 Arası Dönem)

- 1838: Telgrafın piyasaya sürülmesi.
- 1866: Transatlantik kablo ağı, finansal küreselleşme için altyapı sağlayan ilk başarılı transatlantik kablo ağının kurulması.
- 1918: Fedwire, Federal Reserve Bankaları tarafından fon transfer etmek ve tüm 12 rezerv bankası arasında iletişim ağı kurmak amacıyla, Mors kodu [4] sistemi kullanılarak telgraf ağının kurulması.
- 1950: Diner's Club, Frank X. McNamara tarafından kurulan Diner's Club ilk kredi kartı yapısı.
- 1960: Quotron Systems, masaüstü terminalleri vasıtasıyla brokerlere seçilmiş borsa önerilerini sunan ilk elektronik sistem.
- 1966: Telexs, Küresel teleks ağının kurulması, finansal teknolojilerin bir sonraki aşamasında gerekli iletişimi sağlanmıştır.

Finansal Teknolojiler 2.0 (1967-2008 Arası Dönem)

- 1967: Otomatik Vezne Makinesi, (ATM) Barclays bankası tarafından müşterilere günün her saatinde nakit temin etmesini sağlayan, bir "robot kasiyer" olarak adlandırılan ilk otomatik ATM'nin tanıtılması.
- 1969: Gelişmiş Araştırma Projeleri Dairesi Ağı (ARPANET).
- 1970: Bankalararası Kliring Odası Ödeme Sistemi (CHIPS), ilk elektronik ödeme sistemi.
- 1971: Ulusal Menkul Değer Tüccarları Otomatik Piyasa Fiyatlandırma Birliği (NASDAQ).
- 1973: Dünya Bankalararası Finansal İletişim Kuruluşu (SWIFT).
- 1978: Elektronik Fon Transferi Yasası (EFT Act).
- 1980: Telefon bankacılığı.
- 1981: Bloomberg finansal servisleri.

[4] Mors kodu; özel donanıma gerek duymadan doğrudan anlaşılabilen, sabit bir sinyalin açılıp kapatılması ile kısa ve uzun sinyaller oluşturularak bunlara karşılık gelen ışık veya sesleri kullanarak bilgi aktarılmasını sağlayan yöntemdir.

- 1982: İlk online brokerlik işlemi yapıldı. E-Ticaret kuruldu. Bireysel bir yatırımcı tarafından yürütülen ilk elektronik işlem gerçekleştirildi.
- 1983: Online bankacılık ve mobil telefonlar.
- 1984: İlk online alış veriş: Tesco'dan Jane Snowbal tarafından gerçekleştirmiştir.
- 1986: Big Bang[5] (Finansal Piyasalar) & Avrupa Tek Senedi[6] etkileri.
- 1987: Dünya Ekonomik Forumu (WEF).
- 1993: Finansal Teknolojiler (FinTech) terminolojisinin oluşumu.
- 2000: Dot-com Balonu[7] etkileri.

Finansal Teknolojiler 3.0 (2008 ve Sonrası Dönem)

- 2003: Web tabanlı kitlesel fonlama.
- 2008: Eşten eşe (Peer to Peer veya P2P) finansman.
- 2009: Bitcoin, Blok zinciri 1.0.
- 2013: Ethereum ve kripto halka arz süreci (ICO[8]), Blok zinciri 2.0.
- 2015: Akıllı telefon ve diğer aygıtların sunduğu olanaklar sayesinde tüketicilerin yüzlerini tarayarak elektronik ödemeleri doğrulamasına olanak sağlayan gelişmeler.
- 2017: Hyperledger Projesi, Blok zinciri 3.0 başlangıcı.

Yukarıda sayılan finansal gelişmeler çerçevesinde uluslararası para sistemi de zamanla değişime uğramış ve gelişmiştir. Modern zamanlarda, döviz sistemlerini organize eden ve düzenleyen çeşitli mekanizmaların, kurumların yanı sıra uluslararası para ve finansal borsaları tanımlanmaya başlamıştır. Uluslararası para sisteminin gelişimi ve ortaya

[5] Big Bang; finans piyasalarının ani düzenlenmesine ilişkin olarak kullanılan Big Bang deyimi, Margaret Thatcher tarafından 1986'da ortaya atılmıştır. Yabancı yatırımcılar için Londra finansal piyasası açılmış, sabit komisyonlar yerine rekabetçi yapıya geçilmiş ve elektronik sistemler kullanılması gibi birçok yenilik yapılmıştır. Big Bang, Londra'nın dünyadaki en önemli finansal merkezlerden biri haline gelmesini sağlamıştır.

[6] Avrupa Tek Senedi; Avrupa Birliği üye ülkeleri arasında iç pazar'ın oluşturulmasıyla ilgili en önemli belge, 1986 yılında imzalanan ve Temmuz 1987 tarihinde yürürlüğe giren Avrupa Tek Senedi'dir. Avrupa Birliği tek pazarını ve Avrupa Politik İş Birliğini resmen başlatan Roma Antlaşması'nda köklü değişiklikler yapan antlaşmadır.

[7] Dot-com balonu; Dot-com olarak adlandırılan internet bazlı firmaların, borsada gerçek değerinin çok üstünde işlem görmesi ve varlıkların aşırı değer kaybetmesi sonucu oluşan bir ekonomik balondur.

[8] ICO; (Initial Coin Offering) kripto para ile sermaye temini. Kripto para halka arzı, proje finansmanı ve girişim sermayesi temini gibi birçok konuda başvurulan, kripto para kullanımı aracılığıyla yapılan halka arz ve satış yönetimidir.

çıkan en önemli politik gelişmelerden bazıları ise şunlardır (Lin, Fardoust ve Rosenblatt, 2012: 3-7).

- **Altın Standardı Dönemi (1819-1914)**

Altın Standardı 1819 yılında Britanya tarafından oluşturulmuştur. Sonraki yıllarda Kıta Avrupası'ndaki diğer ülkelerin yanı sıra Japonya ve ABD altın standardını para birimlerinin temeli olarak kabul etmiştir. 1880'lerin sonuna gelindiğinde ise birçok ülke, altın standardını farklı şekillerde baz almaktaydı. Merkez bankalarının, altın standardı döneminde öncelikli sorumluluğu, para birimi ve altın arasındaki resmi pariteyi korumak olmuştur. Bu fiyatlamayı sağlayabilmek için merkez bankalarının yeterli miktarda altın bulundurması gerekmekteydi. Bu süre zarfında ödemeler dengesindeki fazlalık veya açık merkez bankaları arasında altın sevkiyatlarıyla finanse edilmek zorundaydı. Birçok açıdan dünya tarihinin önemli bir döneminde, klasik altın standardı kullanılmıştır. Döviz kurları ve fiyatlar genellikle istikrarlıydı ve siyasi sınırlar arasında serbest bir emek ve sermaye akışı gerçekleştirilirdi.

- **Savaşlar Arası Dönem (1914-1939)**

Birinci Dünya Savaşı sırasında (1914-1918) altın standardı çökmüş ve 1925'ten 1931'e altın değişim standardı olarak kısaca geri getirilmiştir. Bu sisteme göre ABD ve İngiltere altın rezervleri elinde tutabilirken, ancak diğer uluslar daha önce sistemi sarsan altın sıkıntısı sorunundan kaçınmak amacıyla rezerv olarak hem altın hem de dolar ya da sterlin tutabilmekteydiler.1929'daki Büyük Buhranın[9] başlangıcının hemen ardından tüm dünyada toplu banka iflasları gerçekleşmiştir.

- **Bretton Woods Sistemi (1946-1973)**

İkinci Dünya Savaşı'nın sonlarına yaklaşıldığı 1944 yılında, müttefik ülkelerin temsilcileri New Hampshire'da ki Bretton Woods'da bir araya gelerek savaş sonrası yeni bir para sistemi oluşturmak için anlaşmaya varmışlardır. Yeni sistem, Uluslararası Para Fonu (IMF) ve Dünya Bankası'nın (World Bank) kurulmasına yol açmıştır. 1969 yılında Özel Çekme Hakkı (SDR, Special Drawing Right) çıkarılmıştır ve hala günümüzde kullanılmaktadır. SDR; üye ülkelerin resmi rezervlerini tamamlayıcısı olarak IMF tarafından oluşturulmuş uluslararası rezerv varlıklarıdır. Mart 2016 itibarıyla 204,1

[9] Büyük Buhran; birçok ülkede 1929 yılından itibaren başlayan küresel ekonomik bunalım. Krizin etkisiyle, sanayi üretimi, dünya ticareti ve uluslararası sermaye akımları büyük bir düşüş yaşanmış, bankacılık krizleri, sosyal sefalet ve birçok şirket iflası sonucu siyasi krizlere neden olan kitlesel işsizlik oluşmuştur.

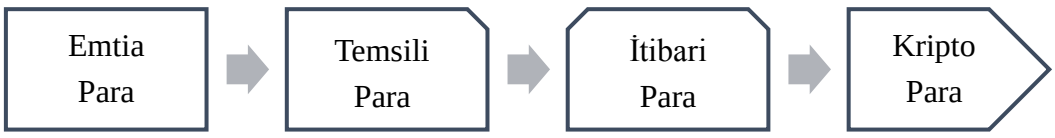
milyar SDR (yaklaşık 285 milyar dolara eşdeğer) ihraç edilmiş ve üyelere tahsis edilmiştir. SDR'ler serbestçe kullanılabilir para birimleri ile değiştirilebilmektedir. SDR'nin değeri, ABD Doları, Avro, Çin Renminbisi, Japon Yeni ve İngiliz Sterlini olmak üzere beş anapara biriminden oluşan bir sepete dayanmaktadır (imf.org, 2017).

- **Bretton Woods Sistemi Sonrası Dönem**

Bretton Woods sistemi giderek savunulamaz hale gelmiş ve ABD'deki makroekonomik politikaların aşırı genişlemesinin etkisiyle sistem çökmüştür. Şubat 1973'te Bretton Woods döviz piyasaları kapanmış ve Mart 1976'ya kadar tüm önemli para birimlerinde dalgalanmalar yaşanmıştır. Bretton Woods sisteminin çöküşünden bu yana döviz kurlarını altına bağlamak haricinde, IMF üyeleri diledikleri her türlü değişim düzenlemesini seçebilmektedirler.

1.2. Para Tanımları ve Türleri

Genellikle para teorisi, ekonomik terimler ile değil hukuksal terimler ile ifade edilmektedir. Bu terminoloji yazarlar, devlet adamları, tüccarlar, hakimler ve başlıca amaçları farklı para ve ikamelerinin yasal özelliklerine ilgi duyan diğer kişiler tarafından oluşturulmuştur. Hukuki bakış, para sisteminin yasal açıdan önem taşıyan yönleriyle ilgilenmek için yararlıdır. Ancak pratik olarak ekonomik araştırmalar için pratik olarak pek yararlı değildir. Ekonomik argümanlarda hukuki terimlerin kullanılması kaçınılmazdır. Ancak ekonomi kendi özel amaçları için kendi özel terminolojisini oluşturmalıdır (Mises, 1912: 34). Şekil 1.2'de paranın zaman içindeki değişimi gösterilerek, ardından farklı para tanımları yapılmaya çalışılmıştır.



Şekil 1.2. Paranın Zaman İçindeki Değişimi

Kaynak: ecb.europa.eu (2015)

Para zaman içinde çeşitli evrelerden geçmiştir. İlk para genelde emtia parası olarak bilinmektedir. Emtia para; ticari bir emtia olan para çeşidi (Mises, 1912: 61) olup

değerini imal edildiği, basıldığı emtiadan almaktadır (Çarkacıoğlu, 2016: 1).

Daha sonra gelişen temsili para, belli miktarda altın veya gümüş karşılığında takas edilebilen banknotlardan oluşur. Temsili para altın, gümüş veya değerli bir mal karşılığında kâğıda basılan, malın gerçek değerini temsil eden ve istenildiği anda karşılığı olan mala çevrilebilen para olarak tanımlanabilir.

Günümüzde modern ekonomik sistemler tamamen itibari para üzerine kurulmuştur. *İtibari para*, özel bir yasal niteliği olan para (Mises, 1912: 61) olup ödeme aracı olarak değerini yasalardan alan, piyasada temsil ettiği satın alma gücünün üretim maliyetinden (kağıt veya maden değeri) karşılaştırılamayacak kadar büyük (çıkarım kazancı[10]) olduğu paradır (TDK, 2014). İtibari para, hukuki kurallar çerçevesinde merkez bankaları tarafından çıkarılmaktadır. Banknotlar için kullanılan kağıt prensipte değersizdir. Ancak mallar ve hizmetler karşılığında kabul edilmektedir. Çünkü insanlar para değerini sabit tutması için merkez bankalarına güvenmektedir. Merkez bankaları başarısız olursa, itibari para genel kabul edilebilirliğini, bir takas aracı ve değer muhafaza özelliklerini kaybedecektir. Günümüzde paraların büyük bir kısmı dijital olarak saklanması kripto para kavramının gündeme gelmesini teşvik etmektedir.

Elektronik para (e-para), ise elektronik para ihraç eden kuruluş tarafından kabul edilen fon karşılığı ihraç edilen, elektronik olarak saklanan, bu kanunda tanımlanan ödeme işlemlerini gerçekleştirmek için kullanılan ve elektronik para ihraç eden kuruluş dışındaki gerçek ve tüzel kişiler tarafından da ödeme aracı olarak kabul edilen parasal değer olarak tanımlanmıştır (Resmi Gazete, 2013: 28690).

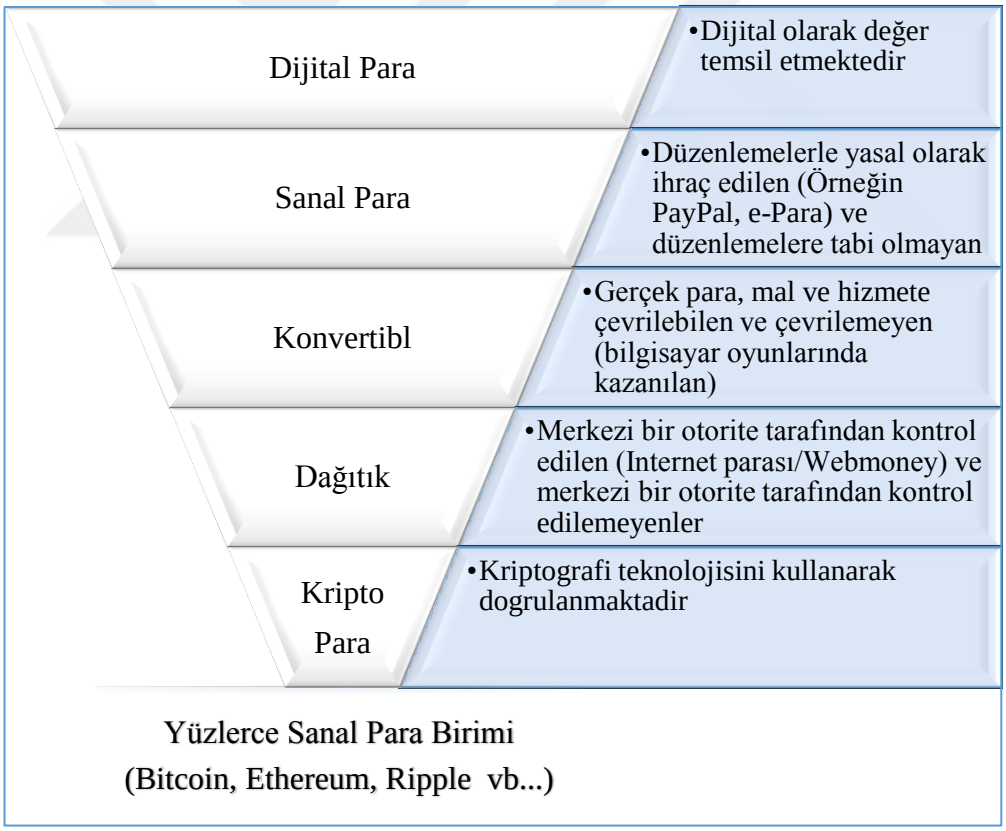
Elektronik paralar, nakit için elektronik bir alternatiftir. Elektronik olarak depolanan ve ödeme işlemleri yapmak için kullanılan bir parasal değerdir. E-Para, kartlarda, cihazlarda veya bir sunucuda tutulabilir. Örnekler arasında, ön ödemeli kartlar, elektronik cüzdanlar veya PayPal gibi web tabanlı hizmetler bulunmaktadır. Bu nedenle, e-para, daha çok belirli elektronik değerli ürün ve hizmetler için çatı terimi oluşturabilmektedir (Fripo, 2009). Avrupa Parlamentosu ve Konseyi Elektronik Para Yönergesine göre, elektronik para, ihraççının, iddiasıyla temsil edilen parasal değerdir,

[10] Çıkarım kazancı; (Senyoraj) Paranın piyasadaki parasal değeri ile basılma maliyeti arasındaki fark dolayısıyla ortaya çıkan kazanç.

elektronik olarak depolanır, ihraç edilen parasal değere kıyasla daha az olmayan bir tutarın fon olarak alınmasından sonra düzenlenir ve ihraççısı dışındaki ekonomik birimler tarafından bir ödeme aracı olarak kabul edilir (European Comission vd. 2009: 110).

1.3. Sanal Para Birimi Yapıları

Literatürde kripto para, sanal para ve dijital para terimlerinin birbirleri yerine kullanıldığı görülmektedir. Sanal para birimi yapılarını tanıtmaya geçmeden önce kısaca sanal para birimi yapılarını sınıflandırmak konuyu daha iyi anlamamıza yardımcı olacaktır. Bu amaçla, ilk sınıflandırma IMF tarafından yapılmış olup aşağıdaki Şekil 1.3'te gösterilmiştir.



Şekil 1.3. IMF'ye Göre Sanal Para Birimlerinin Sınıflandırılması

Kaynak: IMF (2016: 8)

Sanal para yapıları, mallara, hizmetlere, ulusal para birimlerine, veya diğer sanal para yapılarına dönüştürülebilmesi, farklı konvertibilite seviyeleri göz önünde

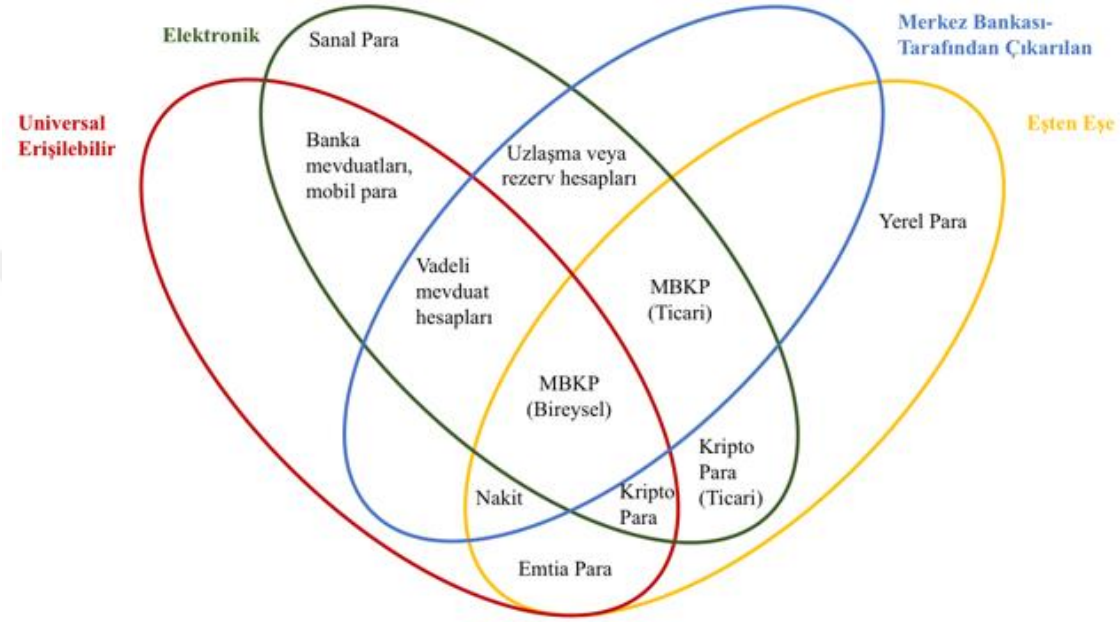
bulundurularak yapılmış bir sınıflandırmadır. Dönüştürülebilir olmayan sanal para yapıları (kapalı yapılar) yalnızca bağımsız bir sanal ortamda çalışmaktadır. Bu tür sistemlerde, itibari para birimi (veya diğer sanal para yapıları) ile değişimi veya sanal alan dışındaki malların ve hizmetlerin ödemelerinde kullanılması önemli ölçüde kısıtlanmıştır. Buna karşılık, takas edilebilir sanal para yapıları (açık yapılar), itibari para birimi (veya diğer sanal para yapıları) ile değiş tokuşuna ve reel ekonomide mal ve hizmetlere yapılan ödemelerde kullanılmasına izin vermektedir.

Geçmişte finansal sektördeki en önemli yenilikleri bankalar başlatmıştır. 1950'lerde kredi kartının başlangıcı ve 1970'lerde Otomatik Vezne Makinesi (ATM, Automated Teller Machine), mallara erişim ve ödeme şeklimizi tamamen değiştirmiştir. Günümüzde bu değişimin hem hızı hem de yönü çok farklı boyutlarda gelişmektedir. İnternet, akıllı telefonlar, nesnelerin interneti[11], büyük veri analizi, sosyal medya ve bulut bilişim vb. gelişen teknolojik kavramlar, her alanda olduğu gibi finans alanında da etkisini göstermekte, önemli gelişmeler ve kolaylıklar sağlamaktadır. Tüketiciler finansal varlıklarını ve araçlarını farklı teknolojiler üzerinden kullanma olanakları talep etmektedirler. Bu nedenle, finansal yenilikler artık bir kaç sektör ile sınırlı değildir. Sektör dışından katılımcılar da finans sektörüne dahil olmaktadır. Finans sektörü, temassız teknoloji, dijital cüzdanlar ve kripto para birimleri gibi birçok etkileyici yeniliğe ve teknolojik ilerlemelere şahit olmaktadır (Barberis vd. 2016, 20). Kayıt altına alarak bir miktar parayı birine vermek, bu işlemi doğrulamak için üçüncü bir tarafa başvurmaksızın anında o değeri kabul edene aktarmaktır. Ancak bu tür eşler arası transferler yalnızca yakın mesafelerde ve belirli durumlarda mümkün olmaktadır. Parayı başka bir şehirdeki veya ülkedeki bir kişiye aktarmak için, başkalarına belirli bir dereceye kadar kontrol izini vermek ve güvenmek gerekir. Posta çalışanının nakit içeren bir zarfı göndermesi veya bankalarda olduğu gibi merkez bankasının onayını gerektiren EFT (Elektronik Fon Transferi) bu duruma örnek verilebilir. Banka, gerçekten de paranın yasadışı faaliyetlerle bağlantılı olduğu kanaatine vardığında, elektronik işlemleri engelleyebilir veya elektronik fonlara el koyabilir. Dünyada finansal ödeme sistemleri, bankalar arasındaki iş ilişkileri, SWIFT[12] gibi elektronik iletişim ağları,

[11] Nesnelerin İnterneti; (IoT, Internet of Things) nesnelerin diğer nesnelerle etkileşim kurabildiği bir gelişim sürecini temsil etmektedir.
[12] SWIFT; 200'den fazla ülkede ve bölgede, 11.000'den fazla bankacılık ve menkul kıymet organizasyonu tarafından kullanılan mesajlaşma platformu servis sağlayıcısıdır.

fiziksel nakidin gerçekten diğer her para biçiminden farklı olduğu gerçeğinin doğrudan bir sonucudur (GOS, 2015: 33).

Diğer bir sınıflandırma ise Uluslararası Ödemeler Bankası tarafından yapılmış olup Şekil 1.4'de gösterilmiştir.



Şekil 1.4. Uluslararası Ödemeler Bankasına Göre Kripto Paralar

Kaynak: Bech ve Garratt (2017: 60)

Bu yeni para birimlerinin ne olduğu konusunda karışıklıklar ve tartışmalar devam ederken, aslında önerilen şey hakkında tam bir fikir birliğine varılamadığı anlaşılmaktadır. Merkez bankası tarafından çıkarılmayan, evrensel olarak erişilebilir olan para şekilleri arasında (özel olarak oluşturulmuş) kripto para, emtia para, ticari bankalar tarafından kullanılan kaydi para ve mobil para gibi paralar bulunmaktadır. Kripto paranın ise diğerlerine nazaran eşten eşe, elektronik ve evrensel olarak erişilebilir olduğu görülmektedir. Başka para biçimleri, eşten eşe ve evrensel olarak erişilememektedir. Merkez bankası tarafından çıkarılacak kripto paraların nasıl konumlandırılabileceği gösterilmiştir. Şimdilik ne bireysel ne de ticari kullanıma sunulmuş merkez bankası tarafından çıkarılan kripto paraları MBKP (Merkez Bankası Kripto Paraları) bulunmamaktadır (Bech ve Garratt, 2017: 58-67). Blok zinciri ve dağıtık kayıt teknolojisi birçok merkez bankasının dikkatini çekmiş durumdadır. Muhtemelen gelecekte şekildeki diğer alanlar farklı paralar ile dolacaktır.

Geleneksel ödeme sistemlerine nazaran güvenli, hızlı, ulaşılabilir olması gibi beklenen kriterlerden bazıları sanal para birimleri ile karşılansa da aralarında önemli farklar vardır. Elektronik para şemalarında, elektronik para ve geleneksel para biçimi arasındaki format korunmaktadır ve yasal temeli vardır. Çünkü depolanan fonlar aynı hesap birimi (ABD Doları, Avro vb.) ile ifade edilmektedir. Sanal para yapılarında hesap birimi, sanal bir para birimi cinsinden işlem görmekte ve değiştirilmektedir (Bitcoin vb. gibi). Elektronik para yapılarında ödeme aracılığı sağlayan para kurumları ihtiyati gözetime tabi iken sanal para birimi yapıları için durum böyle değildir (ECB, 2012: 16). Elektronik paraları, diğer fiziksel olmayan para birimlerinden ayıran en önemli faktör ise hükümetler tarafından düzenlenmemesidir.

Sanal para, bir merkez bankası ya da kamu otoritesi tarafından arz edilmeyen, ya da mutlaka bir emtia para birimine bağlı olmayan dijital bir değer gösterimi olarak tanımlanır. Sanal para birimleri doğal veya tüzel kişiler tarafından bir değişim aracı olarak kullanılmakta olup elektronik olarak aktarılabilir, depolanabilir veya ticareti yapılabilmektedir (EBA, 2014: 5). Ayrıca, sanal para birimi, değerin dijital bir gösterimi olarak ifade edilmektedir. Bir merkez bankası, kredi kuruluşu veya e-para kurumu tarafından ihraç edilmeyen bir para alternatifi olarak kullanılabilmektedir (ECB, 2015: 25). Sanal parayı daha iyi anlayabilmek için dijital para kavramını da bilmek gerekir.

Dijital para, adından anlaşılacağı üzere; para birimlerinin elektronik olarak saklanıp, aktarılabilmesini sağlayan yapıdır. Bir ve sıfırlardan oluşan bit[13] dizileri ile dijital ortamda saklanan herhangi bir para birimi bu tanıma uygundur. Bir banka hesabında saklanan doların aslında bir yerde tutulmuş olan dolarların göstergesi olması, karşılığını bulması gerekmektedir. Dijital para birimleri ve dağıtık kayıt teknolojisi, birçok alanda, özellikle ödeme sistemleri ve hizmetleri üzerinde bir dizi etkiye sahip olabilecek bir yeniliktir. Bu etkilere mevcut iş modellerinin ve sistemlerin değişmesinin yanı sıra yeni mali, ekonomik, sosyal etkileşimlerin ve bağlantıların ortaya çıkması mümkündür. Mevcut dijital para birimi yapıları devam etmese dahi, aynı temel prosedürlere ve dağıtık kayıt teknolojisine dayalı farklı yapıların ortaya çıkması ve gelişmesi muhtemeldir. Dijital para birimlerinin varlık yönü, diğer bağlamlarda yürütülen önceki çalışmalarla benzerlik taşımaktadır. Örneğin, Merkez Bankası ve ticari banka parasıyla

[13] Bit, bir veri ölçü birimidir. Bilgisayarda kullanılan en küçük ölçü birimidir. Bit sadece iki değer alabilir; 1 ya da 0.

rekabet edebilecek e-paranın geliştirilmesi için 1990'ların sonlarından itibaren analitik çalışmalar yapılmış, birçoğunda ödeme sistemleri ile ilgili daha fazla araştırma ihtiyacı vurgulanmıştır. Bununla birlikte, geleneksel e-paradan farklı olarak, dijital para birimleri, bir kişinin veya kurumun sorumluluğunda değildir ve bir yasal yetkili tarafından desteklenmemektedir. Sonuç olarak, dijital para daha sonraki bir zamanda mal ve hizmetler için ya da belirli bir miktarda itibari para birimi karşılığında alınıp alınmayacağına olan güven ile değer elde etmektedir (BIS, 2015:17).

Dijital para birimi, yalnızca elektronik olarak var olan bir ödeme aracıdır. Geleneksel para gibi (banknot gibi), fiziki mal ve hizmet satın almak için kullanılabilmektedir (Bank of England, 2017). Dağıtık sistemlerin kullanılmasına dayanan dijital para birimleri, ödemeler alanındaki bir gelişmeyi temsil etmektedir. Bununla birlikte, sanal para birimlerinin gelişimine neden olan pek çok faktör, daha geleneksel ödeme yöntemlerinde de yeniliği teşvik etmektedir. Bankaların bankası olarak bilinen, Uluslararası Ödemeler Bankası[14] (BIS, Bank for International Settlements), dijital para birimleri ve dağıtık kayıt teknolojisini, e-ticaret ve uluslararası işlemler alanında, maliyetlerin azaltılması ve hızın artması ile hem dijital para birimi gelişimini, hem de daha geniş ödeme sistemi yeniliklerini destekleyen faktörlerden olarak kabul etmektedir (BIS, 2015: 3). Özellikle, dijital para birimlerinin ve diğer yeniliklerin geliştirilebilmesinde teknolojinin önemine işaret etmektedir.

Kripto para birimi ise kriptolama teknikleriyle para birimlerinin oluşturulmasını düzenleyen ve (merkez bankasından bağımsız olarak işlem gören) fonların transferini doğrulayan bir dijital para birimidir (oxforddictionaries.com, 2017).

Hükümetler tarafından çıkarılan fiziki olmayan paralar, basilmiş paralara göre daha kompleks bir yapıya sahiptir. Kripto para birimlerinin ise yasal bir çıkarıcısı bulunmamaktadır. Kripto para birimlerinin boyutu, tıpkı internetin boyutuna oldukça benzemektedir. Bu sebeple merkez bankaları, hükümetler ya da herhangi bir yasal

[14] Uluslararası Mutabakat Bankası olarak da bilinmektedir. Parasal ve finansal istikrarı sağlamaya yönelik olarak merkez bankaları ve diğer kurumların kendi aralarındaki iş birliğini artırmak amacı ile kurulmuş, uluslararası bir organizasyondur. 1930 yılında kurulmuş olup İsviçre'nin Basel kentinde yerleşiktir. Sermayesi altın frank şeklinde ifade edilmekte olup 1 altın frank 0,29 gram altını temsil etmektedir. TCMB 5.000 altın frank ile bankanın hissedarıdır.

dayanağı olmayan kripto para birimlerinin farklı kuruluşlarca farklı tanımlarla ele alındığı bilinmektedir.

1.4. Elektronik Ödemelerde Kriptografi ve Kripto Para

Ödeme, bir mal veya hizmet veya bir yasal yükümlülüğün yerine getirilmesi karşılığında, bir şahsın veya kuruluşun değeri karşı tarafa devretme sürecini ifade etmektedir. Uluslararası ödemeler ise ödemelerin coğrafi sınırlar boyunca birden fazla itibari para birimi üzerinden yapılabilmesidir (WEF, 2016: 47). Kripto para yapıları, geleneksel elektronik ödeme hizmet sağlayıcılarından tamamen farklıdır. Ödemelerde bir sorun yaşanması durumunda kullanıcılar denetlenen bir kuruluş olan ödeme hizmeti sağlayıcısına başvurabilir. Örneğin, Avrupa Birliğinde 100.000 €'ya kadar olan mevduatlar Avrupa Birliği kuralları uyarınca garanti altına alınabilmektedir. Kripto para kullanıcıları genelde doğrudan kendi sorumluluğu ile diğer kullanıcılarla etkileşime girmektedir (ECB, 2017:1). Diğer bir deyişle kripto para ile yapılan işlemler geri döndürülemez olup hatalı işlemlerde sorumluluk yalnızca kullanıcıya aittir.

2008 yılında Lehman Brothers'ın iflasını açıklaması, ABD'deki büyük yatırım bankalarının banka holding şirketlerine dönüştürülmesi, bazı kuruluşların ulusallaştırılması, parçalanması ve satılmasına neden olmuştur. İzlanda'nın en büyük ticari bankasının ardından ülkenin bankacılık sisteminin çökmesi, birçok ülkenin bankalarına ciddi destekler vermesine yol açması gibi bir kısım olaylar henüz kriz durumları için yeterince önlemin alınmadığını ve mevcut sistemin ciddi eksiklikler içerdiğini göstermiştir. Bu bağlamda sarsılan güven, eşler arasında kullanılabilecek paranın gelişimini bir nevi teşvik etmiştir. Krizin ortaya çıkardığı eksiklikleri gidermek amacıyla Basel III düzenlemesi geliştirilmiştir. Basel Komitesi, sistemik olarak önemli bankaların risklerinin tanımlanması hususunda Finansal İstikrar Kurulu (FSB, Financial Stability Board) ile çalışmalarını yürütmektedir. Bu konuda yapılan çalışmalar neticesinde 12 Eylül 2010 tarihinde Merkez Bankaları ve Denetim Otoriteleri Başkanları, sistemik önemi haiz finansal kuruluşların Basel III standartları çerçevesinin ötesinde kayıpları karşılayacak kapasiteye sahip olmaları konusunda fikir birliğine varmışlardır (Cangürel vd. 2010: 4-5). Bu bağlamda uluslararası işbirliğiyle, TCMB ve BDDK, gereklilik ve yükümlülüklerinin yerine getirilmesi şartıyla ödeme kurumunun faaliyetine izin vermektedirler. TCMB, ödeme ve menkul kıymet mutabakat

sistemlerinin yasal altyapısının güçlendirilmesi, dağınık halde bulunan mevzuatın toplu, bütüncül ve küresel ölçekte en iyi uygulama örneklerini esas alan bir mahiyette düzenlenmesi, sistemlere ilişkin ortak kural ve standartların belirlenmesi, ödeme ve elektronik para kuruluşlarına ilişkin mevzuat çerçevesinin oluşturulması ile ödemeler alanında faaliyet gösteren kuruluşlar ve bu kuruluşların sundukları hizmetlerden yararlananlarla ilgili olarak tüketicinin korunması amaçlarıyla bu alanda yeni bir kanunun hazırlanmasında öncü bir rol üstlenmiştir. TCMB tarafından, Avrupa Birliği düzenlemeleri ile uluslararası standartlarla ve uygulamalarla uyumlu bir mevzuat çerçevesi oluşturma çalışmaları sonucunda ilgili paydaşların görüşleri de dikkate alınarak ilk taslağı hazırlanan *"Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun"* 27 Haziran 2013 tarih ve 28690 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir (TCMB, 2014: 21).

TCMB, EFT sisteminin işleticisi ve sahibi olup ödemelere kesinlikle müdahale etmemekte, ödemeleri bekletmemekte veya ödemelere onay vermemektedir (TCMB, 2014: 21). 6493 sayılı "Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun"a göre ödeme sistemi veya menkul kıymet mutabakat sistemi, üç veya daha fazla katılımcı arasındaki transfer emirlerinden kaynaklanan fon ya da menkul kıymet aktarımlarının gerçekleştirilmesini sağlamak amacıyla yapılan takas ve mutabakat işlemleri için gerekli altyapıyı sunan ve ortak kuralları olan yapı olarak tanımlanmaktadır. Ödeme sistemleriyle ilgili başlıca kavramlar arasında *takas* ve *mutabakat* kavramları bulunmaktadır. Elektronik para kuruluşu, 6493 sayılı kanun kapsamında elektronik para ihraç etme yetkisi verilen tüzel kişidir (Resmi Gazete, 2013: 28690).

6493 sayılı Kanuna göre;

- Takas, sisteme gönderilen transfer emirlerinin aktarımı, bu emirlerin karşılıklı olarak iletilmesine ve mutabakat öncesi provizyon [15] alındığı durumlarda provizyon alınmasına aracılık edilmesi ve bazı durumlarda bu emirlerin netleştirilmesi işlemlerini ifade etmektedir.

[15] Provizyon, bir bankada hesabı bulunan kimsenin, o bankanın başka bir şubesinden para çekmek istediğinde, çekilmek istenen bu para miktarının, karşılığının bulunup bulunmadığının, ilgili şubeye sorulması ve teyit alınması durumudur.

- Mutabakat, iki ya da daha fazla taraf arasındaki fon ya da menkul kıymet aktarımından kaynaklanan yükümlülüklerin yerine getirilmesini ifade etmektedir (tcmb.gov.tr, 2017).

Ödeme ve Menkul Kıymet Mutabakat Sistemlerine İlişkin Gözetim Çerçevesine göre, Türkiye'de fiili olarak kullanılan ödeme ve menkul kıymet mutabakat sistemleri Tablo 1.1'de gösterilmektedir.

Tablo 1.1. Türkiye'de Kullanılan Ödeme ve Menkul Kıymet Mutabakat Sistemleri

SİSTEMİN ADI	SİSTEMİN TÜRÜ	SİSTEM İŞLETİCİSİ	SİSTEMİN SINIFI
Elektronik Menkul Kıymet Transfer Sistemi	Menkul kıymet mutabakat sistemi	TCMB	Kritik Önemdeki Sistem
Pay Piyasası Takas Sistemi	Menkul kıymet mutabakat sistemi	TAKASBANK	Kritik Önemdeki Sistem
Borçlanma Araçları Piyasası Takas Sistemi	Menkul kıymet mutabakat sistemi	TAKASBANK	Kritik Önemdeki Sistem
Merkezi Kaydi Sistem	Menkul kıymet mutabakat sistemi	MKK	Kritik Önemdeki Sistem
Bankalararası TL Aktarım Sistemi	Ödeme sistemi	TCMB	Kritik Önemdeki Sistem
Müşterilerarası TL Aktarım Sistemi	Ödeme sistemi	TCMB	Kritik Önemdeki Sistem
Çek Takas Sistemi	Ödeme sistemi	BTOM	Önemli Sistem
Yurtiçi Takas ve Hesaplaşma Sistemi	Ödeme sistemi	BKM	Önemli Sistem
Takasnet Sistemi	Ödeme sistemi	GÖSAŞ	Sınırlı Önemli Sistem
MPTS Takas Sistemi	Ödeme sistemi	MPTS	Sınırlı Önemli Sistem

Kaynak: tcmb.gov.tr (2017)

Tablo 1.1'den anlaşılacağı üzere, Türkiye'de kullanılan ödeme ve menkul kıymet mutabakat sistemleri farklı önem derecelerine sahip olup farklı sistem işleticileri tarafından yürütülmektedir.

Kripto para birimlerinde ödemeler blok zinciri sistemi ile kayıt altına alınmaktadır. Kriptografik bir ekonomik sistem, bilgisayar protokolünde belirtilen temel kurallara uyarak, herhangi bir insan etkileşimi olmaksızın işlemleri tamamen güvenilir bir şekilde organize eden bir sistem olarak tanımlanabilmektedir. Sistem, A'dan B'ye gidecek olan yolcuları güvenli bir şekilde götüren otomatik olarak seyreden mürettebatsız bir tekne veya insansız bir araç ile kıyaslanabilir. Herhangi bir kötü niyetli ve kazara olabilecek

durumu en aza indirgeyen bir şifreleme protokolü tarafından tamamen kontrol edilmektedir. Blok zinciri aslında adından da anlaşıldığı üzere bloklardan oluşan bir zincirdir. Bir blok, belirli bir süre içindeki tüm işlemlerin, verilerini ve kendinden sonraki bloğa referansı içermektedir. Hashing (işlem özet fonksiyonu) algoritmaları[16], tüm blokların iyi oluşturulmuş ve değiştirilmemiş olduğundan emin olmak için kullanılır ve böylece blok zinciri kendisini güvende tutar ve neredeyse kırılmaz olmaktadır. Blok zinciri işlemleri tek bir sunucudan sağlanmamaktadır, yaygın bir bilgisayar ağı üzerinde dağıtılmış bir işlem kaydı olarak çalışmaktadır. Tüm ağ katılımcıları, tüm verileri blok zincirinde tutar ve bunu geliştirmek için birlikte çalışabilmektedirler. Bu işlemleri gerçekleştirenlere genellikle madenciler denilmektedir. Blok zinciri protokolüne bağlı olarak, madenciler ortak kararla, blok zincirine eklenen yeni blokları oluşturmak için, işlemden kazanç sağlamak amacıyla çaba göstermektedirler (Czepluch vd. 2016: 4). Verileri bilişim sistemlerinde çevrimiçi olarak korumanın en popüler yolu şifreleme (kriptografi) yöntemidir.

Verilerin şifrelenmesi, bilginin yalnızca onu çözmek için kullanılan bir anahtar tarafından okunabilmesi için kodlandığı anlamına gelmektedir. Kriptografi, istenmeyen kişilere karşı bilginin gizlenmesi metodudur. Bilgilerin sadece istenen kişilere ulaştırılması ve istenmeyen kişilerden gizlenmesini sağlamak için şifreleme algoritmaları kullanılmaktadır. ATM teknolojisinin güvenliğini, bilgisayar parolalarını ve elektronik ticareti içeren parasal işlemlerin güvenliğini sağlamak için, şifreleme teknikleri uzun zamandan beri bankacılık endüstrilerinde kullanılmaktadır. Herhangi bir özel önlem olmadan okunabilen ve anlaşılabilen verilere düz metin veya açık metin denilmektedir. Modern zamanlara kadar kriptografi neredeyse şifrelemeyi sadece düz metini, özünü gizleyecek şekilde anlaşılmaz bir metin haline dönüştürme süreci olarak bilinmekteydi. Şifre çözme ise bu işlemin tersi olup anlaşılmayan şifreli metninden düz metin oluşturmaktır. Kriptografi, şifreleme ile birlikte ters şifrelemeyi oluşturan bir çift algoritmadır. Bir şifrenin ayrıntılı çalışması esasen, her iki durumda da algoritmanın istenilen zamanlarda kontrol edilebilir olmasıdır. Kriptolojide, bankalar gibi finansal kurumların kullandıkları bazı popüler yöntemler, açık anahtarlı kriptografi (asimetrik), simetrik anahtarlı kriptografi ve veri şifreleme standardı kartografisidir. Kriptografi, çeşitli tekniklerle aşağıdaki hedefleri sağlamaya çalışmaktadır (Kar ve Dey, 2010: 2,

[16] Algoritma; bir amaca ulaşmak için gerekli belirli eylem kurallarıdır.

Network Associates, 1999: 11);

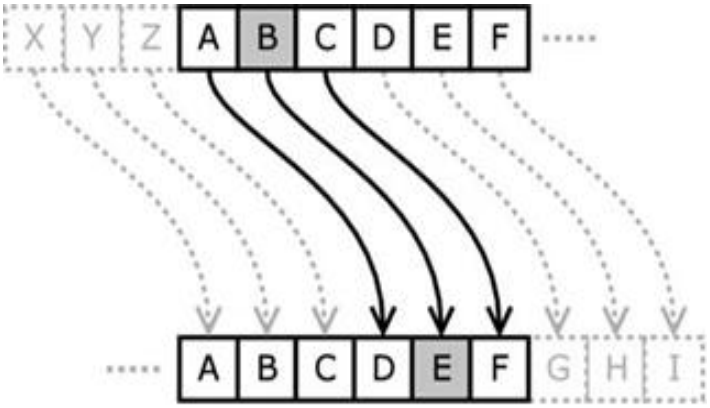
- *Kimlik doğrulama:* Kişinin kimliğinin ispatlaması sürecidir.
- *Gizlilik / Güvenilirlik:* İstenen alıcı dışında kimsenin mesajı okuyamadığından emin olunmasıdır.
- *Bütünlük:* Alıcıya ulaştırılan mesajın, orijinalinden herhangi bir değişikliğe uğramadığından emin olunmasıdır.
- *Reddedilemezlik:* Gönderenin gerçekten bu mesajı gönderdiğini kanıtlayan bir mekanizmadır.

Kriptografi, şifreleme ve şifre çözme için matematik kullanılan bir bilim dalıdır. Böylece hassas bilgiler güvenli olmayan şebekeler (internet gibi) üzerinden iletilir ve istenen alıcı dışındaki herhangi biri tarafından okunamaz. Şifreli verilerin güvenliği tamamen iki faktöre bağlıdır: Bunlar,

- Şifreleme algoritmasının gücü,
- Anahtarın gizliliğidir.

Şifreleme gücü, mevcut bilgi işlem altyapısı ile şifreyi çözerek düz metinlere erişebilmek için gereken zaman ve kaynaklarla ölçülmektedir. Şifreleme anahtarı gizliliği sağlanamazsa en güçlü algoritma dahi olsa güvenlik sağlanamaz.

Sezar şifrelemesi olarak bilinen kriptolama yöntemi, Roma döneminden basit bir şifreleme yöntemidir. Sezar şifrelemesi, şifrelemenin en basit biçimlerinden biridir.



Şekil 1.5. Sezar Şifrelemesi

Kaynak: thecenter.org (2016)

Şekil 1.4'te görüldüğü gibi, orijinal mesajdaki her harf, belirli bir aralıkta, alfabedeki harfe karşılık gelen bir harflerle yer değiştirmektedir. Bu şekilde, başlangıçta oldukça okunabilir olan bir mesaj, basit bir bakışta anlaşılamayan bir hal almaktadır. Sezar şifrelemesi, geleneksel şifrelemenin son derece basit bir örneğidir. Yukarıdaki örnekte anahtar değeri 3 olarak kodlanmıştır. Anahtar olarak alfabe 3 harf kaydırma yapılarak kullanılmaktadır. Aynı olay bilgisayar ortamında gerçekleşmektedir. Her kriptolama yazılımının gizli bir kodu mevcut olup bilgisayarlar arasında taşınan bir bilgi paketinin gizlenmesi amaçlanmaktadır.

Tüm para birimleri açısından hileleri önlemek, kaynağı kontrol etmek ve çeşitli güvenlik önlemleri uygulamak önemli bir gerekliliktir. İtibari para birimlerinde, merkez bankaları gibi kuruluşlar para arzını kontrol eder ve fiziksel para birimlerini sahteciliğe karşı korumak için gerekli önlemleri alır. Benzer şekilde kripto para birimlerinde de kişilerin sisteme müdahalesini önleyen ve farklı bozulmalara karşı güvenlik önlemleri almak gerekmektedir. Örneğin, A şahsının B şahsını kripto parayla yapmış olduğu bir ödeme konusunda ikna ederse, C şahsını da ikna edememesi gerekmektedir (çifte harcama[17] kuralı). Birçok para birimlerinin aksine, kripto para birimlerinin güvenlik kuralları tamamen teknolojik olarak ve genelde merkezi bir kuruluşa dayanmaksızın uygulanmaktadır. Kripto para birimleri, kriptolama işlemini yoğun olarak kullanmaktadır. Kriptografi, kripto para biriminin güvenli bir şekilde kodlaması için bir mekanizma sağlamaktadır. Ayrıca kripto para birimindeki yeni birimlerin

[17] Çifte harcama; (mükerrer harcama) aynı girdinin harcandığı birden çok onaylanmamış işlemelere denilmektedir.

oluşturulmasına ilişkin kuralları matematiksel bir protokole kodlamak için kullanabilmektedir. Kripto para birimlerinin doğru bir şekilde anlaşılabilmesi için şifreleme temellerini araştırmak gerekmektedir. Kriptografi, karmaşık olan birçok gelişmiş matematiksel tekniği kullanan derin bir akademik araştırma alanıdır. Bitcoin, yalnızca, nispeten basit ve iyi bilinen bir şifreleme yapısına dayanmaktadır. Burada bilinmesi gereken ilk şifreleme tekniği temel bir şifreleme olan *hash* işlevidir.

Bir hash, üç temel özelliğe sahip matematiksel yöntemdir. Bunlar;

- Katkıları herhangi bir boyutta herhangi bir dize olabilir.
- Sabit boyutta bir çıktı üretmektedir. Örneğin; 64, 128, 256 bit çıktı boyutu.
- Verimli olarak hesaplanabilmektedir. Sezgisel olarak, belirli bir girdi dizgesi için, hash çıktısının makul bir süre içerisinde ne olduğunu bulabileceğiniz anlamına gelir (Narayanan vd. 2015).

HSBC tarafından yayınlanan teknolojiye olan güven raporu, Ipsos MORI Küresel pazar ve görüş araştırma uzmanları tarafından, HSBC için "*Teknoloji Fobisi Yükselişi – Teknoloji Benimseme Eğitim Anahtarı*" başlıklı bir araştırma adı altında gerçekleştirilmiştir. Çalışma 11 ülkenin (Kanada, Çin, Fransa, Almanya, Hong Kong, Hindistan, Meksika, Singapur, Birleşik Arap Emirlikleri, İngiltere, ABD) ve bu bölgelerdeki toplam 12.019 kişinin görüşlerini temsil etmektedir. Söz konusu nitel araştırma 2017 Mart ve Nisan aylarında gerçekleştirilmiştir. Çalışma, ilgili 11 ülkeden altı üye içeren bir online topluluğun da dahil olduğu 66 üyesiyle yürütülmüştür. Katılımcıların hepsi tüm soruları yanıtlamıştır. Ana kütle, ayrıca konuyla ilgili derinlemesine görüş ve uzmanlık araştırması yapmak üzere bir panel uzmanıyla iki kez istişarede bulunmuştur (HSBC, 2017). Bu anket ile elde edilen önemli veriler aşağıda belirtilmiştir.

Ankete katılanların %84'ü, daha iyi bir hizmet elde etmek amacıyla kendi bankalarıyla kişisel verilerini paylaşacaklarını belirtmiştir. En iyi anlaşmayı bulmak için, makinelerin çok miktarda veriyi analiz etme gücüne rağmen, sadece %11'lik kısmı chatbot'lar[18] da dahil olmak üzere her tür robota güvenerek tasarruf hesabı açma ya da ipotek önerisi almayı kabul etmiştir. Bununla birlikte, kimliklerini doğrulamak için geleneksel

[18] Chatbot; yapay zeka teknolojisini kullanarak insansı cevaplar verebilen bir yazılımdır.

şifreleme yöntemlerine güvenenlerin oranı %70 iken yaklaşık beşte birlik bir kesim (%21) ise parmak izi tanıma özelliğini kullandığı tespit edilmiştir. Ayrıca ankete katılanların sadece %6'sı güvenlik avantajlarından bağımsız olarak ses tanıma özelliğini kullandıklarını ifade etmişlerdir.

Çalışmanın diğer sonuçları ana hatlarıyla aşağıda özetlenmeye çalışılmıştır.

Erkekler bilgisayarlar, dizüstü bilgisayarlar, fakslar, çağrı cihazları ve sabit hatların en yoğun kullanıcıları iken, kadınlar ise erkeklere göre daha çok giyilebilir teknoloji, uygulama ve tablet kullanmaktadırlar. Teknolojinin ilerici doğası gereği, insanların önemli bir çoğunluğu yeni teknolojileri hiç duymamıştır ve eğer duymuşlarsa, yaptıklarını açıklayamamışlardır.

Yine ankete göre en az anlaşılan yeni teknolojilerin anlaşılmama oranı şu şekildedir:

1. Blok zinciri, dijital kayıt teknolojisi (% 80),
2. Robotik danışmanlar, otomatik yatırım danışmanlığı (% 69),
3. Sosyal medyaya bütünleşik (WeChat ve Facebook benzeri) finans uygulamaları (% 60).

Anketten elde edilen bir diğer bulgu ise katılımcıların nakit yönetiminde geleneksel işlem kanallarına bağlılık oranlarıdır. Bunlar;

1. Bir bankanın web sitesi aracılığıyla online bankacılık (% 67),
2. ATM cihazlarının kullanılması (% 55),
3. Şube ziyaretleri (% 41).

Görülüyor ki, beklenen bir şekilde bilinen yöntemlerin kullanımı devam ederken, en az anlaşılabilir olması için blok zinciri ve dijital kayıt defteri teknolojisi tanıtılmaya (açıklanmaya) ihtiyaç duymaktadır.

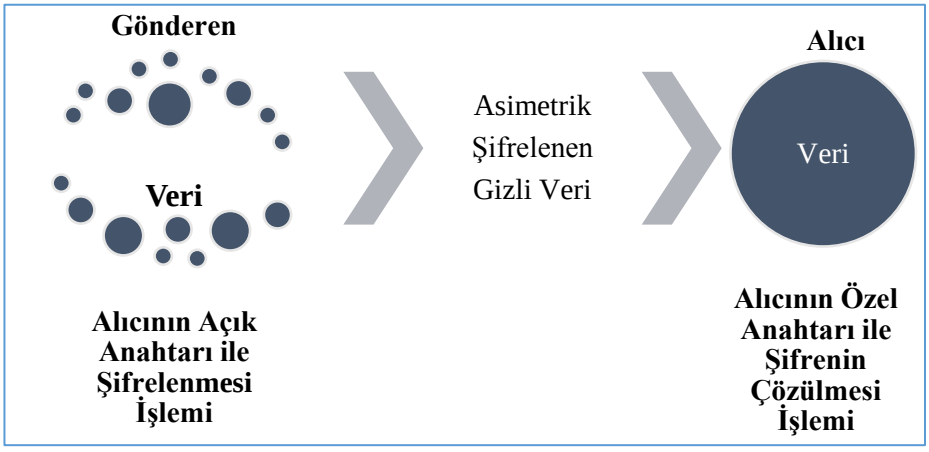
1.4.1. Açık Anahtar Şifrelemesi

Açık anahtar şifrelemesi, gizli anahtarların değiştirilmesine gerek olmadan veri alışverişini yapan iki taraf arasındaki gizli iletişim için bir yöntemdir. Açık anahtar şifrelemesinin başlıca görevi, mevcut güvenlik düzenine sahip olmayan kişilerin iletileri

güvenli bir şekilde iletebilmesini sağlamaktır. Açık anahtar şifrelemesi gönderenin ve alıcının gizli kanalları kullanarak gizli şifrelerini takas etme ihtiyacını ortadan kaldırmaktadır. Tüm iletişimler yalnızca açık anahtarlar içermektedir ve hiçbir özel anahtar iletilmemekte veya paylaşılmamaktadır. Dünyada temel ve yaygın olarak kullanılan bir teknoloji olan açık anahtar şifrelemesi, internette bilgilerin güvenli bir şekilde iletilmesini sağlamak amacıyla kullanılmaktadır. İlk olarak hassas veri aktarım işlemleri için bankacılık kurumları tarafından benimsenmiştir. Bir mesajı şifrelemek için kullanılan anahtar, şifreyi çözmek için kullanılan anahtardan farklı olduğu için asimetrik şifreleme olarak da bilinmektedir. Açık anahtar şifrelemesinde bir kullanıcı bir çift şifreleme anahtarına sahiptir. Bunlar açık (genel) anahtar ve özel anahtar olarak adlandırılmaktadır. Asimetrik anahtar şifrelemesinde, simetrik anahtar şifrelemesinin (aynı anahtarın şifreleme ve şifre çözme için kullanılması) aksine bir anahtar çifti kullanılmaktadır;

- Açık anahtar
- Özel anahtar

Açık anahtar yaygın şekilde dağıtılabilirken özel anahtar ise gizli tutulmaktadır. İletiler alıcının açık anahtarı ile şifrelenir ve yalnızca açık anahtara karşılık gelen özel anahtarı kullanarak şifresi çözülebilmektedir. Anahtarlar matematiksel olarak ilişkilidir ancak özel anahtarlar açık anahtarlardan türetilememektedirler (Kar ve Dey, 2010: 3, Network Associates, 1999: 15).



Şekil 1.6. Açık Anahtar Şifrelemesi

Kaynak: Yazar tarafından hazırlanmıştır

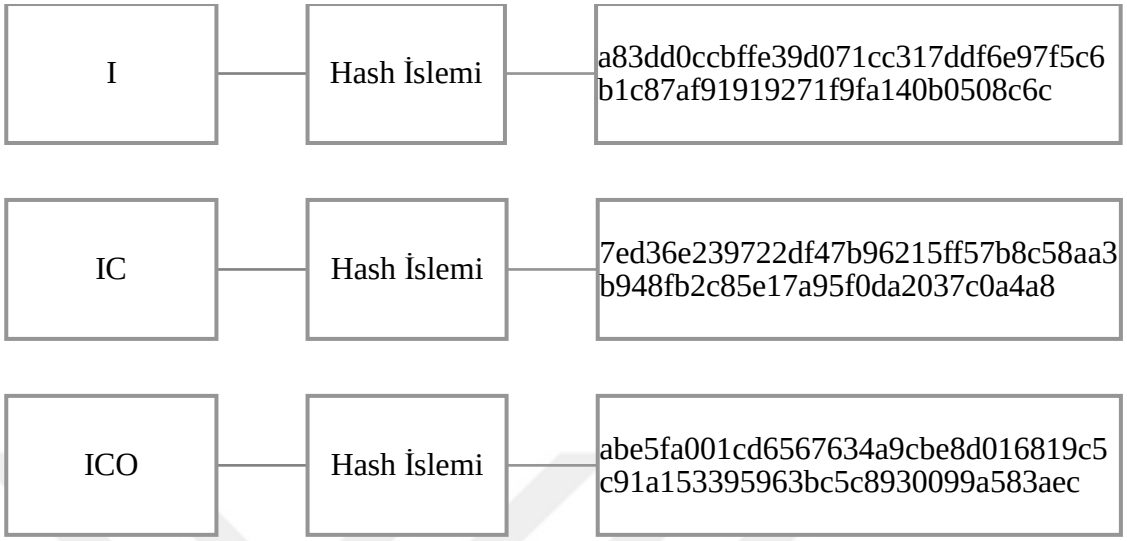
Şekil 1.6'ta görüleceği üzere, açık anahtar veriyi şifrelemek için kullanılırken, özel anahtar verilerin şifresini çözmek için kullanılmaktadır. Örneğin, bir kişi kendisi ve diğer taraflar arasındaki veri alışverişini korumak amacıyla asimetrik anahtar şifrelemesi kullanmak istiyorsa, bu amaçla bir çift anahtar (açık ve özel anahtarlar) oluşturulur. Daha sonra açık anahtar diğer taraflara gönderilirken, özel anahtar ise söz konusu olan kişi tarafından saklanır. Üçüncü bir taraf bu kişiye veri göndermek istediğinde üçüncü taraf verileri şifrelemek için açık anahtarı kullanır. Özel anahtara sahip olan alıcı, üçüncü şahıs tarafından gönderilen şifrelenmiş olan verilerin şifresini çözebilmektedir. Asimetrik anahtar şifrelemesi, iki yabancının, veri güvenliği hakkında endişe duymadan ve tek bir anahtar paylaşmadan kamuya açık ağ üzerinde gizli verileri paylaşmasına izin vermektedir (Hong Kong Monetary Authority, 2016: 25). Asimetrik anahtar şifrelemesi yaygın olarak, ileti gönderilirken ve yayınlanırken dijital imza[19] olarak kullanılmaktadır. Kripto paralar yapılarında asimetrik anahtar şifrelemesi, cüzdan adresi (açık anahtar) ve cüzdan parolası (özel anahtar) olarak kullanılabilmektedir.

1.4.2. Kriptografik Hash Fonksiyonu

Bitcoin, sanal parayı bir dijital imza zinciri olarak tanımlamaktadır. Paranın el değiştirmesi sırasında her sahip kendi dijital imzasıyla parayı bir sonrakine gönderirken bir önceki işlemin özetini (hash), bir sonraki sahibinin açık anahtarı ile imzalar ve bu imzayı paranın sonuna eklemektedir. Ödemeyi alan kişi sahiplik zincirinin doğruluğunu kanıtlamak için dijital imzaları doğrulayabilmektedir (Nakamoto 2008: 2-3). Bir kriptografik işlem özet fonksiyonunda $H : \{0,1\}^* \rightarrow \{0,1\}^n$ herhangi bir istenilen uzunluktaki mesaj olan M için n bitlik bir sabit uzunlukta hash değerini hesaplayan bir fonksiyondur. Kriptografik hash fonksiyonu, dijital imza şemaları, kimlik doğrulama kodları, parola işlem özet fonksiyonları ve içerik adresli depolama da dahil olmak üzere pek çok uygulamada kullanılan temel bir kriptografi yöntemidir. Bu uygulamaların birçoğunun güvenliği veya düzgün işleyişi, kırılmasının[20] (çarpışmaların bulunmasının) pratik olarak mümkün olmadığı varsayımına dayanmaktadır (Stevens vd. 2017: 1). Güvenli Hash Algoritması (SHA-Secure Hash Algorithm), işlevinin daha iyi anlaşılabilmesi için Şekil 1.7'de örnek olarak, farklı girdiler kullanılarak SHA-256

[19] Dijital imza; dijital iletinin özgünlüğünü gösteren matematiksel bir şemadır.
[20] Farklı içeriklerin aynı hash değerini alabilme durumu.

hesaplaması gerçekleştirilmiştir.



Şekil 1.7. SHA 256 Hesaplaması Örneği

Kaynak: hashgenerator.de (2017)

Güvenli Hash Algoritması, bir dizi kriptografik hash işlevinden oluşmaktadır. Kriptografik hash, bir metin veya veri dosyası için bir imza gibidir. SHA-256 algoritması neredeyse benzersiz, sabit büyüklükte 256 bitlik (32 baytlık) bir hash üretmektedir. Kısaca ifade etmek gerekirse Hash, verilerin parmak izidir.

256 adet ardışık 0 veya 1'le, $2^{256} \approx 1.15 \times 10^{77}$ farklı gizli anahtar üretilebilmektedir. Gizli anahtar üretmek, 1 ile 2^{256} arasında rastgele bir tam sayı üretmek olarak da görülebilir. Herhangi iki farklı kişinin gizli anahtarının aynı olma ihtimali (çarpışma), yaklaşık 10^{77} 'de 1'dir. 10^{77} çok büyük bir rakamdır, gözlemlenebilen evrende $\approx 10^{80}$ atom olduğu düşünülmektedir. Eğer açık anahtardan gizli anahtar elde ediliyor olsaydı sistem tamamen güvensiz olmuş olurdu (Çarkacıoğlu, 2016: 23).

Günümüzde birçok uygulama SHA-1'i kullanmakta olup teorik saldırılar 2005 yılından beridir bilinmektedir. SHA-1 resmi olarak 2011'de ABD Federal Devletinin Standart Enstitüsü (NIST, National Institute of Standards and Technology) tarafından kırılabilmiştir (shattered.io, 2017). Google ve Centrum Wiskunde & Informatica'daki (CWI) kriptoloji grubu tarafından toplamda dokuz kentilyondan fazla

(9.223.372.036.854.775.808) SHA-1 hesaplamaları yapılmıştır. Saldırının ilk aşamasını tamamlamak için 6.500 yıllık CPU (Merkezi İşlem Birimi) hesaplaması ve ikinci aşamayı tamamlamak için ise 110 yıl GPU (Grafik İşleme Birimi) hesaplaması sonucunda SHA-1'in kırılabildiği gösterilmiştir (shattered.io, 2017). Bu araştırma Uluslararası Kriptolojik Araştırmalar Birliği (IACR, International Association for Cryptologic Research) tarafından verilen Crypto 2017 en iyi araştırma ödülüne layık görülmüştür. SHA-1'e yönelik pratik saldırı ile farkındalığı artıracak ve endüstriyi SHA-256 gibi daha güvenli alternatiflere hızla geçmesi için ikna etmek amacıyla bir çalışma yapmışlardır (Stevens vd. 2017: 1). Finansal boyutta blok zinciri ile ilgili tanıtıcı ve derinlemesine teknolojik incelemeler, özellikle de ödemeler alanında ki kullanımı için bir gerekliliktir.

1.5. Alternatif Para Birimi Olarak Sanal Para Birimi

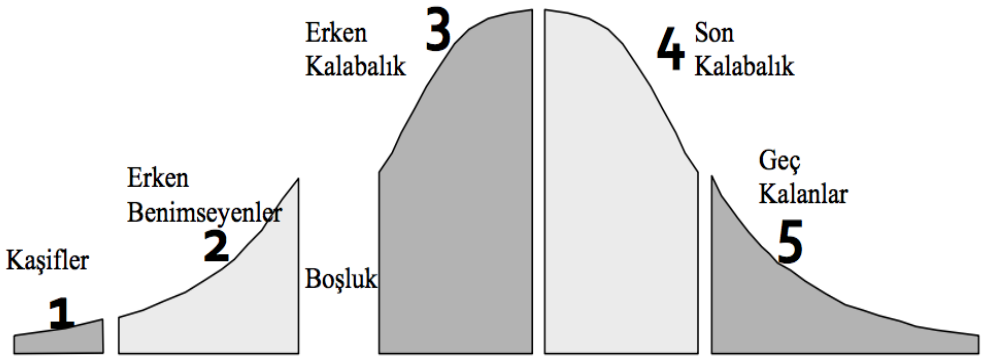
Finansal aracılar hayatta kalabilmek için gelişen ekonomik ortamda kendilerine kar sağlayıcı yeni ürünler araştırmak ve geliştirmek zorundadırlar. İşte bu gereklilik finansal yeniliklerin temelini oluşturmaktadır (Parasız, 2005: 3). Tarih boyunca değer değişimini kolaylaştıracak, alıcıları ve satıcıları koruyan madeni paralar, kağıt paralar, akreditifler ve bankacılık sistemleri gibi güven enstrümanları ortaya çıkmıştır. Geleneksel olarak bankalar ve diğer finansal kurumlar hesapların korunması, kredilerin uzatılması ve ödemelerin kolaylaştırılması gibi mali faaliyetlerin koruyucuları olarak görev yapmışlardır. Ekonomik anlamda ticarette, parasal hareketin belkemiği olmuşlardır. Tüm finansal sistem, merkezi bir güven modeli üzerine inşa edilmiştir ve finansal kuruluşlar tarafından finansal faaliyet akışı sağlanmakta ve denetlenmektedir. Yine de birçok ticari işlem kısıtlamalardan ötürü, pahalı ve savunmasız kalmaktadır (Gupta, 2017: 4). Bunlar;

- Nakit, yalnızca yerel işlemlerde ve nispeten küçük miktarlarda daha yararlıdır.
- İşlemler ve ödeme arasındaki zaman uzun olabilmektedir, üçüncü şahısların veya arabulucuların bulunması gerekliliği işlev etkinliğini azaltmaktadır.
- Dolandırıcılık, siber saldırılar ve basit hatalar iş maliyetini ve karmaşıklığını oldukça artırmaktadır. Merkezi bir sistemin ele geçirilmesi durumunda ağdaki tüm katılımcılar riske maruz kalmaktadır.

- Kredi kartı kuruluşları esasen yüksek katılım ücretlerine sahip yapılar oluşturmaktadır. Ayrıca ticari işletmeler genellikle önemli olan evrak işlemlerini ve zaman alan onay işlemlerini içeren yüksek maliyetli masraflarını ödemek zorundadırlar.
- Dünyadaki insanların yarısının bir banka hesabına erişimi bulunmamaktadır ve işlem yapmak için ödeme sistemleri geliştirmeleri gerekmektedir.

Mükemmel bir şekilde işleyen ve bir eksiği bulunmayan piyasalarda yenilik söz konusu değildir. Başka bir deyişle, bir ürünün gerçekten finansal yenilik olabilmesi için finansal piyasaları daha etkin ve tam rekabetçi hale getirmesi gerekmektedir (Akel, 2006: 4). Geçtiğimiz yıllarda, endüstrilerdeki teknolojik yeniliklerin hızı büyük ölçüde artış göstermiştir. Blok zinciri modeli finansal kuruluşlara kayıt tutma, hesap dengeleme, para alışverişi, dolandırıcılık tespiti ve diğer olguları etkili bir şekilde gerçekleştirmek için gerekli istikrar, güvenlik ve gizliliğe sahip çeşitli hizmetleri sunma olanağı sağlamaktadır. Güvenilir bir bankacılık ekosisteminin daha da geliştirilmesi gerektiğinde bu model gözetim hizmeti sağlayan devlet mevzuatı ve izleme organları ile birlikte kullanılabilir. Gelişen teknolojiyle birlikte bilişim sistemlerindeki (telefon, internet, ağlar, veri depolama ve bilgi işlem gücü) önemli yenilikler ve gelişmeler, alıcıların ve satıcıların arasındaki mesafeyi azaltmakta ve bazen neredeyse tamamen ortadan kaldırmaktadır. Aracı kurumları ortadan kaldırmaya dayalı bu yeni iş modelleri, aynı zamanda diğer sektörlerdeki geleneksel görev ve işlevleri de ortadan kaldırmaktadır. Bunlara Amazon, eBay, Uber ve Airbnb gibi uygulamalar örnek verilebilir. Bu şirketler, kendi endüstrisinde yer alan değerler zincirinin sürtüşmesini gidererek tüketicinin lehine sonuçları olan ve daha yüksek bir satın alma gücü sağlayan yenilikçi ürünler ve hizmetler sağlamaktadır. Bu durum işlemleri çeşitlendirerek işlemlerin kolaylığını, hızını ve verimliliğini artırırken finansal hizmetler endüstrisindeki katılımcıları etkisiz hale getirecek dijital, kripto ve sanal para birimi olarak adlandırılan yeni ve alternatif ödeme araçları çıkartmaktadır. Blok zinciri kolayca erişilebilen güvenli ve yetkisiz müdahalelere izin vermeyen bir dağıtık işlem kaydı teknolojisidir. Blok zinciri kullanıcı ağı üzerinden dağıtılan ve paylaşılan bir işlemler kaydıdır. Blok zinciri bir dizi veri bloğundan oluşmaktadır ve bunlardan her biri bir dizi işlem içermektedir. Açık blok zinciri yapılarında bloklar, elektronik olarak birbirine zincirlenir ve şifreleme ile kilitlenerek, her işlemin kamuya açık bir kaydı

oluşturulmaktadır. Yapı, eklenen bloklar ile pekiştirildiğinden dolayı ne kadar fazla blok var ise blokların değiştirilme olasılığı da o kadar düşüktür. Bilinen birçok blok zinciri tabanlı uygulama, ara yüz ve altyapı sağlayıcı girişimler mevcuttur. Bunların arasında en büyük ve en yaygın olarak kullanılan blok zinciri uygulaması ise Bitcoin sistemi ağıdır. Startup'ların[21] yeni görev alanını belirlemeleri ve pazardaki varlıklarının büyük katılımcı kitlesi tarafından fark edilmesi zaman almaktadır (Biondi, Hetterscheidt ve Obermeier, 2016: 1-7). Bu durum finansal teknoloji ve blok zincir uygulamaları için de aynı şekilde geçerlidir. Şekil 1.8'de gösterilen Teknoloji Adaptasyon Hayat Eğrisi, kullanıcı (benimseyici) grupların demografik ve psikolojik özelliklerine göre yeni bir ürünün veya yeniliğin benimsenmesini veya kabulünü tanımlayan bir sosyolojik modeldir.



Şekil 1.8. Teknoloji Adaptasyon Hayat Eğrisi

Kaynak: Moore, (1991: 13)

Günümüzün tüketici ihtiyaçları önemli derecede ve hızda gelişmekte olduğu bilinen bir durumdur. Teknoloji adaptasyon hayat eğrisi, kullanıcıların demografik ve psikolojik özelliklerine göre, yeni bir ürün veya yeniliğin kabulünü veya benimsenmesini sağlayan bir sosyolojik modeldir. Zaman içerisinde klasik, normal dağılım göstermektedir. Model ilk kullanıcı grubu olarak yeni bir ürünü kullananları "kaşifler" olarak tanımlamaktadır ve bunları "erken benimseyenler" izlemektedir. Bir müddet geçtikten sonra "erken kalabalık" diye adlandırılan daha büyük bir kitle ise teknolojiyi kullanmaya başlar.

[21] Startup'ın kelime anlamı, bir şeyi harekete geçirmek için yapılan iş ya da süreç olarak tanımlanmakla birlikte, kaynaklarda genelde yeni girişim olarak kullanılmaktadır.

Bunları "son kalabalık" takip ederken, en son "geç kalanlar" ise bu teknolojiyi kullanmaya başlar.

İlk web sitesi, 1991 yılında çevrimiçi olan "info.cern.ch/" dir (info.cern.ch, 1991). İlk olarak ağ üzerinden e-posta gönderimi 1971 yılında, Ray Tomlinson tarafından gerçekleştirilmiştir (computinghistory.org.uk, 2017). 2017 yılına gelindiğinde ise dünya çapında e-posta kullanıcılarının sayısı 3,5 milyarın üzerindedir. 2021 yılının sonuna kadar dünya çapındaki e-posta kullanıcılarının sayısının 4 milyarın üzerine çıkması beklenmektedir. Dünya çapındaki nüfusun yaklaşık yarısı e-posta kullanmaktadır (Statista ve The Radicati Group, 2017). E-posta kullanımı internetin gelişimine büyük bir katkı sağlamıştır. Bu katkıyı blok zinciri de kripto para ile sağlamaktadır. Ödemeler alanındaki sanal para kullanımı şu an için sınırlı kalmaktadır. Herhangi bir merkez bankasının görevleri ve ödeme sistemlerinin düzgün çalışması dahil olmak üzere maddi bir risk taşımamaktadır (ECB, 2015: 5).

Özellikle merkezi olmayan bir hesap kütüğünün kullanılmasına dayanan kripto para birimleri, finansal piyasaların yerinden yönetimli ödeme mekanizması üzerine farklı yönlerde daha geniş ve çeşitli ekonomik etkilere sahip olabilecek bir yeniliktir. Bu etkiler arasında iş modelleri ve sistemlerinde potansiyel aksamaların giderilmesinin yanı sıra yeni ekonomik etkileşimlerin ve bağlantıların kolaylaştırılması da sayılabilmektedir. Özellikle, kripto para birimlerinin ve dağıtık kayıt teknolojisinin perakende ödeme hizmetleri üzerindeki potansiyel etkileri oldukça önemlidir. Çünkü bu tür programlar belirli perakende ödemelerini kolaylaştırma potansiyeline sahiptir.

E-ticaret, sınır ötesi işlemler, kişiden kişiye ödemeler ve muhtemelen son kullanıcılar (tüketiciler ve tüccarlar gibi) için ödemelerin daha hızlı ve daha ucuz hale gelmesini sağlayabilecektir. Bununla birlikte kripto para birimleri ve dağıtık kayıt teknolojisi, yüksek hacimli işlemler veya fon transferlerinin ötesinde diğer varlık türleri için de yaygın olarak kullanılmaya başlanırsa, merkez bankaları için ödeme sistemi gözetim, düzenleme ve finansal istikrar gibi diğer alanlar üzerindeki etkileri ve para politikası daha belirgin hale gelebilir (BIS, 2015: 3).

Tıpkı geleneksel ödeme sistemlerinde olduğu gibi herhangi bir elektronik ödeme sisteminde de tüm katılımcıların kabul edebileceği güvenilir bir kayıt yönteminin olması

gerekmektedir. Bu güvenilir kayıt yöntemleri ise kriptografi ve kripto paranın kullanılması ile sağlanmaktadır.

Kripto para birimlerinin değeri genellikle dolar cinsinden ifade edilmektedir. Bitcoin örneğinde, en çok işlem gören ulusal para birimlerinin % 20'den fazlası dolar, neredeyse %20'si Çin renminbisi ve yarıdan fazlasını avro dahil olmak üzere diğer para birimleri cinsi üzerinden takas edilmektedir (coinhills.com, 2017). Ancak, bu oranlar sürekli değişiklik göstermektedir. Kripto para birimleri hala nispeten gelişmekte olduğundan arbitraj olanakları sunmaktadır. Ayrıca kripto para birimlerinin fiyatlandırılmasının tamamen görünmez el [22] ile olup olmadığı ya da ulusal para birimlerinin değer değişiminden etkilenip etkilenmediği tartışmaya açık konulardır. Kripto para alanında oluşan biriken veriler ile araştırmalar yapmak etkilerini belirlemek mümkün olacaktır.

[22] Görünmez el; Adam Smith tarafından 1776 yılında, "Ulusların Zenginliği" kitabında kullanılmıştır. Bireysel ilgi (çıkar) ile gerçekleştirilen eylemlerin, kasıtsız olarak oluşturduğu sosyal faydaları tanımlamak için kullanılan bir terimdir. Serbest fiyat mekanizması işleyişi olarak tanımlanabilir.

İKİNCİ BÖLÜM

BLOK ZİNCİRİ SİSTEMATİĞİ

Finansal piyasalarda yenilik kavramı, literatürde çokça ele alınmış bir konudur. Finansal yenilik, tamamıyla yeni daha önceden keşfedilmemiş bir fikirden ziyade mevcut fikrin geliştirilerek değiştirilmesidir (Akel, 2006: 6). Finansal teknolojiler, finansal hizmetler alanında kullanılan modern teknolojilerden oluşmaktadır. Elektronik ödeme sürecinin derinlemesine anlaşılabilmesi için geleneksel veya geleneksel olmayan ödeme sisteminin işleyişini anlamak gerekmektedir. Geleneksel bir ödeme süreci, banka aracılığıyla nakit veya ödeme bilgilerini (yani, çek ve kredi kartlarında olduğu gibi) alıcıdan satıcısına aktarmayı içermektedir. Nakit ödeme, bir borçlunun banka hesabından para çekmesi ve nakit karşılığını alacaklıya vermesi, borçlunun ödemesini bankanın hesabına yapmasını gerektiren ödeme türüdür. Blok zinciri, bilgisayar ağları içerisindeki değer transferini sağlayan bir veri tabanıdır. Blok zinciri işlemlerinde üçüncü bir taraf gerekmeksizin güvenilir işlemler yapılabilir ve bunun sonucunda birçok alanı etkilemesi beklenmektedir. Bununla birlikte, bu teknolojinin yaygınlaşması için açıklığa kavuşturulması gereken, çözülmesi gereken birçok konu mevcuttur. Web tarayıcıları ve e-posta programları gibi internet uygulamaları, barındıkları aygıtlardaki yazılımların birbirleriyle nasıl iletişim kurabileceğini tanımlayan protokolleri kullanmaktadırlar (OECD, 2016: 107). Geleneksel protokollerin çoğunun amacı bilgi alışverişi yapmaktır, blok zinciri kullanımı ile protokollerin değer değişim aracı olabilmesi sağlayabilmektedir.

Blok zincirleri, bankalardaki ödemeler ve kredi bilgi sistemlerinin altında yatan teknolojiler alanında devrim yapabilir, böylelikle onları iyileştirerek dönüştürebilecek potansiyele sahiptir. Blok zinciri uygulamaları "çok merkezli, zayıf aracılık" senaryolarının oluşumunu teşvik ederek bankacılık endüstrisinin etkinliğini artıracaktır. Ancak her finansal yenilik sürecinin başlangıcında olduğu gibi düzenleme, verimlilik ve

güvenlik sorunlarının tartışmalara yol açacağını belirtmek gerekir. Gelecekte blok zinciri teknolojisinin teknik, düzenleyici ve diğer problemleri nihai olarak çözülmesi beklenmektedir. Dolayısıyla blok zincir teknolojisinin bankacılık sektörüne entegre olması yakın gelecekte büyük olasılıkla ortaya çıkacaktır (Guo ve Liang, 2016: 11).

Blok zinciri teknolojisi, sınırlı veya belirlenmemiş sayıdaki eşten eşe ağındaki birçok katılımcının yeni işlemlerin girişi, yeni işlem bloklarını doğrulaması ve bunların (önceden onaylanmış işlemlerin) işlem bloklarını zincire eklenmesi olarak bilinmektedir. Blok zinciri onaylanmış ve birbirine bağlı bloklar içermektedir. Bilgi bütünlüğünü sağlamak için sürekli güncellenir ve tüm katılımcılara dağıtılır. Ağa katılan herhangi bir taraf, bir blok zinciri dosyasının veya karmasının en son sürümünü elde eder. Blok zincirindeki bir varlığın sahipliği hakkındaki bilgi DLT'lerde bir zincir halinde yapılandırılmaktadır (Pinna ve Ruttenberg, 2016: 15). Bloklar bir kitabın sayfaları olarak düşünülecek olursa blok zinciri de bir kitap olarak düşünülebilir. Gelişen ihtiyaçlarla beraber yenilikler ve finansal teknolojiler alanındaki ilerlemeler, bankaların ötesinde küçük finansal teknoloji firmaları tarafından da yapılabilmektedir. Uygulama Programlama Arayüzü[23] (API, Application Programming Interface), farklı yazılım bileşenlerinin veya sistemlerinin birbirleriyle etkili bir şekilde iletişim kurmasını sağlayan bir takım araçları tanımlamak için kullanılan terimdir. Yenilikçi finansal teknolojiler, kripto para entegrasyonu için bir API kullanarak bankalar, lider finansal hizmet sağlayıcıları veya finansal teknoloji firmalarının teknolojisine, destek olarak gerekli olan kilit alanlara dahil edilmelidir. Bu API'ler klasik ve yeni teknolojileri bir araya getirerek, teknolojik hizmetlerin kullanımını yapıtaşları arasında basitleştirmekte olup finansal lego'ya benzeyen dahil olma sürecini basitleştirebilme olanağı sağlamaktadır. Finansal teknoloji firmaları, bankacılık faaliyetlerinin alt yapısı ve tecrübelerinden yararlanabilirler. Finansal teknoloji firmaları ve bankalar farklılıklarına rağmen her iki tarafta da birlikte çalışmaktan yarar sağlayabilirler (Barberis vd. 2016: 20).

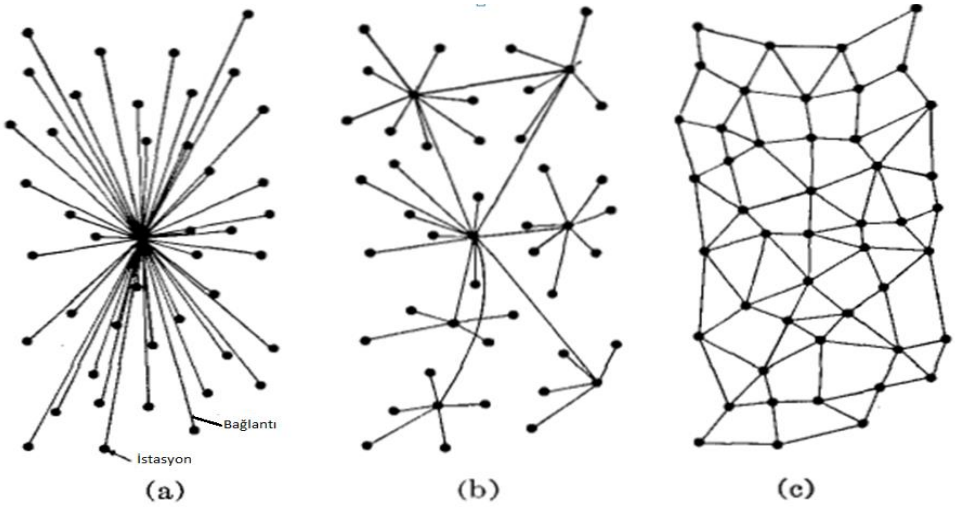
[23] Uygulama Programlama Arayüzü; bir hizmete, uygulamaya veya programa erişmek için kullanılan özellikler topluluğudur. Hizmet çağrıları, her çağrı için gerekli parametreler ve beklenen dönüş değerlerini içermektedir.

2.1. Blok Zinciri Teknolojisi

İnternet, ağ oluşumlarına ve platform temelli sosyal ve ekonomik modellere doğru bir kaymaya neden olmaktadır. Varlıklar paylaşılabilirken, sadece yeni etkinlikler değil aynı zamanda tamamen yeni iş modelleri ve kendini organize edebilen sosyal organizasyon fırsatları sunmaktadır. Blok zinciri gelişmekte olan bir teknoloji olarak, üçüncü bir tarafa ihtiyaç duymadan finansal ve finansal olmayan birçok faaliyetin gerçekleştirilebilmesini sağlamaktadır (WEF, 2015: 5). Yapısal olarak bir blok zinciri, güvenli bir şekilde zincirlenmiş bir dizi bilgi bloğudur. Katılımcılar, yeni bilgi parçaları oluşturduğunda veya bir varlık hakkında mevcut bir bilgiyi değiştirdiklerinde (örneğin, işlem kayıtları, statü değişiklikleri, yeni piyasa fiyatları veya yeni sahipler girildiğinde) yeni bloklar tanımlanmaktadır. İlk bloktan sonra yeni oluşturulmuş geçerli bloklar, güvenilen bir önceki bloğa güvenli bir şekilde zincirlenir. Böylece blokların güvenilirliğini garanti ederek güvenilir bir denetim kanıtı oluşturulmaktadır (Hong Kong Monetary Authority, 2016: 5). Bu işlemlerin altında yatan temel saik ise bir güven mimarisi oluşturmaktır.

Blok zinciri, Bitcoin'in ana teknolojik yeniliği olarak görülmektedir. Çünkü ağdaki tüm işlemler güven gerektirir ve blok zinciri ile birlikte bir kanıt mekanizması ile güven oluşturmaktadır. Kullanıcılar, madenciler tarafından muhafaza edilen dünya genelinde depolanan, merkezi olmayan birçok düğümden oluşan halka açık kayıt sistemine güvenmektedirler. Katılımcılar, banka gibi veya bir üçüncü taraf arabulucusu ile güven kurmak ve devam ettirmek zorunda kalmamaktadır. Merkezi ve güvenilir olmayan işlemler için yeni bir mimari olarak blok zinciri, kilit düzeye haiz önemli bir yeniliktir.

Blok zinciri, tüm taraflar arasında herhangi bir türdeki tüm işlemlerin küresel bazda dağılmasına ve yerinden yönetimine izin vermektedir (Swan, 2015: 5). Blok zinciri, ödemeler alanında çok hızlı kabul görmüş bir alt yapı hizmeti sunmaktadır. Evrensel bir hesap defteri gibi işlem yapabilecek bir yapıdadır. Dağıtık bir ağ yapısının, merkezi ya da çok merkezli ağ yapılarına göre farkı, Şekil 2.1'de gösterilmiştir.



Şekil 2.1. Merkezi, Çok Merkezli ve Dağıtık Ağ Yapıları

Kaynak: Baran vd. (1962: 4)

Blok zincirinin dağıtık ekosistemi para birimi olarak sunduğu altyapının yansıra ayrıca, birçok farklı uygulama alanıyla beraber, elektronik ödemeler için mevcut kurumsal platformların yerine kullanılabilecek ademi merkezi bir sistem oluşturabilir. Blok zinciri sistematiği güvenlik, kimlik yönetimi, merkezi olmayan yapılar, varlık yönetimi gibi konularda şu anda kullanılan ağ protokollerinin yerini alabilir. Bu ihtiyaçlardan doğan gereksinimleri karşılayabilecek özellikler blok zincirine eklenebilmektedir. Merkezi, Çok Merkezli ve Dağıtık Sistem Yapıları hakkında kısa bir bilgi vermek yerinde olacaktır.

- *Merkezi sistemler*; tüm kullanıcıların bir merkezi sunucuya bağlandığı ağ yapısıdır.
- *Çok merkezli sistemler*; ağ yapısında düğümler arasında birçok sunucunun bağlantı kurduğu eşler arası iletişim yapısıdır. Ağ üzerindeki aygıtlar birbirleriyle iletişim kurarak çeşitli düğümler arasındaki bağlantıları yönetebilmektedir. Bileşenlerin merkezi bir etkinin sonucunda değil, hedefleri gerçekleştirmek için çok merkezli bilgi üzerinde çalışan yapıya sahip sistemdir.
- *Dağıtık sistemler*; işlemlerin bileşenler arasında dağıtıldığı, bilgileri ileterek eylemlerin koordine edildiği sistemlerdir. Bileşenler ortak bir hedefe ulaşmak için birbirleriyle etkileşime girmektedir. Her bir düğüm bir sunucu görevi görebildiğinden merkezi bir başarısızlık (hata) noktası bulunmamaktadır.

Bitcoin blok zinciri teknolojisi, dijital paranın yeni bir biçimini elde etmek için BitTorrent [24] gibi eşler arası dosya paylaşım teknolojisi ve açık anahtar şifreleme yöntemini birleştirerek çifte harcama sorununu çözmektedir. Paranın mülkiyeti kamuya açık muhasebede kaydedilirken, kriptografik protokoller ve madencilik topluluğu tarafından teyit edilmektedir. Blok zincirinde herhangi bir kullanıcının işlem sırasında karşı tarafa veya merkez bir aracıya güvenmesi gerekmemektedir. Başka bir ifadeyle, kullanıcılar yaptıkları işlemlerde blok zinciri protokolü yazılım sistemine güvenmesi gerekmektedir. Zincirdeki "bloklar", sırayla kayıt defterine gönderilen işlem gruplarıdır ve blok zincirine sırasıyla eklenmektedir. Blok zinciri kayıt tutucuları, bir blok zinciri adresini girerek (kullanıcının *1DpZHXi5bEjNn6SriUKjh6wE4HwPFBPvfx* gibi bir genel anahtar adresi) işlenen blokları, internet siteleri üzerinden (örn. Bitcoin blok zinciri için www.Blockchain.info) genel olarak denetleyebilmektedirler. Genelde herkese açık olan *adres* başkalarının Bitcoin gönderebileceği yerdir. *Özel anahtar* ise Bitcoin'in başkalarına gönderilebileceği gizli şifreleme için kullanılmaktadır. Elektronik cüzdan (cüzdan yazılımı), Bitcoin'unu yönetmek için kullanılan yazılımdır. Kullanıcılar, başka bir kuruluşa kaydolmayı gerektiren merkezi bir hesaba ihtiyaç duymamaktadır. Bir adrese ait özel anahtar mevcut ise internet'e bağlı herhangi bir bilgisayardan (akıllı telefonlar da dahil olmak üzere) özel anahtar kullanarak bu adres ile ilişkilendirilmiş olan hesap yönetilebilmektedir. Ayrıca cüzdan yazılımı, sanal para birimi cinsinden gerçekleşen tüm işlem kayıtları olan blok zincirinin bir kopyasını, sanal para işlemlerinin doğrulandığı merkezi olmayan yapının bir parçası olarak da tutabilmektedir (Swan, 2015: 2).

Açık kaynak kod[25] kullanan blok zinciri protokollerinde tüm kullanıcılar, blok zinciri kodunun herhangi bir güvenlik kusuru veya bir arka kapı içerip içermediğini doğrulayabilmektedir. Blok zincirdeki tüm işlemlere ilişkin bilgiler tüm kullanıcılar tarafından erişilebilir durumdadır. Bu şeffaflık, tüm kullanıcıların diğer kullanıcıların kopyalarıyla tutarlı olması için defterin/kayıtların kopyasını kontrol etmelerini sağlamaktadır. Ayrıca düzgün olarak bağlı herhangi bir düğüm, veri kümesinde bir

[24] BitTorrent; bir sunucuya bağlı kalınmadan dosya paylaşımı için eşten eşe ağ yapısı.
[25] Açık kaynak kod (yazılım); orijinal kaynak kodun serbestçe kullanılabilen yazılımdır. Yeniden dağıtılabilir, değiştirilebilir ve (erişim olanağından) daha fazlasını sunabilen yazılım demektir.

işlemin mevcut olup olmadığını belirli bir kesinlik ile tanımlayabilmektedir. Bir işlemi oluşturan herhangi bir düğüm doğrulama sonrası işlemin geçerli olup olmadığını, gerçekleşip gerçekleşemeyeceğini makul bir düzeyde belirleyebilmektedir. Diğer bir ifadeyle, yeni işlem girişini geçersiz kılacak herhangi bir çelişkili işlem, kripto para biriminin başka bir yerde harcanması (iki defa harcanması), gibi işlemler onaylanmamaktadır (Gronbaek, 2016).

Finansal teknolojilerin birçok destekçisi, DLT'nin yaygınlaşmasının sadece finansal piyasaların teknolojik mimarisinde değil, aynı zamanda finansal sistemin yapısında da köklü değişiklikler getireceğini öne sürmektedir. Federal Reserve ekibi tarafından sektör katılımcılarıyla gerçekleştirilen röportajlar sonucu toplanan bilgiler, şirketlerin DLT düzenlemelerini geliştirme ve uygulama çabalarının arkasında birkaç ortak motivasyona sahip olduklarını göstermektedir. DLT varlıkların muhafaza edilip depolama, yükümlülükleri yerine getirme şekli, sözleşmeleri yürürlüğe koyma ve risklerin yönetilmesi alanında olumlu köklü değişiklikler yapabilmesini olası olarak görmektedir (Mills vd. 2016: 4-17). Bu değişiklikler;

- Karmaşıklığı azaltmak (özellikle çok taraflı, sınır ötesi işlemlerde),
- İyileştirilmiş uçtan uca[26] işlem hızı ile varlıkların ve fonların kullanılabilirliğini arttırmak,
- Birden fazla kayıt tutma altyapısında mutabakat ihtiyacını azaltmak,
- İşlem kaydında şeffaflığı ve değişmezliği arttırmak,
- Dağıtılmış veri yönetimi vasıtasıyla ağ esnekliğini arttırmanın yansıra operasyonel ve finansal riskleri azaltmaktır.

2.2. Blok Zinciri -Veri Madenciliği İlişkisi

Blok zinciri merkezi bir mimari olmadan aynı kayıtları tutma işlevselliğini sunmaktadır. Buradaki sorun ise kontrol etmek için merkezi bir otoritenin olmadığı bir işlemin meşruluğunu kanıtlamaktır. Blok zinciri sistematiği, madencilerin işlem kayıtlarının bir kopyasını elinde tutması sebebiyle kayıtları merkezi yapı olmadan tutmaktadır. Herkes herhangi bir işlemin blok zincirine eklenmesini talep edebilir. Ancak bu ekleme işlemi,

[26] Uçtan uca; çok sayında işlem aşamalarını ortadan kaldırarak veya azaltarak sürecin etkinliğini artırmayı hedefleyen süreçtir.

tüm kullanıcıların işlemin onaylanabilir olduğu konusunda hemfikir olması halinde gerçekleşebilmektedir. Örneğin; bir ev satışı için talebin yetkili kişiden geldiği, evin henüz satılmadığı ve alıcının da paraya sahip olduğu doğrulanmalıdır. Bu kontrol, her kullanıcı adına güvenilir ve otomatik olarak yapılmaktadır. Kaydedilecek her yeni işlem, diğer yeni işlemlerle birlikte geçmiş işlemlerin uzun bir zincirinde, en son bağlantı olarak bir blok paketi eklenmektedir. Bu zincir, tüm kullanıcılar tarafından tutulabilen blok zinciri dağıtık kayıt sistemini oluşturmaktadır. Bu çalışma *madencilik* olarak adlandırılmaktadır. Herkes bir madenci olabilir.

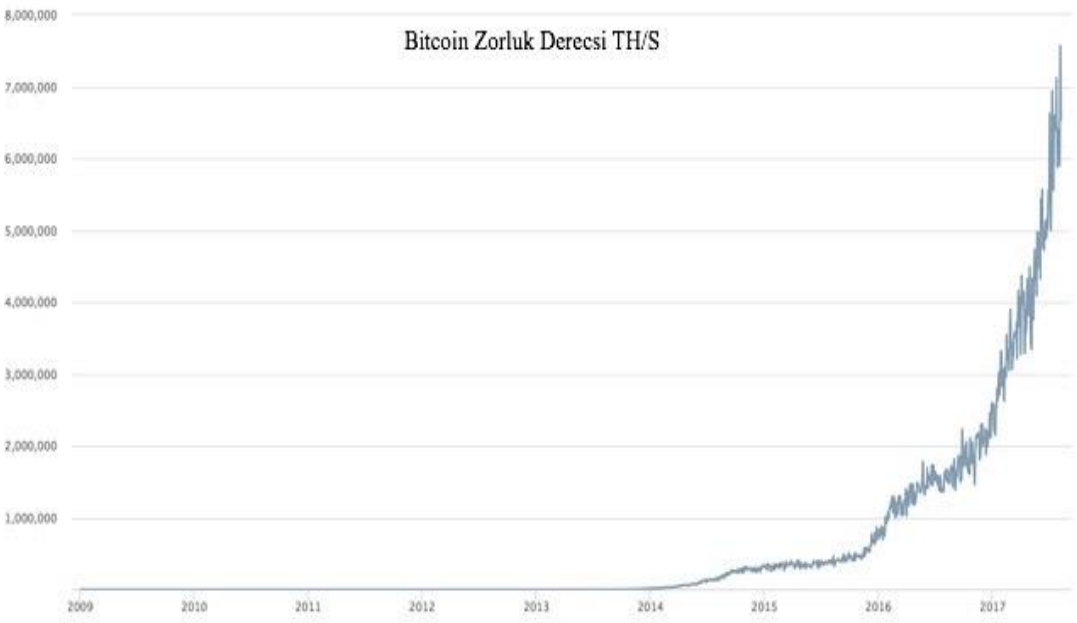
Madenciler, blok zincirine ekleme yapmak amacıyla geçerli bir blok oluşturmanın karmaşık matematiksel problemini çözen ilk kişi olmak için yarışırcasına çaba sarf etmektedirler. İnsanları bu işi yapmaya teşvik etmek için çeşitli yollar mevcuttur. Çoğu zaman geçerli bir blok oluşturup zincire ekleyen ilk madenci, işlemlerine ilişkin ücretlerin toplamıyla ödüllendirilmektedir. Bitcoin işlemlerinde ücretler şu anda işlem başına 0.10 € civarındadır. Bloklar düzenli olarak eklenmekte ve binlerce işlem yapılmaktadır (Boucher, Nascimento ve Kritikos, 2017: 5-7). Ancak Bitcoin veya diğer kripto para birimlerinin satın alma ve transaksiyon[27] maliyetleri işlem yapılan platforma göre değişiklik göstermektedir.

Madencilik, merkezi olmayan bir takas sistemine benzetilebilir (Çarkacıoğlu, 2016: 48). Protokole bağlı olarak kripto paranın tüm birimleri dolaşımda değil ise madenciler, enflasyon mekanizması gibi oluşturulan ve dolaşıma giren yeni para birimini teslim alabilmektedir. Zincire yeni bir blok eklenmesi, tüm kullanıcılar tarafından tutulan kaydın güncellenmesi demektir. Kullanıcılar yeni blokları yalnızca tüm işlemlerinin geçerli olduğu doğrulandığında kabul edebilmektedir. Bir tutarsızlık bulunursa blok reddedilir. İşlem doğru olduğunda blok eklenerek kalıcı ve halka açık bir kayıt olarak saklanmaktadır. Hiçbir kullanıcı bu eklenen geçerli bloğu kaldıramaz. Genel olarak bir kaydın imha edilmesi ya da tahrip edilmesi için aracıya saldırı gerekirken, bunu blok zincirine yapmak aynı anda kayıtların tutulan her bir kopyasına ayrı ayrı saldırı gerektirmektedir. Başka bir ifadeyle, tüm kullanıcılar karşılıklı kontrol amacıyla kendi orijinal sürümüne sahip olmasında dolayı "sahte kayıt defteri" bulunmamaktadır. İşlemlerin kontrol edilmesini ve eklenmesini onaylayan ya da reddeden özel bir makam

[27] Transaksiyon; bir hesabı etkileyen, hesap sahibi ya da isteği üzerine yapılan faaliyet.

bulunmadığı için tüm işlemler şeffaftır ve blok zincirleri genellikle izinsiz olarak tanımlanır. İzin verilen blok zincirleri, izinsiz muadillerinden daha az şeffaf ve merkezi bir yapıda olacaktır. Bu nedenle, farklı sosyal ve politik değerleri somutlaştırmaktadırlar (Boucher, Nascimento ve Kritikos, 2017: 5-7).

Bitcoin madenciliği, Bitcoin ağının işlemleri onaylaması amacıyla bilgisayarlara matematiksel işlemler yaptırmak ve güvenliği artırmak anlamına gelmektedir. Bitcoin madencileri yaptıkları işin ödülü olarak onayladıkları işlemlerin masraflarını (faturalarını) ve yeni oluşturulan Bitcoin'leri hak etmektedir. Madencilik ödülleri ne kadar hesap yapıldığıyla doğru orantılı olup rekabetçi bir ortamda belirlenmektedir. Tüm Bitcoin kullanıcıları madencilik yapamamaktadır. Madencilik para kazanmanın kolay bir yolu da değildir (bitcoin.org, 2009). Madencilerin yapması gereken hesaplamalar sürekli olarak zorlaşmaktadır ve madencilere verilen ödül yaklaşık her dört yılda bir yarıya inmektedir. Maksimum elde edilecek Bitcoin sayısı 21 milyonla sınırlıdır. Hiç kimse, hiçbir kuruluş, Bitcoin sistemine dışarıdan para arz edemez. Oysa, kağıt banknotlar halindeki itibari para, merkezi otoriteler tarafından basılmakta ve uygun görüldüğünde ek para arzı sağlanmaktadır (Çarkacıoğlu, 2016: 13). Bitcoin madenciliğinin zorluk derecesi ve ne anlama geldiği Grafik 2.2 ile Tablo 2.1'de anlatılmaya çalışılmıştır.



Grafik 2.1. Veri Madenciliği Zorluk Derecesi - Bitcoin Örneği

Kaynak: blockchain.info (2017)

Zorluk Derecesi, Bitcoin yapısında yeni bir blok bulmanın ne kadar zor olduğunu gösteren göreceli bir ölçüttür. Zorluk derecesi periyodik olarak madencilik ağı tarafından ne kadar hash gücünün kullanıldığına bağlı olarak değerlendirilmektedir. Şekil 2.2'den anlaşılacağı üzere, Bitcoinin zorluk derecesi 2017 ortalarında 7 Milyon Tera-Hash/s boyutuna ulaşmıştır. Blok zinciri madenciliği uygulamalarında karşılaşılan zorluk, genelde yeni bir blok bulmanın, şimdiye kadar olabilecek en kolay blok ile karşılaştırıldığında ne kadar zor olduğunun ölçeğidir. Kullanımına göre, işlemler yalnızca tüm blokların en büyük kümülatif zorluğuna sahip ana zincire ait olduğunda doğrulanmış olup kabul edilmektedir. Bu işlemlerin ne anlama geldiği Tablo 2.1'de kısaca açıklanmaya çalışılmıştır.

Tablo 2.1. Hash/Saniye Ölçü Birimleri

1 Tera-Hash/s	1.000.000.000.000 Hash Hesaplaması / Saniyede
1 Giga-Hash/s	1.000.000.000 Hash Hesaplaması / Saniyede
1 Mega-Hash/s	1.000.000 Hash Hesaplaması / Saniyede

Kaynak: Yazar tarafından hazırlanmıştır

Bitcoin madenciliği temel olarak, blok başlığının çift SHA256 algoritması ile elde edilen özetinin başlangıç kısmında belli sayıda sıfır olmasını inceleyen süreçtir. Teknik olarak işlem özet fonksiyonu değerinin başlangıç kısmındaki sıfırların sayısı, hedefin mevcut değerinin zorluk değerine bölünmesi ile elde edilmektedir. Temel olarak yapılan işlem bloğun başlık kısmına çift SHA256 algoritması uygulanarak hedeflenen değeri bulmaktır (Balcısoy, 2017: 23). Bitcoin madenciliğinde Hash oranı ise Bitcoin ağının işlemci gücünün ölçü birimidir. Bitcoin ağı güvenlik amacıyla aşırı matematiksel işlemler yapmaktadır. Ağın 10 TH/s hash oranına varması saniyede 10 trilyon hesap yapabilmesi anlamına gelmektedir (bitcoin.org, 2017). Bu işlemler küresel boyutta oldukça maliyetli bir hal almaktadır. Bir Bitcoin transaksiyonunu gerçekleştirebilmek için tüketilen elektrik 223 kilowatt saattir (digiconomist.net, 2017). Bu durum elektronik ödemeler alanındaki kullanımı için oldukça düşündürücüdür.

2.3. Blok Zincirinin Temel Bileşenleri

İnternetin bilgiyi demokratikleştirdiği gibi blok zincirinin de bazı değerleri demokratikleştirmesi beklenilmektedir (WEF White Paper, 2017: 8). Blok zinciri, hükümet tarafından kamu yararının korunmasının beklenildiği para, servet, fikri mülkiyet ve farklı değerlerin her türlü biçiminin yönetimi ile ilgili olabilmektedir. Bazı kurumlar ödemelerde, takaslarda ve uzlaşmalarda aracılık yapmaktadır ve finansal sistemin düzgün işleyişinin geliştirilmesinde bir veya daha fazla kritik görev üstlenmektedir. Bu roller genelde finansal, operasyonel ve hukuksal risk yönetimi ile birlikte hizmet sunumu kapsamında müşterilerine ve hizmet sundukları pazarlara yönelik bir yönetim yapısını içermektedir. Buna ek olarak, kriptografi hesaptaki işlem bilgisini şifrelemek için kullanılabilir, böylece yalnızca belirli katılımcılar her işlemin ayrıntılarını çözebilir. Bu amaçla kullanılan şifreleme, gizlilik gerektiren durumlarda önemli bir araç olabilir (Mills vd. 2016: 6-13).

Blok zincirinin fonksiyonlarını tıpkı paranın fonksiyonlarında olduğu gibi kesin bir şekilde belirlemek zor olmakla birlikte farklı kullanım alanlarına göre değişik fonksiyonları öne çıkmaktadır. Genel olarak, blok zinciri hizmetleri üç temel bileşenden oluşmaktadır (Hyperledger Whitepaper, 2016):

- *Eşler Arası Protokolü (P2P Protocol)*
- *Dağıtık Kayıt Teknolojisi (DLT)*
- *Mutabakat Birliği (Fikir Birliği) Protokolü (Consensus Protocol)*

Şimdi bu temel bileşenler hakkında kısaca bilgi vermek yerinde olacaktır.

2.3.1. Blok Zinciri Eşler Arası Protokolü

Blok zinciri, kullanıcıların içerisindeki bilgilere bakabildiği bir dijital kayıttır ve herkese açık olması mümkündür. Açık blok zincirlerinde kayıtlardan kullanıcı taraflar sorumlu değildir, isteyen herkes kullanabilmektedir. Bir kişi ya da kuruluş tarafından değil, dağıtık bir ağda dünyanın farklı yerlerinde bulunan binlerce işlemci tarafından tutulabilecek bir yapıya sahiptir.

Blok zinciri teknolojisi, güvene dayalı eşler arası işlemlere ilişkin merkezi olmayan model olarak en temel seviyede aracı bulunmayan işlemleri ifade etmektedir.

Bununla birlikte her çeşit etkileşim ve işlem için küresel bazda ademi merkeziyetçi ve güvenilmeyen işlemlerde, geçiş imkanı sağlamaktadır (insandan-insana, insandan-makineye, makineden-makineye). Henüz öngörülemeyen ancak mevcut kurulu güç ilişkileri ve hiyerarşilerinin kullanımını etkileyebilecek, toplumun kolayca fayda sağlayabileceği farklı bir işleyiş ve yapının kullanılmasını mümkün kılabilmektedir (Swan, 2015: 7). Blok zinciri yapısı, katılımcılara her işlem gerçekleştiğinde eşler arası çoğaltma yoluyla güncellenen kayıtları paylaşma olanağı sunmaktadır. Eşler arası bildirim, ağdaki her katılımcının (düğümün) bir yayıncı ve bir abone gibi davranması anlamına gelmektedir. Her düğüm, diğer düğümlere işlemler gönderebilir veya alabilir. Veriler, aktarıldığı andan itibaren ağ üzerinden senkronize edilmektedir (Gupta, 2017: 6).

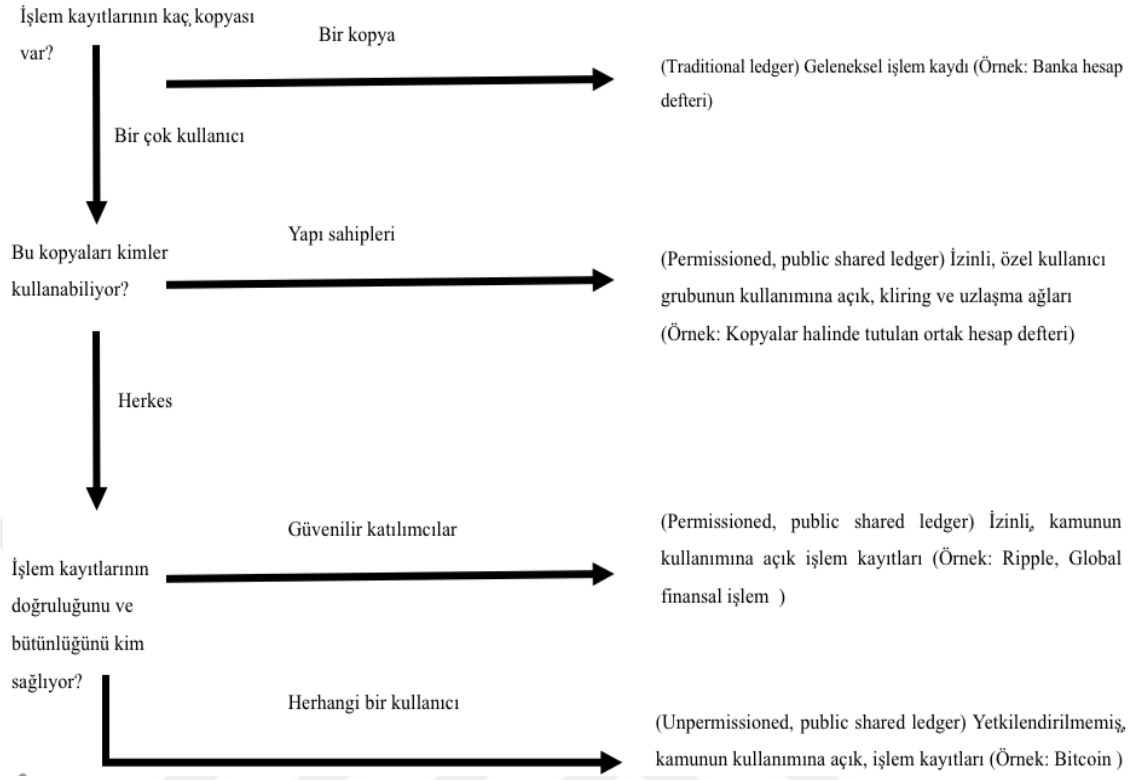
2.3.2. Blok Zinciri Dağıtık Kayıt Teknolojisi

Blok zinciri, en tanınmış şekli ile elektronik ödemelerde dağıtık kayıt teknolojisinde kullanılmaktadır. Bununla birlikte tüm dağıtık kayıt teknolojisi uygulamaları blok zinciri teknolojisini kullanmak zorunda değildir. Dağıtık kayıt teknolojisi için blok zinciri birçok veri yapısından yalnızca bir tanesidir.

Dağıtık kayıt teknolojisi, üç kilit özelliği uygulayarak blok zinciri işlemlerini yönetmektedir (Hyperledger Whitepaper, 2016);

- Her bir veri kümesinin, verimli bir şekilde her bir bloktan sonra şifreli işlem özetini hesaplamaktadır.
- Bir eşin senkronize olmadığı ve yakalaması gereken veri kümesine minimal düzeyde bir delta değişikliğini etkili bir şekilde iletmektedir.
- Her bir katılımcı, dağıtık kayıt teknolojisinin çalışması için gereken depolanmış veri miktarını en aza indirgemektedir.

Birleşik Krallık Hükümeti Baş Bilim Danışmanı tarafından hazırlanan "Dağıtık Kayıt Teknolojisi: Blok Zincirinin Ötesinde" raporunda yer verilen dağıtık işlem kayıtları sınıflandırmasının nasıl olabileceği Şekil 2.2'de gösterilmiştir.



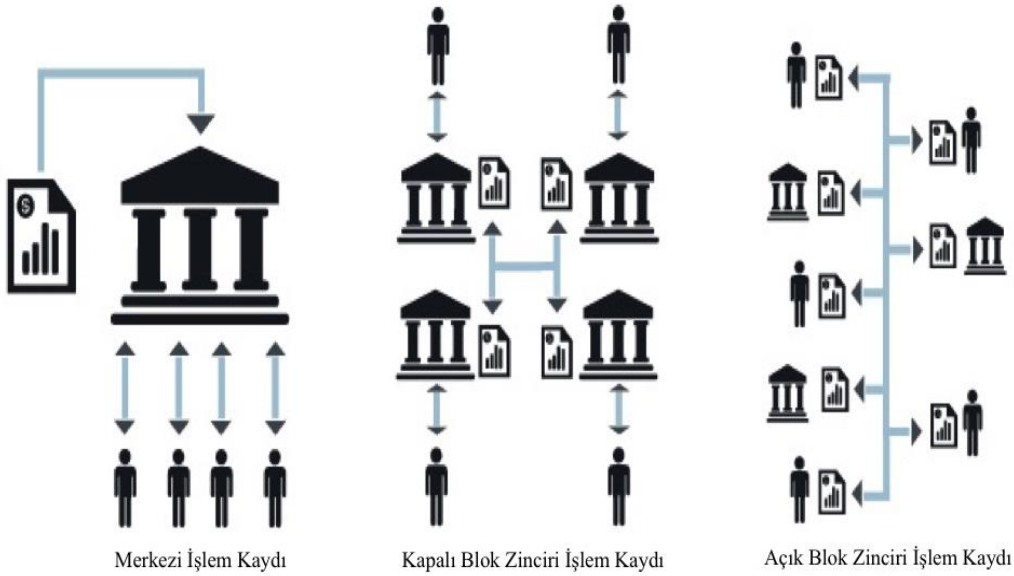
Şekil 2.2. Dağıtık İşlem Kayıtları Sınıflandırması

Kaynak: GOS (2015: 19)

Raporda tıpkı blok zincirinin kripto para birimlerinin ötesinde kullanım olanakları sağladığı gibi, dağıtık kayıt teknolojisinin de blok zincirinin ötesinde kullanım olanaklarının ekonomik faydalarını açığa çıkarmak, tanıtmak istenilmiştir. Özetle, dağıtık kayıt teknolojisi, hükümetin dolandırıcılık, yolsuzluk, hata ve kağıt yoğun süreçlerinin maliyetini azaltma olanağı sağlamaktadır. Bilgi paylaşımı, şeffaflık ve güven açısından hükümet ve vatandaş arasındaki ilişkiyi yeniden düzenleme potansiyeline sahiptir. Özel sektör için de benzer imkanlar sunmaktadır Adından da anlaşılacağı gibi son derece yaygın biçimde tam kontrollü bir şekilde dağıtılırlar. Bunun için, hükümetin teknolojiyi uygulamak üzere uzman bir kullanıcı olarak hareket etmesi ve uygulanabilir olduğu yerde dağıtılmış kayıt çözümleri tedarik etmesi gerekmektedir. Dağınık kayıt uygulanmasının kullananımı için, uyumluluk, maliyet etkinliği ve hesap verebilirlik açısından önemli gelişmelere yol açması gerektiği kanısına varılmıştır.

Bir dağıtık kayıt teknolojisi düzenlemesinin açık ya da kapalı olmasına bakılmaksızın, katılımcılar (dolayısıyla bulundukları düğümler) izin verilen roller ya da gerçekleştirmelerine izin verilen işlevler ile farklılıklar gösterebilmektedir.

Katılımcıların tüm faaliyetleri gerçekleştirmesine izin verilen dağıtık kayıt teknolojileri düzenlemelerine genellikle, izinsiz dağıtık kayıt denilmektedir. Katılımcıların faaliyetlerini kısıtlayanların çoğu, izinli dağıtık kayıt olarak anılmaktadır. Örneğin, bazı dağıtık kayıt teknolojisi düzenlemeleri, bazı katılımcılara mevcut varlıkları için varlık transferleri gönderen ve alan düğümlere sahip olmalarına izin verilmektedir. Diğer katılımcılar ise hem transfer, hem de yeni varlıkları çıkarma ve piyasaya sürme hakkına sahip olabilmektedirler. Belirtilen yetkilere ek olarak işlemlerin geçerliliğini onaylama iznine de sahip olabilmektedir. Bazı katılımcıların yetkisi yalnızca defteri / kayıtları okumakla sınırlı olabilirken, bazılarına da dağıtık kayıt sistemine yazmaya izin verilebilmektedir. Bitcoin gibi kripto para birimleri dağıtık kayıt teknolojisinin düzenlenmesi açısından izinsiz bir sistem örneğidir. Bununla birlikte, mevcut finans sektörü izinli sistemler geliştirmek üzerine odaklanmıştır. Çünkü izinli sistemler, düzenlemede yapılan önemli işlevler üzerinde kontrol imkanı sunmaktadır (Mills, vd. 2016: 12). Dağıtık işlem kayıtlarının ve blok zincirinin Şekil 2.1'de gösterilen ağ yapılarında, elektronik ödemeler alanında nasıl hayat bulduğu ise Şekil 2.3'te gösterilmeye çalışılmıştır.



Şekil 2.3. Merkezi İşlem Kayıtları, Kapalı ve Açık Blok Zinciri İşlem Kayıtları
Kaynak: lankabusinessonline.com (2016)

Merkezi işlem kayıtlarında güven, mutabakat, doğrulama gibi fonksiyonel ve sistemsel konular merkezi yapılar aracılığıyla sağlanmaktadır. Kapalı veya özel blok zinciri uygulamaları işlemler için yetkilendirme gerektiren genelde izinli, yetkilendirilmiş ve düzenlemelere tabi yapılardır. Açık blok zinciri uygulamalarında blok zinciri ile ilgilenen her kullanıcı tarafından her kayıt görüntülenebilir ve protokol koşullarına uygun işlemler kullanıcılar tarafından gerçekleştirilebilmektedir. Merkezi işlem kayıtlarında bütün bilgiler ve işlemler merkez onayı ile doğrulanarak gerçekleştirilebilmektedir.

2.3.2.1. Açık Blok Zinciri

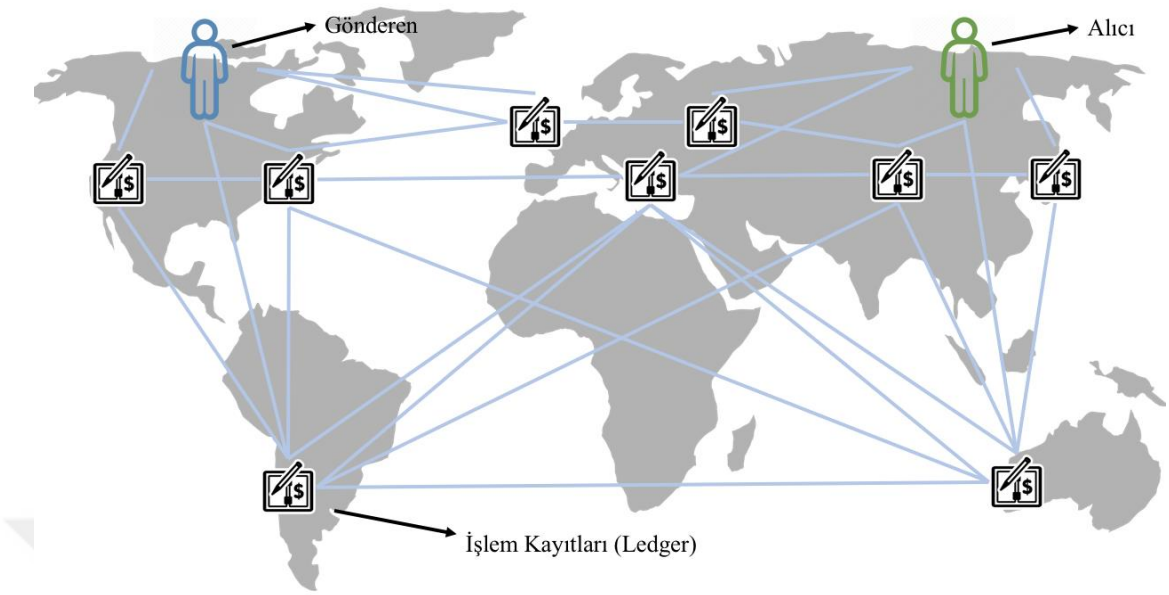
Başka bir makam tarafından herhangi bir izne gerek olmaksızın herkesin veri yazabildiği ve okuyabildiği sistemlere açık blok zinciri denilmektedir. Genellikle kamunun kullanımına açık blok zincirinden bahsedilirken herkesin yazabileceği ve okuyabileceği bir sistem olduğu varsayılmaktadır.

Tüm katılımcılar, açık blok zincirlerinde esasen aynı haklara sahiptirler. Bu durum herkesin blok zincirinin içeriğini görüntüleyebileceği, işlem yapabileceği ve blok zincirinin güvenliği ve bütünlüğüne katkıda bulunabileceği anlamına gelmektedir. Bu yaklaşımın muhtemel avantajları ise şunlardır:

- *Yüksek güvenlik düzeyine sahip olması,*
- *Düşük maliyetli olması,*
- *Potansiyel bireysel hataların önüne geçilmesidir.*

Ancak katılımcılar matematiksel bir algoritmaya tamamen güvenmek durumundadır (bafin.de, 2017).

Dağıtık kayıt teknolojisi olan blok zinciri kullanımı ile merkezi ödeme sistemleri arasındaki fark, Şekil 2.4 ve Şekil 2.5'de anlatılmaya çalışılmıştır.



Şekil 2.4. Örnek Bir Dağıtık Kayıt Teknolojisi Gösterimi

Kaynak: IMF (2016: 20)

Şekil 2.4'e göre, dağıtık kayıt teknolojisinin kullanıldığı açık blok zinciri sistemlerinde, göndericiden alıcıya yapılan bir ödemede işlem adımları kısaca aşağıdaki gibi olacaktır.

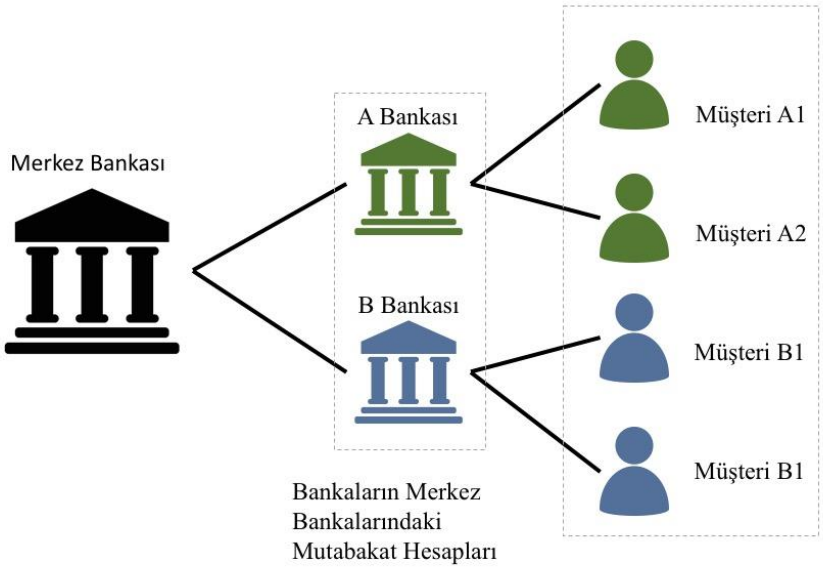
- Ağdaki birçok bilgisayarda işlem kayıtlarının (ledger) kopyaları aynı anda tutulur ve herkes tarafından görülebilmektedir.
- İşlem, çok sayıda bireysel düğüm (madenci) tarafından ağda yer alan bilgisayar kaynakları ile gerçekleştirilmektedir.
- Bitcoin örneğinde olduğu gibi, çözümü diğerlerinden daha hızlı bulan madenci, hizmetin karşılığı olarak Bitcoin elde edebilmektedir.
- Yoğun emekler sonunda güven teşkil edilir. Eğer bir madenci yanlış bir işlemi kaydetmek istiyorsa, dürüstçe davranan diğer madencilere karşı rekabet etmesi gerekmektedir.

2.3.2.2. Kapalı Blok Zinciri

Kapalı blok zinciri daha çok özel/kapalı bir blok zinciri olarak katılımcıların bilindiği, güvenildiği bir yapının geçerli olduğu, yetkisiz katılımcıların ise bilgileri okuyamadığı ve değiştiremediği bir blok zinciri sistematiğidir.

Özel blok zincirlerinde normalde bir çeşit merkezi yönetim ya da en azından yetkili katılımcılar mevcuttur. Ağa bağlı olan düğümlere, farklı haklar atanabilir ve işlemler yalnızca yetkili katılımcılar tarafından gerçekleştirilebilir. Kapalı blok zincirleri açık blok zincirlerinden bazı konularda daha avantajlı olsa da kapalı blok zincirleri uygulamalarının en çok eleştirilen yönleri, daha büyük manipülasyon riskine sahip olması ve merkezi bir yapıya olan bağımlılığıdır (bafin.de, 2017).

Açık veya kapalı blok zinciri kullanımının seçimi, avantaj ve dezavantajlarından dolayı kullanım amacına göre değişiklik göstermektedir. Merkezi veri tabanı, kapalı bir sistem yapısıdır. Blok zinciri sistemine kıyasla, merkezi veri tabanında işlem kayıtları genelde bir veri tabanı sunucusunda tutulmaktadır.



Şekil 2.5. Merkezi Ödeme Sistemi

Kaynak: IMF (2016: 20)

Şekil 2.5'te merkezi bir ödeme sisteminde ödemelerin nasıl gerçekleştirildiği görülmektedir. Örneğin A1'den B1'e yapılacak bir ödeme işlemi şu adımlardan oluşmaktadır.

- İlk olarak A1'in A Bankasındaki hesabından ödeme tutarı düşülür.
- Merkez bankası, A Bankasının tasfiye hesabından tutarı çekerek B bankasına yönlendirir.

- Merkez bankası, işlemlerin geçerliliğini doğrulayarak, çifte harcama ve dolandırıcılığa karşı koruma sağlayarak bankalar arası işlemlerin merkezi kaydını (kasa defteri) tutar.
- B bankası ise Müşteri B1'in hesabına havale tutarını geçer.
- Müşterileri için A1 ve B1 işlemlerinin kaydını A ve B bankaları tutmaktadır.

2.3.3. Blok Zinciri Mutabakat Birliği Protokolü

Mutabakat, iki ya da daha fazla taraf arasındaki fon ya da menkul kıymet aktarımından kaynaklanan yükümlülüklerin yerine getirilmesidir (TCMB, 2014: 2). Mutabakat birliği ise oybirliği, fikir birliği anlamında kullanılmaktadır.

Mutabakat mekanizmaları, dağıtık paylaşılan bir durumun güvenli bir şekilde güncellenmesine izin vermektedir ve son otuz yıldır aktif bir araştırma konusu haline gelmiştir. Dağıtık bir sistemde hata toleransını sağlamak için kullanılan ortak yöntem, paylaşılan durumu ağdaki katılımcılara dağıtmaktır. Yinelenmiş paylaşılan durumun güncellenmesi, tüm kopyalar üzerinde yürütülen *"durum makinesi"* (state machine) tarafından, önceden belirtilmiş *durum geçiş* kurallarına göre gerçekleşmektedir. Bu teknik, *durum makinesi replikasyonu*[28] olarak adlandırılmaktadır. Durum replikasyonu, bir veya daha fazla düğümün çökmesi ihtimaline karşı, durumun kaybolmamasını sağlamaktadır. Durum makinesi tüm düğümlerin aynı veriyi işlemesini sağlamaktadır. Aynı veriyi işleyen düğümler sonunda muhtemelen aynı çıktıyı üreteceklerdir. Bunun sonucu olarak mutabakat protokolü yoluyla durum değişimi konusunda nihai anlaşmaya varılması muhtemeldir. Replikalar da aynı zamanda bir fikir birliği oluşturmak ve bir durum değişikliği gerçekleştirildikten sonra durumu bütün olarak kabul etmek için birbirleriyle iletişim kurmaktadır. Blok zinciri tabanlı bir sistemde paylaşılan durum, blok zincirini oluşturmaktadır ve durum geçiş kuralları, blok zinciri protokolünün öngördüğü kurallardır. Dağıtık bir sistemde fikir birliği sağlanması zordur. Mutabakat algoritmaları, düğümlerin başarısızlıklarına, ağın bölümlenmesine, mesaj gecikmelerine, sırasız halde ulaşan mesajlara, bozuk mesajlara ve daha başka risklere karşı dayanıklı olmalıdır. Ayrıca kasten kötü amaçlı işlem gerçekleştirmeye çalışan düğümlerle mücadele etmek zorundadır. Her algoritma, senkronizasyon açısından gerekli

[28] Replika; Eşlenme.

varsayımlar dizisini oluştururken senkronizasyon, mesaj yayınları, arıza, kötü niyetli düğümler, değiş tokuş edilen mesajların güvenliği ve performansı açısından, gerekli varsayımlar dizisini oluşturmaktadır. Bir blok zinciri ağı için fikir birliği sağlanması, ağdaki tüm düğümlerin blok zincirinin tutarlı bir genel durumu kabul etmesini sağladığı anlamına gelmektedir (Baliga, 2017: 9). Başka bir ifadeyle, madencilerin çoğunluk olarak onay verdikleri işlemler fikir birliği sağlamaktadır.

Protokole bağlı olarak oluşabilecek risklerden biri çoğunluklu saldırıdır. Bitcoin örneğinde çoğunluklu saldırı, genellikle % 51 atağı ya da >% 50 atağı olarak da bilinmekte olup ağa yapılan bir saldırıyı ifade eder (bitcoin.it, 2017). Çoğunluk atağı Bitcoin ağının %50'sinden fazlasının kötü niyetli madencilerin eline geçmesi durumunda ortaya çıkan bir risk olup atağın başarılı olma ihtimali %100'e yakındır (Çarkacıoğlu, 2016: 41). Bu durumda saldırgan, ödeme işlemleri üzerinde birçok değişiklik yapabilir. Bu mutabakat riski literatürde, *"Bizans generalleri problemi"* olarak uzun zamandır bilinmektedir.

Bizans generalleri problemi ise kısaca aşağıda özetlenmiştir.

Bir grup Bizans generali aynı planı uygulamaya karar verirler. Başarılı olmak için, hepsi aynı amaçla hareket etmelidir. Ancak aralarında plana sadık kalmayan hainler olabilir. Karşılaştıkları sorun ise içlerinde bilinmeyen, sadik olmayan hain generaller ile planı başarılı olarak uygulaya bilmektir. Bu problem aslında birçok bilgisayar ağını rahatsız eden bir sorunu gözler önüne sermektedir . Bir grup nasıl davranacağına ilişkin toplu bir karar vermeye çalışırken, grup içindeki hainler tercihleri hakkında karışık mesajlar gönderebilirler. Hainler, grubun bazı üyelerine bir şey yapmak istediklerini söyleyebilir ve grubun diğer üyelerine bunun tam tersini söyleyebilir. Bu durum, grubun uygulamak istediği planı etkili bir şekilde koordine etme becerisi açısından sorunlara neden olabilir. Grubun bazı üyelerinin bir şeye inanmaya yönlendirilmesi ve diğerlerinin farklı şeyler düşünmesi halinde grup üyeleri ortak hareket etmeyi başaramayacaklardır. Sonuçta, grubun tutarlılığı ve etkililiği bozulacaktır. Bütün sadık generaller beklenen şekilde plana göre hareket etmeli ve az sayıda hain general, sadık generallerin kötü bir plan yapmasına neden olmamalıdır (Lamport, Shostak ve Pease, 1982: 383).

Dağıtık kayıtlarda güvenilmez aktörlerin isleyişe zarar verme riski mevcuttur. Bir bilgisayar ağı üzerinde işlem gerçekleştirenler bilgi alışverişi yaparken kullanılacak ortak bir ağ protokolünü kabul etmeleri gerekmektedir. Güvenilirliği sağlamak için, dağıtık kayıt teknolojileri Bizans generalleri problemi olarak bilinen bu sorunu çözecek şekilde tasarlanmalıdır. Merkezi bir düzenleyicinin olmadığı blok zinciri yapılarında bu durum daha da önem kazanmaktadır. Blok zincirini bu kadar güçlü kılan olguların başında, fikir birliğine dayalı işlemleri meşru kılma kabiliyeti gelmektedir.

Bir mutabakat protokolünün, uygulanabilirliği ve etkinliği için belirlenebilen üç temel özelliği mevcut olup aşağıda sıralanmıştır.

- *Güvenlik:* Bütün düğümlerin aynı çıktıyı üretmesi ve düğümler tarafından üretilen çıktıların protokol kurallarına göre geçerli olması durumunda, bir mutabakat protokolünün güvenli olduğu tespit edilir. Buna aynı zamanda paylaşılan durum tutarlılığı denilmektedir.
- *Canlılık:* Mutabakat protokolü, uzlaşmaya katılan tüm arızasız düğümlerin muhtemel olarak katkı sağlayacağını ve canlılığını garanti etmektedir.
- *Hata Toleransı:* Mutabakat protokolü, mutabakata katılan bir düğümün hatasından kurtarması mümkün olduğu sürece hata toleransı sağlamaktadır (Baliga, 2017: 5).

Bir düğüm, kanıtını bulduktan sonra, kanıtı blokla birlikte yayınlamaktadır. Artık diğer tüm düğümlerin, yalnızca sağlanan kanıtın doğruluğunu, doğrulamak için bir işlem özeti hesaplaması yeterlidir. Doğrulamadan sonra blok, blok zincirine dahil edilir. Diğer her düğüm artık yaptıkları işi terk edebilir (yapılan işlemi, yayınlanan bir bloğa dahil etmeye çalışmaktaydı) ve yeni işlemler yapmaya başlayabilirler (Müller ve Hasic, 2016: 10-11). Bu şekilde protokol sayesinde mutabakat sağlanabilmektedir.

Bitcoin kullanımında geçerli olan bir mutabakat protokolü en basit haliyle aşağıdaki gibi özetlenebilir.

1. Yeni işlemler tüm düğümlere yayınlanır.
2. Her düğüm, yeni işlemleri bir blok halinde toplar.
3. Her turda rasgele bir düğüm bloğunu yayınlar.

4. Yalnızca tüm işlemler geçerli olduğunda diğer düğümler, bloğu kabul eder (sarf edilmemiş, geçerli imzası olanları).
5. Düğümler, sonraki oluşturdukları bloğa işlem özetini ekleyerek bloğu kabul ettiklerini ifade eder (Narayanan vd. 2016).

2.4. Blok Zinciri Karakteristikleri

Yapılan işlemler, sözleşmeler ve bunların kayıtları ekonomik, yasal ve politik sistemlerde belirleyici yapılar arasındadır. Bu belirleyici yapılar, varlıkları korumaktadır ve örgütsel sınırları belirlemektedir ve ülkeler, kuruluşlar, topluluklar ve bireyler arasındaki etkileşimleri yönetmektedir. Genellikle bunlar, işlemi yapanların kimliklerini belirleyerek geçmiş olayları doğrulamaktadır. Ayrıca belirleyici yapılar, yönetsel ve toplumsal eylemleri yönlendirmektedir. Yine de onları yönetmek için kurulan kritik araçlar ve bürokrasiler, ekonominin dijital dönüşümüne ayak uyduramamıştır. Buna istinaden dijital dünyada, idari kontrolü düzenleyip sürdürme şeklimiz değişmek zorundadır. Bu noktada Blok zinciri bu sorunu çözmeyi vaat etmektedir. Blok zinciri, iki taraf arasındaki gerçekleşen işlemleri etkin, doğrulanabilir ve kalıcı bir şekilde kaydedebilen açık, dağıtılmış bir kayıt defteridir. Defterin kendisi de işlemleri otomatik olarak tetikleyecek şekilde programlanabilmektedir (Ianisti ve Lakhani, 2017).

Genel olarak blok zinciri teknolojisinin altında yatan ilkeler ise şunlardır;

a. Dağıtımlı Veri Tabanı: Blok zincirindeki her katılımcının, tüm veri tabanına ve geçmişine erişimi bulunmaktadır yani verileri tek taraf kontrol etmez. Her katılımcı, arada bir aracıya gerek duymadan işlem ortaklarının kayıtlarını doğrudan doğrulayabilmektedir.

b. Eşler Arası İletim: İletişim merkezi bir düğüm yerine, doğrudan katılımcılar arasında gerçekleşmektedir. Her düğüm, diğer tüm düğümlere bilgi depolamakta ve iletmektedir.

c. Kullanıcı Kimliği ile Şeffaflık: Her işlem ve onunla ilişkili sisteme erişim herkes tarafından görülebilmektedir. Bir blok zinciri üzerindeki her düğüm veya kullanıcı, onu tanımlayan 30'dan daha fazla karakterli harf ve rakamlardan oluşan bir adrese sahiptir.

Kullanıcılar, anonim olarak veya başkalarına kimliğini kanıtlamayı tercih edebilmektedir. İşlemler, blok zinciri adresleri arasında gerçekleşmektedir.

d. Kayıtların Değişmezliği: Veri tabanına bir işlem girildikten ve hesaplar da güncellendikten sonra kayıtlar değiştirilememektedir; çünkü onlardan önce gelen tüm işlem kayıtlarıyla bağlantılıdırlar ("zincir" terimi oluşumu). Veri tabanındaki kayıtların kalıcı olacak şekilde kronolojik olarak sıralanmasını ve ağdaki diğer tüm kullanıcıların kullanabilmesini sağlamak için çeşitli hesaplama algoritmaları ve yaklaşımlarını bünyesinde barındırmaktadır.

e. Sayısal Hesaplamalı Mantık: Kayıt tutmanın dijital doğası, blok zinciri işlemlerinin hesaplama mantığına bağlıdır ve bunlar özünde programlanmıştır. Dolayısıyla kullanıcılar, düğümler arasındaki işlemleri otomatik olarak başlatan algoritmalar ve kurallar oluşturabilmektedir (Ianisti ve Lakhani, 2017).

Blok zincirinde ki her düğüm aynı işlem geçmişine sahiptir. Bu nedenle, başarısızlık noktası mevcut değildir ve kesinti zamanlarını ortadan kaldırmaktadır. İşlem kayıtları ardışık olarak bloklar halinde saklanmaktadır. Saklanan işlem kayıtlarının ardışık blokları yine ardışık olarak mevcut blok zincirine eklenmektedir. Bu nedenle, sahtekârlık yapmak son derece zordur. Blok zinciri tabanlı sistemler, dağıtık yapısı ve mutabakat protokolü gibi teknoloji unsurlarını bir araya getirerek, benzer güvenlik düzeyindeki mevcut sistemlere göre daha düşük maliyetlerle geliştirilebilmektedir (METI, 2017: 1-3).

2.5. Herşey İçin Blok Zinciri Kullanımı

Blok zinciri ekonomisi birçok yeni fikri tetiklemekle beraber, mevcut kavramların ve terminolojinin yenilikçi şekillerde yeniden kullanılmalarını sağlamaktadır. Yıllarca tartışmasız kabul edilen para, para birimi, mülkiyet, hükümet, egemenlik ve fikri mülkiyet gibi kullanılan terimlerin tanımlarının araştırılmasına yönlendirmektedir. Bahsi geçen tanımların sorgulanması, terimlerin yeniden ele alınması, bu kavramların mevcut durumlara uygulanması için daha açık ve erişilebilir bir konuma getirilmesini sağlayacaktır. Blok zinciri ile ilgili kavramlar insanların zihinlerinde daha aktiftir ve genel bir seviyede uygulamaya hazırdır. Blok zincir teknolojisi gibi yeni modeller,

gerçeği belirli bir örneklemenin arkasındaki kavramların daha genel seviyesinde değerlendirmeye itmektedir. Bu kavramlarla gerçekleştirilebilecek diğer belirli durumları hayal etmemizi sağlamaktadır. Örneğin, blok zinciri ademi merkeziyetçilik için kullanılan bir teknolojidir. Bitcoin, merkezsizleşmeyi dijital para birimi olarak somutlaştırmaktır, ademi merkezi sistemler, akıllı sözleşmeler[29] gibi birçok açıdan örneklenebilmektedir (Swan, 2015: 69). Blok zinciri tabanlı ödeme uygulamaları, elektronik ödemelerin überizasyonu[30] olarak görülebilir.

Konvansiyonel sistemlere kıyasla blok zinciri teknolojisinde, sahtecilik yapmak son derece zordur ve devre dışı kalma süresini ortadan kaldıran ucuz sistemler inşa edilebilmesi kritik özelliklerinden biridir. Bu nedenle çok çeşitli alanlarda teknolojinin uygulanması beklenmektedir. Bununla birlikte, teknolojinin özelliklerini yeterince değerlendirmek ve mevcut sistemlerle karşılaştırmak amacıyla kıyaslama endekslerine veya ölçütlerine gerek vardır. Aksi halde insanlarda kaygı, yanlış anlaşılma, makul olmayan umutlara, teknolojileri engellemesine ve teknolojiyi tanıtmak için potansiyel bir isteksizliğe neden olabilmektedir (METI, 2017: 1-3). Çok disiplinli yapısı nedeniyle çıkarıcılar, kullanıcılar ve otoriteler arasında kuvvetli işbirlikleri gerektirmektedir.

[29] Akıllı sözleşme; bilgisayar kodu ile programlanabilir bir protokoldür. Bu özelliği ile akıllı sözleşmeler birçok fonksiyon edinebilmektedir.
[30] Überizasyon; (Uberization) bir ekonomik modeli veya piyasayı değiştiren etkili bir alternatifin (genelde eşten eşe çalışan) gelişimi anlamında kullanılmaktadır.

ÜÇÜNCÜ BÖLÜM

FİNANSTA BLOK ZİNCİRİ UYGULAMALARI

Artan uluslararası rekabet ve hızlı bir şekilde gelişmeye devam eden ticaret teknolojileri karsısında, finansal yeniliklerin ve risk yönetim tekniklerinin artan bir şekilde kullanılmasını gerektirmektedir. Finansal yenilikler, gelişmelere ayak uyduramayan finansal kurumlar, piyasaları düzenlemek ve denetlemekle yükümlü olan devlet kurumları için de bazı zorluklara neden olmaktadır (Akel, 2006: 56). Bankalar arasındaki ödemeler ve kayıtlar arasındaki işlemler, mutabakat gerektirmektedir. Genellikle bir hesaptan başka bir hesaba aktarım yapmak için bir dizi banka hesabı gerekmektedir. Bu işlemler, bağımlılıklara, günlerce süren işlem sürelerine, yüksek maliyetlere ve operasyonel risklerin dogmasına sebep olmaktadır. Sermaye piyasaları ve yatırım bankacılığı işlemleri, sözleşme hakları, yükümlülükler ve ödeme akışlarının sağlanması olarak tanımlanmaktadır. Bu temelde, merkezi olmayan bir kayıt sistemi riskleri azaltabilir, önemli maliyet ve sermaye tasarrufu sağlayabilmektedir (McKinsey, 2015: 8).

Paranın fonksiyonları ağ etkisi ile ilişkilidir. Kısaca ağ etkisi, iktisadi açıdan ürün ya da hizmetin faydasının, her bir katılımcı ile birlikte daha da artması olarak tanımlanabilir. Ağ etkisinin ekonomik prensibi bilgi teknolojilerini, belki diğer tüm faktörlerden daha fazla etkilemektedir. Ağ teknolojisinin çok güçlü etkileri nedeniyle ağ etkisi oldukça değerli olabilir. Popüler ve ikna edici örnek olarak telefon ağı örneği gösterilebilir. Telefon ile haberleşmenin değeri, güçlü bir şekilde telefon kullanan diğer kişilerin sayısına bağlıdır. Telefon kullanıcılarının sayısının artması ile birlikte, telefon ile haberleşmeden kaynaklanan fayda da artmaktadır. Yenilikçi teknolojiler bu örneği büyük ölçüde genişletmektedir. Belirli bir ağdaki katılımcılar, her yeni ağ katılımcısından yarar sağlar ve her yeni katılımcı ile birlikte ağın değeri artar. Ağ

etkilerinin değerli olmasının bir başka nedeni ise inşa edildikten sonra kendisini kalıcı bir hale getirme eğiliminde olmasıdır.

Blok zinciri ve dağıtık kayıt teknolojisi gibi yenilikler sanal para birimi ötesinde bir önem taşımaktadır. Blok zinciri, birbirlerine karşı hiçbir güveni olmayan kişilerin tarafsız bir merkezi otoriteye gitmek zorunda kalmadan işbirliği yapmalarını sağlayan ve bilinenin çok ötesinde güçlü bir yapıya sahip bir teknolojidir. Sistemin özünde, herkesin denetleyebileceği, paylaşılan, güvenilir bir kayıt defteri oluşturma mantığı yatmaktadır. Bir blok zinciri sistemindeki katılımcılar topluca kayıtları güncel tutmaktadırlar. Blok zinciri kullanıcıları, sıkı kurallar ve genel anlaşma çerçevesinde işlemleri gerçekleştirmektedir. Bitcoin'in blok asıllı kaydı, çifte harcamayı önlemektedir ve işlemlerin sürekli olarak takip edilmesini sağlamaktadır. İşte bu işlem yapısı, merkezi bir otoriteye olan ihtiyacı ortadan kaldırmaktadır (The Economist, 2015). İşlemlerin dağıtık bir yapıda gerçekleştirilebilmesini sağlamaktadır.

Blok zinciri sistematiği, kriptografinin beklenmedik bir meyvesi olarak değerlendirilmektedir (The Economist, 2015). Dağıtık kayıt teknolojisine dayalı sanal para birimleri ve teknolojisi yaygın olarak kullanılmasa da başta bankalar olmak üzere, finansal sistemdeki mevcut aktörlerin aracılık rolüne meydan okuyabilecek güçlü temellere sahip bir sistemdir. Bankalar, mevduat sahipleri adına borç alanların gözetim altında tutulmasında görev yapan finansal aracılardır. Ayrıca bankalar, mevduat sahiplerinden borç alanlara para akışında genellikle likidite ve vade dönüşümünü gerçekleştirmektedirler. Dijital para birimleri ve dağıtılmış defterler yaygınlaştıkça meydana gelecek herhangi bir arabuluculuk, tasarruf veya kredi mekanizmaları üzerinde etkili olabilecektir. Ekonomideki bu planların kullanılmasına dayanan geleneksel finansal aracı rollerini kimin üstleneceği veya bu hizmetlerin böyle bir bağlamda sunulup sunulamayacağı belirsizdir (BIS, 2015: 3). İlerleyen dönemde bu alandaki belirsizliklerin ortadan kalkmasıyla birlikte piyasalar yeniden şekillenecektir.

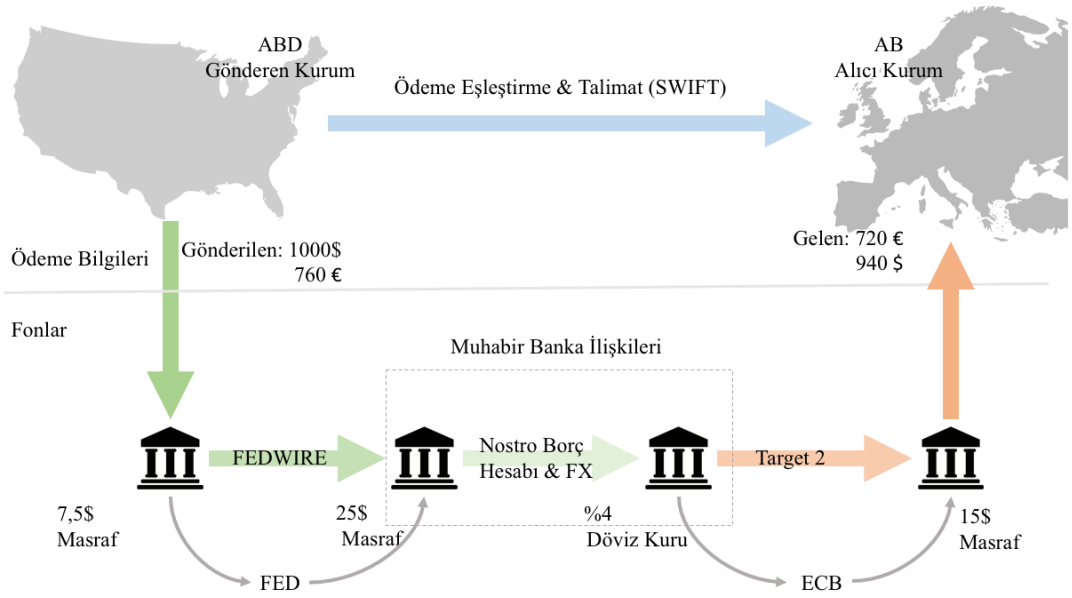
3.1. Blok Zinciri 1.0

İlk blok zincir uygulaması, ödemeleri gönderen ile alıcı arasında merkezi bir karşı taraf olmaksızın yürütüldüğü bir şifreleme sistemi sonucu oluşmuştur. Bu sistemin zamanla

yaşanan gelişimini takip etmek, finans alanındaki potansiyel faydasını daha iyi anlamak için faydalı olacaktır.

Blok zinciri internet için şimdiden tıpkı nakit para gibi olup dijital bir ödeme sistemidir. Nesnelerin internetinin (IoT, Internet of Things) makineleri birbirine bağladığı gibi finansal ekonomiyi bir birine bağlayabilecek yapıdadır. Para birimi ve ödemeler, bu alanda ilk ve en belirgin uygulamayı oluşturmaktadır. Dahası kullanıcılar, günlerce transfer beklemek yerine derhal (neredeyse gerçek zamanlı) dijital cüzdanlarla para alabilmektedir. Blok zinciri tabanlı para birimlerinin temel işlevselliği, iki kişi arasındaki transfer işlemini internet üzerinden doğrudan sağlayarak gerçekleştirebilmesidir. Bu fonksiyonları ile kripto para, tüm kaynakların dağıtık yapıda ticareti için, para birimi özelliği ve ödemelerin çok ötesinde, programlanabilir bir açık ağ oluşturabilmektedir. Böylece, programlanabilir para olarak Bitcoin'in daha güçlü işlevselliğinden yararlanmak için, para ve ödemeler için Blok zinciri 1.0 zaten Blok zinciri 2.0'a genişlemektedir (Swan, 2016: 5). Blok zinciri tabanlı uygulamalar durdurulamamakta, sansürlenememekte veya kontrol edilememekte olup etkileşimde yer alan tüm taraflar arasında şeffaflık ve güven sağlamaktadır (Müller ve Hasic, 2017: 14).

Kripto odaklı bilgisayar bilimleri yenilikleri sadece kripto para birimlerinden ibaret olmayan ve para birimleri ötesine geçen kavramları da içermektedir. Kripto paralar, programlanabilir paralardır, ancak blok zinciri de programlanabilir değerler, programlanabilir yönetişim, programlanabilir sözleşmeler, programlanabilir mülkiyetler, programlanabilir güvenlik uygulamaları, programlanabilir varlıklar vb. birçok sistem için kullanılabilmektedir (Mougayar, 2015). Elektronik ödemelerde blok zinciri teknolojisi, EFT ya da yurtiçi ödeme ve mutabakat sistemleri gibi işlemleri gerçekleştirebilecek kapasiteye sahip bir sistem olarak kullanılabilir. Uluslararası boyutta ise Şekil 3.1'deki anlatımdan da anlaşılacağı üzere karmaşık aşamaları azaltacaktır. Blok zinciri tabanlı kripto para birimlerinin halihazırdaki sınır tanımayan kullanımlarında olduğu gibi, uluslararası para transferleri işlemleri farklı boyutlara taşınabilir. Blok zinciri sistematiğinin kullanımıyla daha hızlı, daha düşük maliyetli ve etkin işleyen bir transfer işlemi gerçekleştirmek mümkün olmaktadır.



Şekil 3.1. Uluslararası Para Transferinin İzlediği Yol[31]

Kaynak: Ripple (2014: 7)

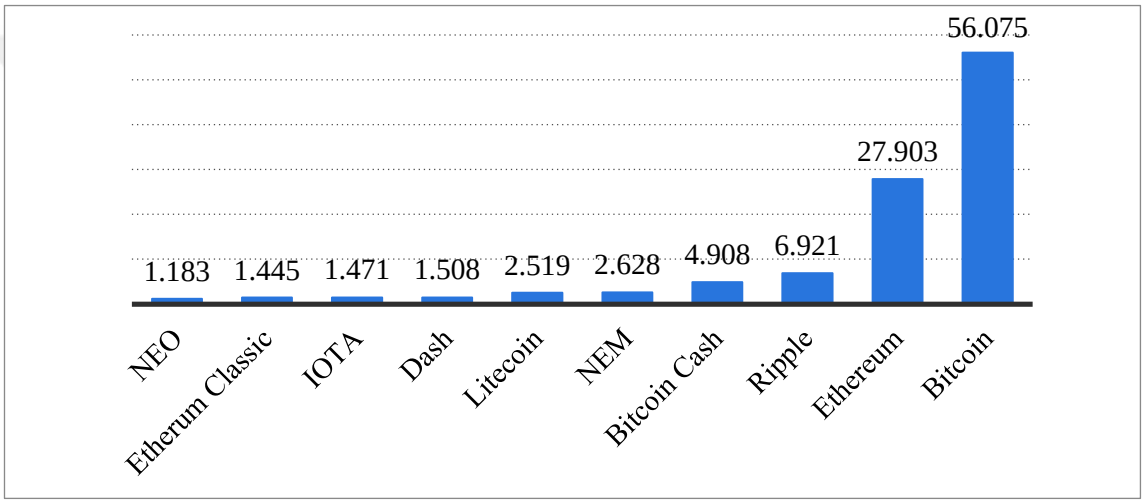
Bankanın en önemli işlevlerinden biri yurtiçi, yurtdışı fon transferidir ve tüm dünya çapındaki bankalar tarafından uygulanmaktadır. Ortak kurallar ve standartlaştırılmış düzenlemelerle üyeler arasında doğan para yükümlülüklerinin iletimi gerçekleştirilmektedir. Ancak işlem süresi ve masrafları gerekli yasal düzenlemeler dolayısıyla oldukça artmaktadır.

Nihai alıcıya para göndermenin ortalama maliyeti, aktarılan tutarın % 7.68'i oranındadır. Banka olmayan aracı kurumlarda ise bu oran %10'u geçmektedir (WEF, 2015: 24). Uluslararası işlemlerde bankaların, nostro / vostro hesaplarını yönetmenin daha etkin olması gerekmektedir. Nostro (bizimki), yerli bir bankanın yabancı bir bankada yabancı ülkenin para birimi cinsinden tuttuğu bir hesaba karşılık gelmektedir. Vostro (sizinki) ise yabancı bankanın bu hesaba nasıl yönlendirdiğidir. Bu hesaplar, ticaret ve döviz işlemlerini mutabakat yoluyla kolaylaştırmak ve ayrıca basitleştirmek için kullanılmaktadır. Blok zinciri ile Nostro / Vostro hesapların otomatik olarak mutabakat yoluyla şeffaf ve önemli ölçüde etkin olarak kullanılabilmesi sağlanabilmektedir.

[31] Fedwire; Amerika Birleşik Devletleri Gerçek Zamanlı Mutabakat Sistemi (RTGS, Real Time Gross Settlement System). Nostro veya Vostro hesabı; bir bankanın yabancı bir muhabir bankada uluslararası ödemelerini yapmak için bulundurduğu döviz hesabı anlamına gelmektedir. Target2; Eurosystem (RTGS) Gerçek Zamanlı Mutabakat Sistemi.

Tek bir ara yüz aracılığıyla tüm bankanın, Nostro/Vostro hesaplarındaki işlemleri yönetme olanağı sağlamaktadır. İşlem durumunun, mevcut dengesinin ve zaman içindeki takibinin daha fazla görünürlüğü mümkündür. Tüm Nostro/Vostro hesaplar hakkında tutarlı, zamanında ve doğru bir resim oluşturmaktadır (Gupta, 2017: 26).

Elektronik ödemeler alanında kripto para birimleri oldukça yaygın olarak kullanılmaktadır. Grafik 3.1'de kripto paraların kullanımı ile doğru orantılı olan piyasa değerleri gösterilmiştir. Kripto para birimlerinin piyasa değerleri, sürekli olarak değişiklik göstermektedir.



Grafik 3.1. En Büyük Sanal Para Birimlerinin Piyasa Değerleri
(10.08.2017 İtibariyle, Milyon Dolar)

Kaynak: statista.com (2017) ve coinmarketcap.com (2017)

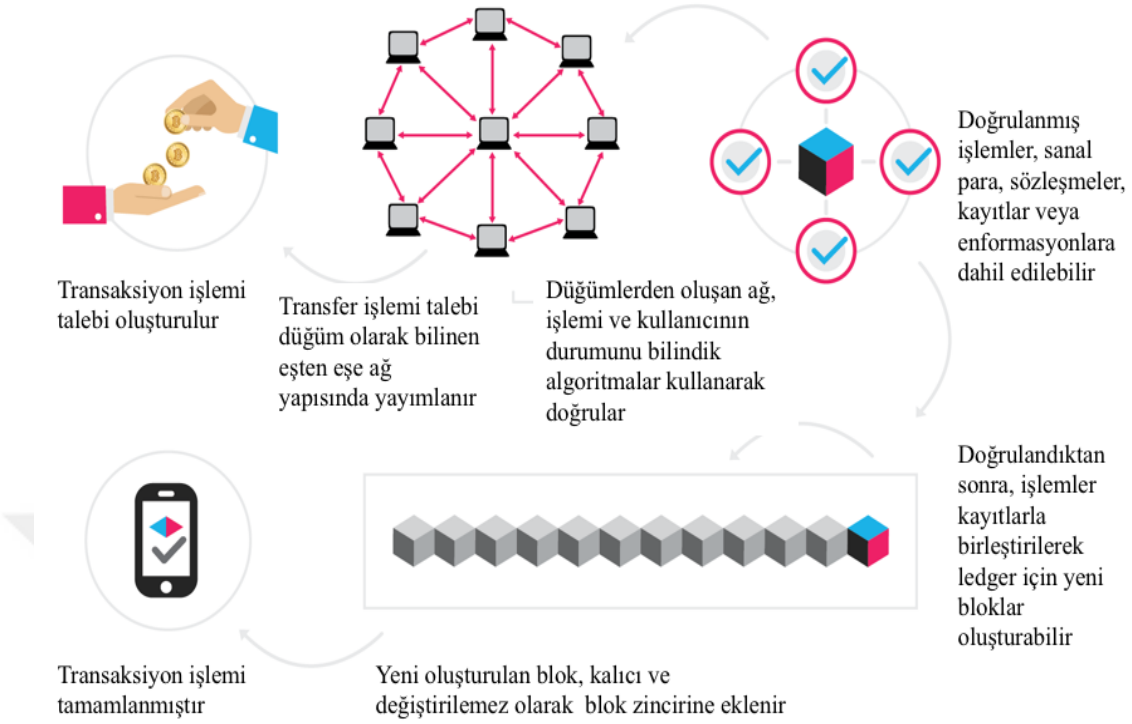
Toplam sanal para birimleri yaklaşık 150 Milyar dolarlık piyasa değerine sahiptir (coinmarketcap.com, 2017). Ağustos 2017'deki piyasa değerine göre en büyük sanal para birimlerinin sıralamasına göre, en büyük pazar payına Bitcoin sahiptir. İkinci sırada ise Ethereum yer almaktadır. Bitcoin ve Ethereum'dan sonraki sıralamada yer alan para birimleri ise sürekli değişiklik gösterebilmektedir.

3.1.1 Bitcoin Uygulaması

Tamamen eşten-eşe çalışan bir elektronik para sistemi olarak herhangi bir finansal kurumdan geçmeden, bir taraftan diğerine çevrimiçi ödeme gönderilmesini mümkün kılmaktadır. Dijital imzalar bu anlamda çözümün bir parçasıdır, ancak mükerrer harcamaları önlemek için hala güvenilir bir üçüncü tarafa ihtiyaç duyulmasıyla temel faydalarını kaybetmektedir. Bitcoin ile mükerrer harcama problemine eşler arası ağ kullanarak bir çözüm önerilmiştir (Nakamoto, 2008: 1).

Bitcoin, bilindik para birimleri gibi sabit birimlerden oluşmamaktadır, BTC (Bitcoin) olarak kısaltılmaktadır. Bitcoinler yalnızca işlem çıktılarıdır ve kurallar dahilinde ondalık olarak istenilen birçok değere sahip olabilmektedir. Toplam Bitcoin sayısı 21.000.000 ile sınırlıdır ve olası en küçük değeri 0.00000001 BTC, 1 Satoshi olarak adlandırılmaktadır. Eşler arası olan Bitcoin ağının amacı, bütün yeni hareketleri ve oluşturulan blokları, mevcut bulunan tüm Bitcoin esler arası düğümlere yaymaktır. Sistemin güvenliği, eşler arası ağın eksiksiz bir yapı oluşturma çabasından değil blok zincirinden ve mutabakat birliğinden kaynaklanmaktadır (Narayanan vd. 2015).

Günümüzde internet üzerinden alışveriş, neredeyse bugün tamamen güvenilir bir üçüncü taraf olarak elektronik ödemeleri gerçekleştiren sistem olarak işleyen finansal kurumlara bağımlı hale gelmiştir. Birçok işlem için bu sistem oldukça iyi çalışıyor olsa da hala güvene dayalı bir model olmanın zayıflığını barındırmaktadır. Finansal kurumlar, ihtilaflarda arabuluculuktan kaçamadıklarından dolayı tamamen geri dönüşü olmayan işlemler gerçekte mümkün değildir. Arabuluculuk hizmeti giderleri, işlem giderlerini yükseltir ve mümkün olan en küçük işlem miktarını sınırladığı için küçük ödeme işlemlerini engellemektedir. Geri döndürme ihtimali ile birlikte işlemlerde tarafların güven ihtiyacı da artmaktadır (Nakamoto, 2008: 1). Elektronik ödemelerde genel olarak blok zincirinin nasıl kullanıldığını anlatmak üzere, Şekil 3.2'de elektronik ödemelerde blok zinciri isleyiş yapısı gösterilmiştir.



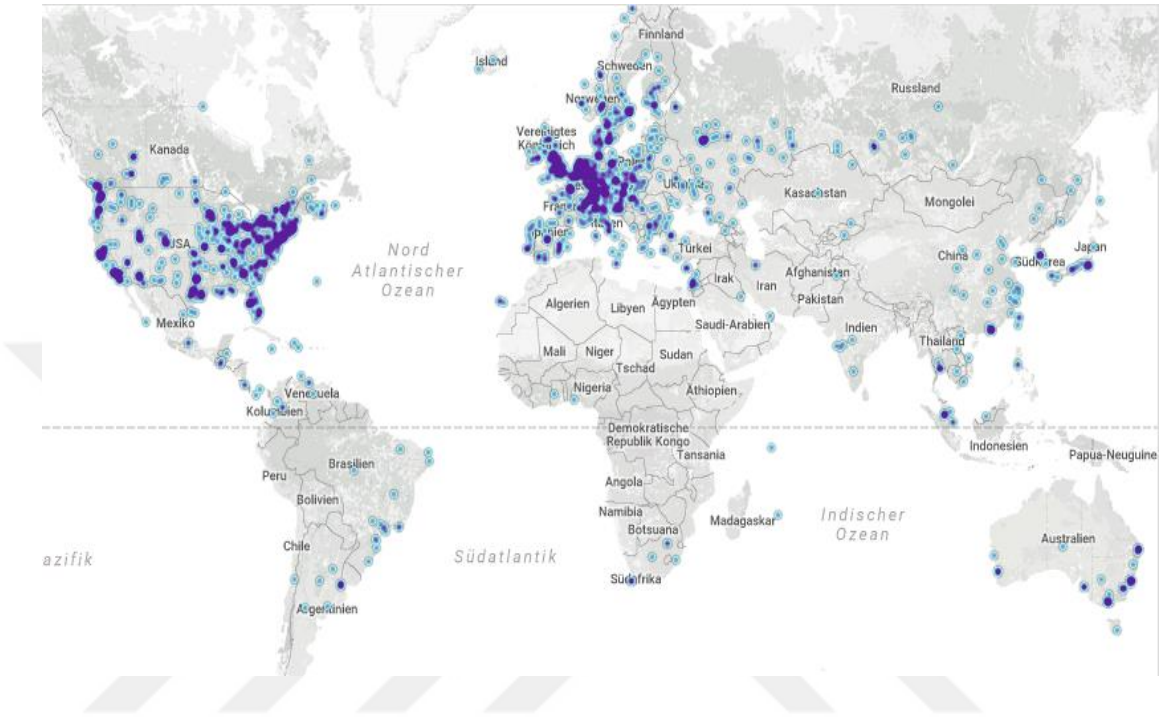
Şekil 3.2. Elektronik Ödemelerde Blok Zinciri İsleyiş Yapısı

Kaynak: blockgeeks.com (2015)

Yeni bir kullanıcı olarak teknik ayrıntıları anlamadan da elektronik ödemelerde blok zinciri kullanmaya başlanabilmektedir. Örneğin, bilgisayara veya cep telefonuna bir Bitcoin cüzdanı kurduktan sonra, ilk Bitcoin adresi üretilebilir ve ihtiyaç duyulduğunda daha fazla cüzdan oluşturabilir. Oluşturulan adresi ilgili taraflara bildirebilir, böylece taraflar ödeme yapabilir ya da istenilen adrese ödeme yapılabilir. Aslında bu durum e-postanın isleyişi ile oldukça benzerdir. Blok zinciri, tüm Bitcoin ağının dayandığı paylaşılan bir kayıt defterdir. Tüm onaylanmış işlemler blok zincirine dahil olmaktadır. Bu şekilde Bitcoin cüzdanı harcanabilir bakiyeyi hesaplayabilir ve kullanıcıya ait yeni işlemleri onaylanabilir. Blok zincirinin bütünlüğü ve kronolojik sıra yapısı, kriptoloji ile desteklenmektedir. Bu işlemler ağa her yerden katılabilen düğümler tarafından yapılabilmektedir.

Bitcoin blok zinciri ağı ile günde yaklaşık 250.000 transaksiyon gerçekleştirilmektedir, 2016 yılında yılında ise toplamda 80 Milyondan fazla transaksiyon işlemi gerçekleştirilmiştir (blockchain.info, 2017). Dünyanın en büyük perakende ödeme ağı olan Visa Inc. 2016 yılında 3.1 Milyar kart ile 141 milyar transaksiyon işlemi

gerçekleştirmiştir (Visa Inc, 2017: 2). Bitcoin blok zinciri ağında işlemler, madenciler tarafından doğrulanarak gerçekleştirilmektedir. 2017 yılı ortalarındaki Bitcoin madencilik boyutuna ilişkin bilgi, Şekil 3.3'de sunulmuştur.



Sıralama / Ülke • Düğüm Sayısı • Yüzde	1. A.B.D. • 2.227 • % 28,65	2. Almanya • 1.507 • % 19,39	3. Fransa • 535 • % 6,88	4. Hollanda • 459 • % 5,79	5. Kanada • 303 • % 3,90
	6. İngiltere • 291 • % 3,74	7. Bilinmeyen • 262 • % 3,37	8. Rusya • 236 • % 3,04	9. Çin • 234 • % 3,01	10. Singapur • 130 • % 1,67

Şekil 3.3. Küresel Bitcoin Düğüm Dağılımı

Kaynak: bitnodes.21.co (2017)

Ağ yapısı üzerindeki düğümler, dağıtık kayıt teknolojisi işlemlerini tutan veya gerçekleştiren, erişilebilen madencileri yaklaşık olarak sembolize etmektedir. Bitnodes, bir Bitcoin protokolü olan sürüm 70001'i kullanmaktadır[32]. Bu nedenle eski bir protokol sürümünü işleten düğümler hesaba katılmamaktadır (bitnodes.21.co, 2017).

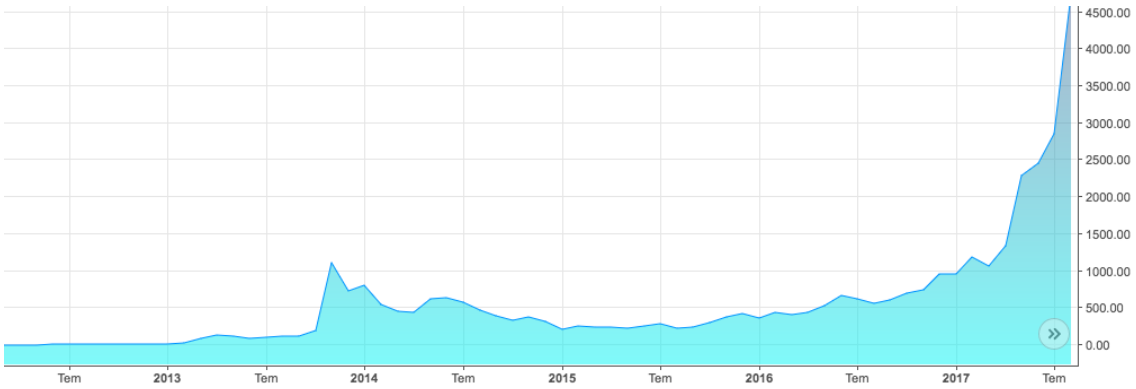
[32] Hesaba dahil sürümler >=/Satoshi:0.8.x/

Bitcoin'ler nakit para karşılığında ATM'lerden takas edilebilmektedirler. Eylül 2017 itibariyle 58 ülkede, 1.500'den fazla ATM bulunmaktadır ve sayıları her gecen gün artmaktadır (coinatmradar.com, 2017).

Genel olarak Bitcoin ATM'lerinden Bitcoin satın alma süreci şu şekilde olmaktadır:

- Doğrulama aşaması (isteğe bağlıdır, ayrıca makinenin türüne bağlı olarak büyük ölçüde değişebilir).
- Depozit için Bitcoin adresi belirtilir ya da temin edilir (anında bazı ATM'lerde isteğe bağlı olarak üretilebilir ve e-postayla gönderilebilir).
- ATM'ye nakit para eklenip işlem onaylanır (Bitcoin, Bitcoin adresinize gönderilir).

İşlemler ATM'den ATM'ye bazı farklılıklar gösterdiği için doğrulama işlemleri ve limitler farklılık gösterebilmektedir (coinatmradar.com, 2017). Bitcoin'un elektronik ödemeler alanındaki artan kullanımı, hızlı yaygınlaşmasına neden olmaktadır. Artan kullanımı aynı zamanda Grafik 3.2'de görüldüğü gibi ani sayılabilecek fiyat artışına da neden olmaktadır.



Grafik 3.2. Bitcoin'un Fiyat Grafiği

Kaynak: tradingview.com (2017)

2008 finansal krizinin ardından Ocak 2009'da çıkarılan Bitcoin'un başlarda nicelleştirilebilecek bir değeri bulunmazken ilk olarak 2010 yılında işlem görmeye başlamıştır. 2011 yılına kadar tek haneli rakamlar ile işlem görmüş ve Bitcoin'un açık kaynakkoduna dayanarak kripto para birimleri ortaya çıkmaya başlamıştır. 2012 yılında iki haneli rakamlar ile işlem gören Bitcoin'un, 2013 yılında ilk defa piyasa fiyatı 1.000

doları geçmiştir. Takip eden yıllarda ise 2017 yılına kadar 1.000 dalların altında işlem görmüştür. 2017 yılı Ocak ayında 1.000 Dolar iken Mayıs ayında 2.000, Ağustos ayında ise 4.000 Dolar seviyelerine kadar yükselmiştir.

Açık blok zinciri sistemlerinde varlığın ve işlemlerin kantına ihtiyaç duyulmaktadır. Bitcoin işlemleri sürecinde iş kanıtı üretilmesi, diğer katılımcıların doğrulamasını gerektiren ve doğrulamayı sağlayan, ayni zamanda nispeten kolaylaştırarak, belirli gereksinimleri karşılayan zor (maliyetli, zaman alan) bir veri parçasıdır. İş kanıtı üretmek, olasılığı düşük ve rasgele bir süreçtir. Geçerli bir iş kanıtı oluşturulmadan önce çoğunlukla, birçok deneme yanılma gerekmektedir. Bitcoin sisteminde Hashcash kanıt yöntemi kullanılmaktadır (Nakamoto, 2008: 3). İş kanıtı sayesinde üçüncü bir tarafa yani işlemleri doğrulayan bir arabulucuya ihtiyaç duymadan işlemler doğrulanabilmektedir.

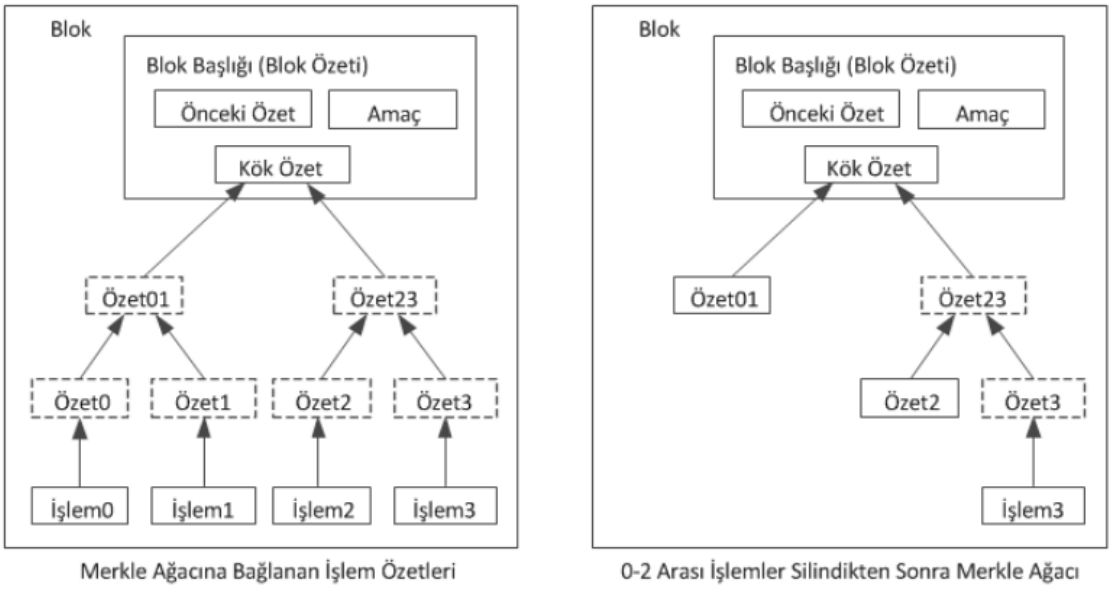
Bu kanıt yönteminin uygulaması, Hashcash'in kullanmış olduğu e-posta spam[33] ını önlemek için geliştirilmiş bir yöntemdir. Başka bir ifadeyle, her gelen mailden, postanın içeriği hakkında bir iş kanıtı istenilmektedir. Meşru e-postalar, iş kanıtını kolayca oluşturmaktadır. Ancak kitlesel spam e-posta gönderenleri, (bu da büyük bilgisayar kaynakları gerektirir) gerekli delilleri oluşturmakta zorluk çekecektir. Hashcash iş kanıtları, blok üretimi için Bitcoin'de kullanılmaktadır. Bir bloğun ağ katılımcıları tarafından kabul edilmesi için madenciler bloktaki tüm verileri kapsayan bir iş kanıtını tamamlamalıdır. Bu çalışmanın zorluğu, ağ tarafından yeni blokların her 600 saniyede bir üretilebileceği şekilde sınırlandırılmış olmasıdır. Başarılı üretim olasılığı çok düşük olduğundan, ağdaki çalışan hangi bilgisayarın bir sonraki bloğu oluşturabileceğini önceden tahmin etmek günümüz imkânlarıyla oldukça zordur. Bir bloğun geçerli olabilmesi, o an ki hedefin altında bir hash değerine sahip olmasını gerektirmektedir. Bu ise her bloğun, işin tamamlandığını onayladığı anlamına gelmektedir. Her bir blok önceki bloğun işlem özet fonksiyonunu içermektedir, bu nedenle her bloğun bünyesinde birlikte birçok işi barındıran bir bloklar zinciri vardır. Bir bloğu değiştirme işlemi, (ki bu sadece aynı selefi içeren yeni bir blok oluşturarak mümkün olmaktadır) tüm ardılları yenilemek ve içerdikleri işlemleri yeniden gerçekleştirmek gerekmektedir. Bu sistem

[33] Spam; (Önemsiz) çoğunlukla reklam içeriği içeren istenmeyen, genellikle elektronik olarak iletilen mesajları ifade etmektedir.

blok zincirini müdahalelere karşı korumaktadır. En yaygın kullanılan iş kanıtı yöntemi SHA256'ya dayalıdır ve Bitcoin'in bir parçası olarak tanıtılmaktadır (bitcoin.it, 2017).

İki madencinin aynı anda aynı işlemlerden bir blok oluşturması durumunda diğer bilgisayarlar bu blokların birinde zinciri inşa etmeye devam eder. Diğerine "yetim blok" (orphan block) denilmektedir. Ana zincirin parçası haline gelen bloğa ise "kardeş blok" (sister block) denilmektedir. Yetim bloğun bir parçası olan ve henüz işlem yapılmayan, doğrulanmamış bloklar açık işlem havuzuna geri dönmektedir. Sonuç olarak söz konusu işlemi içeren blok üzerinde bloklar oluşturulduktan sonra işlem güvenle doğrulanmakta, yani ana zincirin bir parçası haline gelmektedir (Geiling, 2016). Merkle ağacı ismini, hash ağacı kavramının patentini alan Ralph Merkle'den almıştır. Merkle ağacı, işlem özetlerinden oluşan çok gövdeli bir ağaçtır. Birçok yaprak, düğümleri özetlemek için verimli bir yol sağlamaktadır. Dağıtık kayıt defterinde, blok içerisindeki işlemleri özetlemek için Merkle ağacı kullanılmakta olup her işlem bir hash değeri ile temsil edilmektedir. İşlem hashları, Merkle ağacının altına yaprak düğümleri olarak eklenilir. Daha sonra Merkle ağacının yaprak düğümlerinden, Merkle ağacının tepesine ulaşıncaya kadar yukarı doğru inşa edilmektedir; orada yalnızca Merkle ağacı kökü olarak bilinen bir düğüm bulunmaktadır. Bu esnada SHA256 olan güvenli Hash algoritması kullanılmaktadır. Bloğun içinde bir işlemin varlığını kanıtlamak için bloğun içindeki tüm işlemlerin özetlerini bilinmesine gerek duyulmamaktadır. Bir N işlemler bloğu içinde, işlemlerin varlığını ispatlamak için gereken tek şey log2 (N) özet değerlerin sayısı ve eşit sayıda özet işlem gerçekleştirmesidir. Her seviyede özet işlem, sonraki adımda da tekrarlanarak kök düzeyine ulaşıncaya kadar yukarı doğru devam etmektedir. Hesaplanan kök özet değeri, bilinen kök değeri ile aynı ise işlemin doğruluğu kanıtlanmış olmaktadır. Bu yöntem işlemlerin doğrulanması için hızı önemli ölçüde arttırırken, aynı zamanda blok içindeki belirli bir işlemin varlığını kanıtlamak için gereken blok bilgilerini azaltmaktadır (Hong Kong Monetary Authority, 2016: 90). Bitcoin yapısında blok zinciri, kronolojik bir sırada bütün Bitcoin işlemlerinin halka açık bir kaydıdır. Blok zinciri, bütün Bitcoin kullanıcılarıyla paylaşılır. Bu işlem Bitcoin işlemlerinin kalıcılığını doğrular ve çifte harcama yapmayı önlemektedir (bitcoin.org, 2017). Blok zinciri, kökte ilk (genesis) bloğu ile başlayan ağaç şeklindeki bir yapıdır. Her blok potansiyel olarak bir sonraki bloktan oluşan birden çok adaya sahiptir

(Nakamoto, 2008). Şekil 3.4'te Merkle ağacının blok yapısının oluşumu gösterilmektedir, sadece uygun adaylar Merkle ağacına eklenmektedir.



Şekil 3.4. Merkle Ağacı Blok Yapısı

Kaynak: Nakamoto (2008: 4)

Eski bloklar ağaç dalları budanarak sıkıştırılabilmektedir. Ara özetlerin saklanmasına ihtiyaç duyulmamaktadır. Yalnızca onaylanan bloklar ana gövdenin/zincirin bir parçası haline gelmektedir.

Blok zinciri büyüklüğüne dair bazı hesaplamalar aşağıda anlatılmaya çalışılmıştır.

i. Bir blok başlığı işlemler hariç yaklaşık 80 bayt uzunluğundadır. Her 10 dakikada bir yeni blok üretildiğini varsayarsak 80 bayt * 6 * 24 * 365 = 4.2 MB / yıl etmektedir. 2008 yılında tipik bilgisayar sistemlerinin 2GB RAM ile satıldığı ve Moore yasasına dayanarak senede 1.2GB büyüme öngörüsüyle, blok başlıkları hafızada tutulsa dahi saklama bir sorun olmayacaktır (Nakamoto, 2008, 4).

ii. Bitcoin ile mevcut blok zincirin boyutu, saatte yaklaşık 1 (Megebayt) MB büyümektedir ve yaklaşık 20 (Gigabayt) GB'dır. Bitcoin ağı Visa gibi saniyede

> 2000 işlemi işlemesi durumunda, üç saniyede bir 1 MB[34] büyümesi gerekecektir (saatte 1 GB, yılda yaklaşık 8 (Terabayt) TB). Bu denli büyük bir blok zinciri boyutundaki sorun ise merkezileşme riskidir. Blok zinciri boyutu, örneğin 100 TB'a çıkarsa, muhtemelen yalnızca çok küçük sayıda büyük işletmenin tam düğümleri çalıştırmasını mümkün kılacaktır. Ethereum ile ilgili yaygın bir endişe ise ölçeklenebilirlik meselesidir. Bitcoin gibi Ethereum da, her işlemin, ağdaki her düğüm tarafından işlenmesi gerektiği kusurundan muzdariptir (Buterin, 2014: 33).

Bitcoin çok daha hızlı büyümektedir. 2017 yılı ortalarında Bitcoin blok zinciri boyutu yaklaşık olarak 130 GB'tır (blockchain.info, 2017). Blok büyüklüğü gibi bazı konu başlıklarının teşkil edeceği sorunlar ve tartışmalar devam etmektedir. Protokolde yapılacak değişimler çatallaşma (Fork) gerektirebilmektedir. Yumuşak çatallaşma (Soft Fork), protokolün güncellenmiş sürümlerinin önceki sürümlerle geriye dönük olarak uyumlu olduğu çatallaşmadır. SegWit[35] gibi yumuşak çatallaşma gerçekleştirildiğinde, tüm düğümler (güncellenmiş olsun olmasın) yeni blokları tanımaya ve blok zinciri üzerinde uzlaşmayı sürdürmeye devam edecektir. Sert çatallaşma[36] (Hard Fork), zorunlu çatallaşma da denilebilir. Sert çatallaşma, blok zinciri protokolünün eski sürümleri ile uyumlu olmayan değişikliktir. Köklü protokol değişikliği ile yeni bir blok zinciri oluşumu olarak düşünülebilir (bitcoincore.org, 2017). Bitcoin çatallaşması olan, Bitcoin Cash (BCH) ve Ethereum Classic (ETC) çatallaşması olan Ethereum (ETH) gibi sayıları her geçen gün artan yüzlerce alternatif uygulama, kripto para birimi olarak faaliyet göstermektedir (coinmarketcap.com, 2017). Sistemik önem derecesi düşük olan kripto paralara genel olarak Altcoin denilmektedir. Global yasal ödeme aracı olarak kullanılmakta olan ve tedavülden kalkmış, yüzlerce para birimi mevcuttur. Kripto para birimlerinde de benzer ya da farklı etkenler ile bir gelişim süreci olacaktır.

Blok zinciri, merkezi olmayan bir veri yapısına sahip olduğundan, farklı kopyaları daima senkronize değildir. Bloklar farklı zamanlarda farklı düğümlere varabilir, bu da

---

[34] 1 MB= 1.048.576 Bit

[35] SegWit; Segregasyonlu (Ayrık / Ayrılmış) Tanık (Segregated Witness). Bitcoin yazılımındaki bir takım problemlere ilişkin bir çözüm önerisidir. SegWit, Bitcoin çekirdek geliştirici ekibi (Bitcoin Core Team) tarafından yönetilen Bitcoin çekirdek kaynak kodu için bir güncelleştirmedir.

[36] Sert çatallaşma ile Bitcoin için Bitcoin Cash (BCH), Bitcoin Gold (BTG) ve Bitcoin SegWit2X (B2X) gibi blok zincirleri kullanımı söz konusudur.

düğümlerin blok zincirinin farklı perspektiflerine sahip olmalarına neden olmaktadır. Bunu çözmek için, her düğüm daima bilinen en uzun zincir veya en büyük kümülatif zorluğa sahip zincir olarak tanımlanan, iş kanıtını temsil eden blok zincirini seçerek denemeye başlamaktadır. Bir düğüm, zincirdeki her blokta kaydedilen zorluğu toplarken bu zinciri oluşturmak için harcanmış olan iş kanıtının toplam miktarını hesaplayabilmektedir. Tüm düğümler en uzun kümülatif zorluk zincirini seçtikleri sürece global Bitcoin ağı (sonunda) istikrarlı bir hal almaktadır (Antonopoulos, 2014, 204-205).

İş kanıtı aynı zamanda mutabakat birliğinin (çoğunluk kararının temsil edilmesi) sağlanmasından kaynaklanabilecek problemi de çözmektedir. Çoğunluk kararı (İnternet Protokolü) IP adreslerine dayalı bir yöntemle hesaplanıyor olsaydı birçok IP adresine sahip olanlar tarafından suiistimal edilebilirdi. İş kanıtı yönteminde 1 CPU, 1 oya eşittir. Çoğunluk kararı, iş kanıtının en fazla yapıldığı yani en uzun zincir tarafından temsil edilmektedir. CPU işlem gücünün çoğunluğu dürüst düğümlerin elindeyse dürüst zincir diğerlerinden daha uzun olacaktır ve rakip zincirleri alt edecektir. Saldırgan, geçmiş bloklardan birini değiştirmek için sonrasında gelen tüm bloklardaki işi tekrar yapması ve dürüst düğümlerin yaptığı işi yakalayıp geçmesi gereklidir. İş kanıtının zorluk seviyesi, artan donanım hızlarına ve değişken aktif düğüm sayısına ayak uydurmak için saatte ortalama blok hedefini tutturacak şekilde tekrar ayarlatılmaktadır. Eğer çok hızlı blok üretiliyorsa zorluk seviyesi yükselmektedir (Nakamoto, 2008, 3). Yüksek hızda (Güvenli Hash Algoritması) SHA256 algoritmasını çalıştırmanın yolu FPGA (Alanda Programlanabilir Kapı Dizileri) ya da ASIC (Uygulamaya Özgü Bütünleşik Devre) gibi donanım tabanında kodlama ile gerçekleştirilmektedir. Teknik olarak yapılan optimizasyonlar ile verimlilik daha da artırılabilir ve güç tüketimi azaltılabilmektedir (Balcısoy, 2017: 53). Bitcoin madenciliği için artık sıradan CPU ve GPU'nun kullanımı etkin değildir ve madencilik işlemleri düşündürücü derecede elektrik tüketimi gerektirmektedir.

3.2. Blok Zinciri 2.0

Tamamen dijital, merkezi olmayan, eşler arası para birimi ve özellikle Bitcoin, kripto para birimi çağını başlatmıştır. Kripto para birimlerinin paraya yenilik katmaları ve finansal piyasalara müdahil olma potansiyelleri çok büyüktür. Belki daha da önemlisi,

kripto para birimlerinin dayandığı dağıtılmış defter veri yapısı olan blok zincir sistematiğidir. Blok zincirine dayalı yeni startup'lara yapılan sermaye yatırımları, 2012'de başlayan yeni bir eğilim olarak ortaya çıkmıştır. Ancak o zamandan bu yana yatırımın yıllık büyüme hızı, dot-com balonundan bile daha hızlı bir büyüme göstermiştir. Blok zinciri uygulamaları, şirketlerin ve kişilerin işlem yapma, ödeme gönderme, sözleşme imzalama, sahiplik hakları ve daha birçok alanda kullanılabilmektedir. İşlem masraflarının azaltılması, bazen belirsiz ve masraflı olan arabuluculuk işlemlerini ortadan kaldırması, toplumun menfaati için olacak finansal içeriğe sahiptir. Bununla birlikte blok zinciri teknolojisi kullanıcıları ve piyasa katılımcıları, dolandırıcılık, kara para aklama ve siber suçlar gibi yeni risklerle de yüz yüze gelecektir. Bu nedenle, blok zinciri teknolojilerinin benimsenmesinden etkilenecek yeni alanlarda piyasa istikrarını garanti altına almak için yeni teknoloji düzenlemeleri tasarlanmalı ve uygulanmalıdır (Barberis vd. 2016: 219).

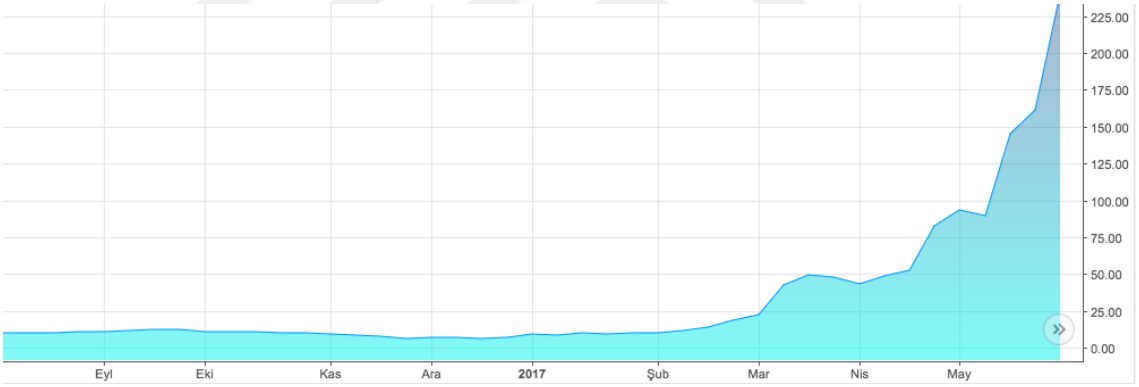
3.2.1 Ethereum Uygulaması

Ethereum, rakip bir para birimi olarak değil, dijital ekosistem içinde bir tamamlayıcı olarak görülmektedir Bitcoin olmadan Ethereum'un çıkarılması mümkün olamazdı. (etherium.org, 2017).

Dağıtık kayıt teknolojisi, iş dünyasına taktik kazanç sağlamaktadır. Blok zinciri akıllı sözleşmeler alanında da oldukça dikkat çekmektedir. Akıllı sözleşmeler, bir blok zincirde konuşlandırılabilen ve bir grup paydaş tarafından topluca paylaşılan ve onaylanan iş kuralları birikimidir. Akıllı sözleşmeler, iş süreçlerini güvenilir bir şekilde otomatikleştirmede çok yararlı olabilmektedir. Tüm paydaşların sözleşme kurallarını bir grup olarak işleyerek, doğrulamalarına imkan sağlamaktadır (Hyperledger Whitepaper, 2016). Akıllı sözleşmeler, en azından teorik olarak tamamen otomatikleştirilmiş, kendi kendini zorlayıcı ve geliştirici olabilmektedir. Bilgisayar kodunda sözleşme şartları ve koşulları belirlendikten sonra, sözleşme kendi işlemlerini sürdürebilir ve koşullar bilgisayar tarafından kod ve dışsal olaylar temelinde tarafsız bir şekilde yürütülmesi hedeflenilmektedir. Bu özellikler, akıllı sözleşmeleri birçok ticaret ilişkisinde özellikle mali hizmetler dahilinde çok çekici kılmaktadır. Otomasyon, blok zincirinin dağıtık yapısı ile ilişkili olarak, geleneksel güven inşa maliyetlerinin azalması ile birlikte, işlem

maliyetlerini önemli ölçüde düşürerek bu tür kullanımları çok daha karlı hale getirmektedir (Gronbaek, 2016).

Ethereum projesinin birçok amacı vardır. Kilit hedeflerden biri, birbirlerine güvenme imkânı bulamayan bireylerin arasındaki onaylanması gereken işlemlerin gerçekleştirilebilmesini sağlamak ve kolaylaştırmaktır. Bu güvensizliğin sebebi coğrafi bir ayrım, ara yüz oluşturma zorluğu, mevcut yasal sistemlerin belki de uyuşmazlığı, yeterince beceri sahibi olmaması, isteksizliği, masrafı, belirsizliği veya yolsuzluğa bağlı olarak olan zorluklar olabilir. Bu amaçla, zengin ve açık bir dil aracılığıyla bir geliştirme sistemi belirleyerek ve böylece bir anlaşmanın özerk olarak uygulanacağının, makul bir şekilde beklenebileceği bir sistem tasarlayarak, bu işlemler için bir araç sağlanmak istenilmiştir (Wood, 2014, 1). Kripto para birimi olmanın ve elektronik ödemelerin ötesinde kullanım olanakları sağlayan Ethereum'a karşı gösterilen ilgi Grafik 3.3'den anlaşılacağı gibi oldukça artmıştır.



Grafik 3.3. Ethereum'un Fiyat Grafiği

Kaynak: tradingview.com (2017)

Ethereum 2014 yılında halka arz edilmiş olup, halka arzın 42 gün olması belirlenmiştir. Halka arz süresi boyunca ilk iki hafta için fiyatlandırması 2.000 ETH = 1 BTC olarak ayarlanmıştır. Takip eden günler için oran doğrusal azalarak 1337 ETH = 1 BTC nihai oranı olarak belirlenmiştir (Buterin, 2014). Ethereum halka arz süresinde Bitcoin fiyatı yaklaşık olarak 450$ - 650$ dolar arasında işlem görmüştür. Mayıs 2016'da 10 dolar olan Ethereum fiyatı, Mayıs 2017'de 100 dolara ulaşmıştır. 2017 Haziran ayında ise 300 doları geçmiştir.

Bitcoin ve Ethereum birbirlerine benzeselerde, birbirlerinden ayıran birçok farklılıkları vardır. Ethereum blok zinciri protokolü, ödeme sisteminden çok daha fazlası olacak şekilde tasarlanmıştır. Akıllı sözleşmeleri çalıştıran ancak merkezi olmayan bir platform olarak kesinti, sansür, dolandırıcılık veya üncü parti müdahaleleri olmadan programlanmış olarak çalışan uygulama olması amaçlanmaktadır. Ethereum'un protokolü, Ethereum sistemi içinde çok çeşitli akıllı sözleşmeler programlama olanağı sağlamak için esneklik sağlamak ve işlevselliği artırmak için oluşturulmuştur. Ethereum, yedi farklı programlama dili içeren Turing-bütün programlama dilinde yazılmış olup C ++ ile yazılmış olan Bitcoin'den birçok farklılıklar göstermektedir (Harm, Obregon ve Stubbendick, 2016, 3).

Grafik 3.4. Bitcoin ve Etherumun Piyasa Değerinin Toplam Piyasa Değerine Oranı

Kaynak: coinmarketcap.com (2017)

Grafik 3.4'te görüldüğü gibi Bitcoin'un diğer kripto para birimleri arasındaki pazar payı % 95'lerden, 2017 yılının üçüncü çeyreği itibariyle, %40'lara gerilemiş durumdadır. Bitcoin'un pazar payının azalmasına rağmen kripto para sektörünün büyümesi, yaygınlaşan kullanımı sonucu, işlem hacmi sürekli artmış ve hala en çok işlem hacmine sahip kripto para olmasını mümkün kılmıştır. Ethereum %20 pazar payına yaklaşırken diğer kalan kripto para birimlerinin toplam pazar payı %30'ların üzerindedir.

Ethereum blok zinciri protokolü, doğrudan herhangi bir uygulamayı desteklememektedir. Geliştirilen Ethereum protokolü ile yalnızca bir para birimi

oluşturmanın ötesine geçmek amaçlanmaktadır. Merkezi olmayan dosya depolama, merkezi olmayan hesaplamalar ve merkezi olmayan pazarlar etrafındaki protokoller ve merkezi olmayan uygulamalar gibi, diğer konseptlerin etkinliğini önemli ölçüde artırarak diğer eşler arası protokollere büyük bir destek sağlayabilmektedir. Nihai olarak, para ile doğrudan ilgisi olmayan önemli bir dizi uygulamaları da bünyesinde barındırmaktadır. Ethereum, veri depolama ve finans alanındaki belirli bir uygulama dizisi için tasarlanmış kapalı uçlu tek amaçlı bir protokol olmaktan ziyade, açık uçlu tasarıma sahiptir. Bir temel yapı olarak Ethereum, hizmet vermek için son derecede uygundur. Önümüzdeki yıllarda çok sayıda finansal ve finansal olmayan protokoller için bir yapı oluşturması beklenmektedir (Buterin, 2014: 33-34). Ethereum ağı kendi dahili para birimini, Ether olarak adlandırmaktadır (Buterin, 2014: 13). Ethereum Gas ise temel ağ maliyet birimidir. Gas, dahili Ethereum hesaplama motorunun dışında mevcut değildir. Fiyatı işlem tarafından belirlenir ve madenciler Gas fiyatı çok düşük işlemleri göz ardı etmekte özgürdürler (Wood, 2014: 15). Bitcoin'in blok zincirinde yeni bir bloğun eklenmesi yaklaşık 10 dakikada gerçekleşmektedir. Ethereum da ise ortalama blok zamanı yaklaşık 20 saniyedir (etherscan.io, 2017). Blok zinciri sistemlerinde yapısal değişiklikler yapmak mümkündür. Ethereum'un mevcut tasarımına ilişkin yapısal iyileşme planlamaları mevcuttur. 2017 yılında Ethereum, kanıt mekanizması olarak kullanmış olduğu iş kanıtından (PoW, Proof of Work), Casper pay kanıtı (PoS, Proof of Stake) denilen daha verimli olması beklenen ve daha az madenci desteği gereksinimini öngören yeni bir fikir birliği algoritmasına geçmeyi planlanmaktadır (ethereum.org, 2017).

Kripto para ekosistemi her geçen gün büyümektedir. ICO (Initial Coin Offering), kripto para alanındaki halka açılma, halka arz ve satış yönetimini temsil etmektedir. ICO, şirketlerin ilk halka arzıyla (IPO, Initial Public Offering) oldukça benzerlik göstermektedir. ICO, Kripto para kullanımı aracılığıyla yapılan bir tür kitlesel fonlama yöntemidir. Genellikle ICO öncesi, ihraççı tarafından IPO'daki izahnameye benzeyen White Paper[37] adında bir bilgilendirme raporu hazırlanır. Daha sonra, farklı özelliklere sahip payları temsil etmek üzere Token'ler ihraç edilmektedir. Token, oy kullanma hakkı, bilgi edinme hakkı gibi belirlenen çok farklı hakkı temsil ederken farklı fonksiyonlara da sahip olabilmektedir. Çeşitli yapılarda ihraç edilmiş olan yüzlerce

[37] White Paper; (Doküman) spesifik bir konuda bilgilendirme çalışması.

kripto para ile finanse edilebilen varlığın mevcut olduğu bilinmektedir (coinmarketcap.com, 2017). Elektronik ödeme kullanılarak kripto para ile yapılabilecek ICO yatırımlarının, yakın bir gelecekte binlerle ifade edilmesi beklenmektedir.

ICO ve Token piyasalarına düzenlemeler getirmek için bazı ihraççılar ile düzenleyici ve denetleyici kurumlar tarafından yapılan çalışmalar devam etmektedir. Bu düzenlemelerin asıl amacı, kripto para birimlerine karşı güven sağlayabilmek ve mevcut finansal sisteme başarılı bir şekilde entegre edebilmektir. ICO ve Token piyasaları düzenlemeleri gelecekte, Internet Tahsisli Sayılar ve İsimler Kurumu (ICANN[38], Internet Corporation for Assigned Names and Numbers) benzeri bir yapıda gerçekleşebilir.

3.3. Blok Zinciri 3.0

Önceleri işlem ve varlık bilgileri, fiziksel kitaplarda saklanılmaktaydı. Teknoloji geliştikçe fiziksel kitaplar, dijital kayıtlara dönüştürülmüştür. Bugün, her finansal kuruluş kendi dijital "kayıt defteri" deposunu bulundurmaktadır. Bunun sonucunda, merkezi aracılar çoğalmakta ve tarafların birbirlerine güvenmelerini gerektirmeden işlemleri kolaylaştırmak için tarafsız uzlaşma hizmetleri sağlamaktadırlar (WEF, 2016: 25).

Blok zincirleri merkezi olmayan ve izinsiz denilen yapıda olabilmektedir. Bu nedenle, finans sektöründe büyük değişiklere neden olabilir, özellikle de ödemeler alanında. 2015'ten bu yana, bir dizi büyük uluslararası finansal kurum blok zinciri-sektörü için planlar oluşturmaya başlamışlardır. Goldman Sachs, J.P. Morgan, UBS ve diğer bankacılık devleri, blok zinciri platformlarıyla yakın işbirliği içinde çalışarak kendi blok zinciri laboratuvarlarını kurmuşlardır ve bu konuda birçok çalışma yayınlamışlardır. Goldman Sachs, bünyesinde blok zincir teknolojisine dayalı ödeme işlemleri için bir patent bulundurmaktadır. Buna ek olarak, Nasdaq ve New York Borsası gibi çeşitli

[38] ICANN; global organize olmuş, İnternet Protokolü adresi alanı tahsisi, protokol tanıtıcı ataması, genel (gTLD) ve ülke kodu (ccTLD) Üst Düzey Alan ismi sistemi yönetimi ve kök sunucu sistemi yönetimi işlevlerinden sorumlu kâr amacı gütmeyen bir kurumdur. ICANN'in yapısı içinde hükümetler ve uluslararası anlaşmalarla kurulan organizasyonlar, şirketler, ve küresel internet ağının inşa edilmesine ve korumasına katkıda bulunma kabiliyetine sahip bireyler bulunmaktadır.

ulusal borsalar da blok zinciri teknolojisi hakkında ayrıntılı araştırmalar yapmışlardır. Aralık 2015'te Nasdaq, Linq markalı blok zinciri işlem platformunu kullanarak ilk menkul kıymet işlemini tamamladığını açıklamıştır. Ayrıca, ABD Mevduat Muhafaza ve Takas Şirketi (DTCC, Depository Trust & Clearing Corporation), Visa, Dünya Bankalararası Finansal İletişim Kuruluşu vb. planlarını blok zinciri teknolojileri sektöründe genişletmektedirler (Guo ve Liang, 2016: 2). DLT, aracıların sayısını azaltarak ve mutabakat sürecini daha verimli hale getirerek, bazı finansal işlemlerin gerçekleştirebilmesini hızlandırabilmektedir. Ayrıca DLT, tarafların ülkeler arasında birbirleri ile daha kolay işlem yapmasını sağlayarak birden fazla aracıya duyulan gereksinimi azaltabilmektedir. Muhasebeciler paylaşılan yapısı nedeniyle, DLT ağına katılanların hepsi kendi kopyalarını ellerinde tutacak ve bir fikir birliği üzerinde anlaşmaya varmak için algoritmalar kullanarak, DLT mutabakat sürecini daha hızlı ve daha verimli gerçekleştirebileceklerdir (ESMA, 2016: 10).

Blok zincir teknolojileri hakkındaki farkındalığın artması, sonuçta, dağıtılmış fikir birliği ve hesaplama için karmaşık kriptografik tekniklerin hakkında farkındalığı arttıracaktır (Baron vd. 2015: 69). Kripto para birimlerinin geleceği genel olarak, Bitcoin'un geleceğinden daha parlaktır. Bitcoin tamamen yeni bir yerel olmayan örgütlenme ve fikir birliğini ortaya koymaktadır. Bu fikirler, ekonominin geniş sektörlerini, para birimleri, merkez bankacılığı ve kurumsal yönetişime kadar birçok alanda etkili olmaya aday konumundadır. Merkezi kurumlar veya kuruluşlar, daha önceleri yetkili veya güvenilir kontrol noktalarının görevleri artık ademi merkezi olarak merkezden uzaklaşabilecektir. Blok zinciri ve mutabakat sisteminin büyük ölçekli sistemlerde örgütlenme ve koordinasyon maliyetini önemli ölçüde azaltması beklenmektedir. Aynı zamanda güç odağı olma, yolsuzluk ve piyasayı düzenlemekten kaynaklanan bazı sorunları ortadan kaldıracağı ifade edilmektedir (Antonopoulos, 2014: 233). Ayrıca ödemeler alanının dışında, blok zinciri sistematiğinin Endüstri 4.0[39] ve Web 3.0[40] gibi gelişmelerde de önemli fonksiyonlar üstlenmesi beklenmektedir.

[39] Endüstri 4.0; Ağ oluşumu, enformasyon şeffaflığı, teknik yardım, ademi merkezi karar verme ilkelerini temel alan örgütsel bir tasarım konseptidir.

[40] Web 3.0; Aynı zamanda Semantik Web olarak da adlandırılmaktadır. Semantik Web kavramı, World Wide Web'in kurucusu olan Tim Berners-Lee'nin önerisine dayanmaktadır. Enformasyonların iyi tanımlanmış (anlam verildiği), bilgisayarların ve kişilerin işbirliğinde mevcut web' in daha iyi çalışmasını sağlayacak bir gelişmedir.

3.3.1. Hyperledger Projesi

Hyperledger, gelişmekte olan bir blok zinciri yapısı olup işletmeler arasında ve işletmeyle müşterileri arasında yapılan işlemlerde kullanılmaktadır. Hyperledger projesi, rakip işletmelerin aynı sektörde faaliyette bulunurken ortaya çıkan çeşitli gereksinimleri destekleyerek, hukuki ve diğer düzenlemelere uyum sağlamayı mümkün kılmayı amaçlamaktadır. Bu gereksinimler ise şunlardır;

- Akıllı sözleşmeler,
- Dijital varlıklar,
- Veri birikimleri,
- Merkezi olmayan mutabakat tabanlı ağlar,
- Kriptografik güvenliktir.

Blok zinciri alanında, performans iyileştirmesi için endüstri gereksinimleri, kimlik doğrulamaları, özel ve gizli işlemler ve eklenebilir bir mutabakat modeli içermektedir.

Blok zinciri teknolojisinin potansiyelini tam olarak gerçekleştirmek ve birçok farklı kullanıma adapte olabilecek bir standart oluşturmak için, Hyperledger yapısı esnek ve genişletilebilir olarak tasarlanmıştır. Buna ek olarak, çeşitli bilgisayar bilimleri disiplinlerinde son gelişmelerin çoğunu içeren ve ekleyebilen yapıya sahiptir (Hyperledger Whitepaper, 2016).

Hyperledger Projesinde (www.hyperledger.org), kurumsal düzeyde, açık kaynaklı, dağıtık kayıt yapısı ve bir kod tabanı oluşturmak için ortak bir çaba gösterilmektedir. Ticari işlemlerin global olarak belirli düzeyde yürütme şeklini değiştirebilecek, dağıtık kayıt için sektörler arası açık ve standart bir platform tanımlayarak, blok zinciri teknolojisini geliştirmeyi amaçlamaktadır. 2016 yılının başında Linux Vakfı'nın bir projesi olarak kurulan Hyperledger Projesi, 2017 ortalarında 130'den fazla üyeye sahiptir (hyperledger.org, 2016).

Hyperledger, Linux Foundation'ın açık kaynaklı, işbirlikçi ve işletmelere uygun blok zinciri teknolojisi için çalışmaktadır. Hyperledger Fabric, bir blok zinciri çerçeve uygulamasıdır. The Linux Foundation tarafından modüler bir mimari ile bünyesinde

değiştirilebilir hizmetler barındıran Hyperledger projelerinden biridir. Hyperledger Fabric`in başlıca amaçları ise kısaca aşağıda verilmiştir.

- Özel ve kamusal işlemlerde tanımlı kimlikleri desteklemek,
- İzinli paylaşılan kayıtlar oluşturmak ve destek sağlamak,
- Performansın ölçülmesinde ve değerlendirilmesinde kimlik güvenliği ve gizliliğini temin etmek,
- İş kanıtı ile ilgili ortaya çıkan maliyetleri azaltmaktır,
- Hukuki düzenlemelere uyumlu bir sistem ile farklı ihtiyaçlar için değişik sektörlerdeki kullanım durumlarını desteklemek (Gupta, 2017: 32).

İlk blok zinciri uygulamaları bir takım amaçlara hizmet etmektedir. Ancak çoğu zaman, belirli endüstrilerin ihtiyaçları için mevcut blok zinciri uygulamaları uygun değildir. Modern pazarların taleplerini karşılamak için Fabric, endüstri odaklı bir tasarım üzerine kurulmuştur. Fabric, izinli ağlar ile çoklu blok zinciri ağlarında gizlilik sağlamak için yeni bir yaklaşım ortaya koymaktadır (Hyperledger Fabric, 2017: 27). Fabric, eklenebilir bir mimariye dayanmakta ve böylece geliştiriciler, görevlendirmelerini, kendi gereksinimlerine en uygun olan uyumlu modül ile yapılandırabilmektedir.

Hyperledger yapısı, İnternet Mühendisliği Görev Grubu[41] (IETF, Internet Engineering Task Force) gibi, teknik bir yönlendirme komitesini ve gerekirse oylama ile fikir birliğine ulaşmak için gerekli süreci desteklemektedir ve kod tabanında değişiklikler yapılabilmektedir. Endüstriyel kullanım ve eğitim için, aynı zamanda bir pazarlama komitesi ve son kullanıcı teknik danışma kurulu mevcuttur. Hyperledger projesinde güvensizliğin oluşmasını engellemek üzere kodları görülebilir yapmak mümkündür (WEF White Paper, 2017: 18). En popüler izinli blok zinciri platformlarından olan Hyperledger Fabric, eklenebilir mutabakat modeli ile esnek bir mimari sunmaktadır. Fabric, konsorsiyumlarında katılımcı grupların tanımlanmasının yanında aynı zamanda kimlikleri kayıt altına alınmış ve sistemde çalışan merkezi bir kayıt servisiyle doğrulanmış olan konsorsiyumlar için tasarlanmıştır. Ayrıca blok zincirindeki, zincir kod olarak da bilinen akıllı sözleşmeleri desteklemektedir. Gelecekteki sürümleri için de alternatif fikir birliği algoritması önerileri bulunmaktadır (Baliga, 2017: 9). SWIFT

[41] İnternet Mühendisliği Görev Grubu; internet mimarisinin gelişimi ve internetin düzgün çalışması ile ilgilenen herkesin katılabileceği uluslararası bir topluluktur.

önde gelen global transaksiyon bankalarıyla işbirliği içerisinde Hyper ledger teknolojisini kullanarak, dağıtık kayıt teknolojisi ile kullanılabilecek olan konsept kanıtlaması (Proof of Concept, PoC) üzerinde çalışmalar yürütmektedir. Konsept kanıtlaması ile bankalar açısından gerçek zamanlı nostro hesaplarının mutabakatını iyileştirerek global çapta likidite optimizasyonu sağlanmak istenilmektedir (swift.com, 2017). Blok zinciri teknolojisinin gelişimi ile birlikte elektronik ödemeler ve diğer alanlarda kullanılabilecek konsept kanıtlaması, otorite kanıtlaması (Proof of Authority, PoA) veya farklı kanıt yapıları daha da geliştirilecektir.

3.4. Blok Zincir Sistematiğinin Başlıca Kullanım Alanları

Genel olarak blok zincirinin olası kullanım alanları, yedi ana başlık altında aşağıda gösterilmiştir (ledracapital.com, 2014):

I. Finansal Araçlar, Kayıtlar ve Modeller
1. Para Birimi
2. Akıllı sözleşmeler
3. Özel sermaye / Hisse senetleri
4. Tahviller
5. Türev araçları
6. Yukarıdaki maddelerden herhangi biriyle bağlantılı oy hakları ve Token yapısı
7. Emtialar
8. Harcama kayıtları
9. Ticaret kayıtları
10. İpotek / kredi kayıtları
11. Servis kayıtları
12. Kitlesel fonlama
13. Mikrofinans
14. Mikro yardımlaşma

II. Herkese Açık Kayıtlar
15. Arazi kayıtları
16. Araç kayıtları
17. İşletme lisansı
18. Ticari işletmelerin kuruluş / kapatma kayıtları
19. İşletme sahipliği kayıtları
20. Düzenleyici kayıtlar
21. Suç kayıtları
22. Pasaportlar
23. Doğum belgeleri
24. Ölüm sertifikaları
25. Oy kullanma kimlikleri
26. Oylama
27. Sağlık / güvenlik denetimleri
28. İnşaat izinleri
29. Silah ruhsatları
30. Adli tıp kanıtları
31. Mahkeme kayıtları
32. Oylama kayıtları
33. Kâr Amacı Gütmeyen Kayıtlar
34. Devlet / kâr amacı gütmeyen muhasebe / şeffaflık

III. Özel Kayıtlar
35. Sözleşmeler
36. İmzalar
37. İstekler
38. Vakıflar
39. Emanetler
40. GPS kayıtları (kişisel)

IV. Diğer Yarı Açık Kayıtlar
41. Unvanlar
42. Sertifikalar
43. Öğrenme çıktıları
44. Notlar
45. İnsan kaynakları kayıtları (maaş, performans incelemeleri, başarı)
46. Tıbbi kayıtlar
47. Muhasebe kayıtları
48. Ticari işlem kayıtları
49. Genom verileri
50. GPS kayıtları (kurumsal)
51. Teslimat kayıtları
52. Hakemlik

V. Fiziksel Varlık Anahtarları

53. Ev / daire anahtarları
54. Tatil evleri / devre mülk anahtarları
55. Otel oda anahtarları
56. Araba tuşları
57. Kiralık araba anahtarları
58. Leasing araç anahtarları
59. Kilitleme tuşları
60. Güvenlik kasası tuşları
61. Paket teslimatı
62. Bahis kayıtları

VI. Sanal Değerler

63. Kuponlar
64. Makbuzlar
65. Rezervasyonlar
66. Film biletleri
67. Patentler
68. Telif hakları
69. Ticari Markalar
70. Yazılım lisansları
71. Video oyun lisansları
72. Müzik / film / kitap lisansı
73. Alan adları (Domain)
74. Çevrimiçi kimlikler
75. Yazarlık kanıtı / eserin kanıtı

VII. Diğer Alanlar

3.5. Blok Zincir Sistematiğinin Finansal Piyasalar Üzerine Muhtemel Etkileri

Blok zinciri, dijital kayıtların herhangi bir merkezi otorite olmadan güvenli bir şekilde tutulabileceğini gösteren bir teknolojik yeniliktir. Verileri dağıtılmış veri tabanları aracılığıyla paylaşma fırsatları yıllardadır mevcuttur. Karşılıklı olarak dağıtık kayıt teknolojisine karşı duyulan güncel ilgi, değişim için gerçek bir fırsattır. Ancak, bu teknolojinin hangi alanlarda kullanılacağına dair gerçekçi olmayan beklentiler oluşturulması tehlikesi vardır. Düzenleyiciler doğal olarak temkinlidirler. Çünkü, hafızalarda, 2007-2009 küresel mali krizinde yeterince düzenlememiş olan ABD doları gölge bankacılığı[42] nın hatıraları vardır (SWIFT Institute, 2016: 32).

Federal Reserve ve diğer merkez bankaları ödeme sisteminin gelişmesine, gözetimine rehberlik etmek için geniş kamu politikası hedeflerini benimsemişlerdir. Etkin bir ödeme sisteminin, parayı düşük maliyetli ve uygun yollarla aktarmak için gereken altyapıyı sağlaması gerekmektedir. Verimli sistemler, değişen teknolojiye ve değişen taleplere yanıt olarak hizmet kalitesini yükseltmede yenilikçidirler. Verimli sistemler genel olarak, ülkedeki tüketiciler, işletmeler ve finansal kuruluşlar için uygun araçlar vasıtasıyla erişilebilirdir. Güvenli ödeme sistemleri kendisini kanıtlanmış teknolojiden üretilmektedir, güvenilirdir ve bütünlük içinde çalışmaktadır. Güvenli sistemler, yasal, operasyonel, güvenlik ve finansal riskler de dahil olmak üzere bir dizi iyi bilinen riski

[42] Gölge bankacılık sistemi; (Shadow Banking) Bankacılık sektörü kadar sıkı düzenlemelere tabi olmamakla birlikte likidite riskine ve yüksek kaldıraçtan kaynaklı risklere maruz kalan bir bankacılık türüdür.

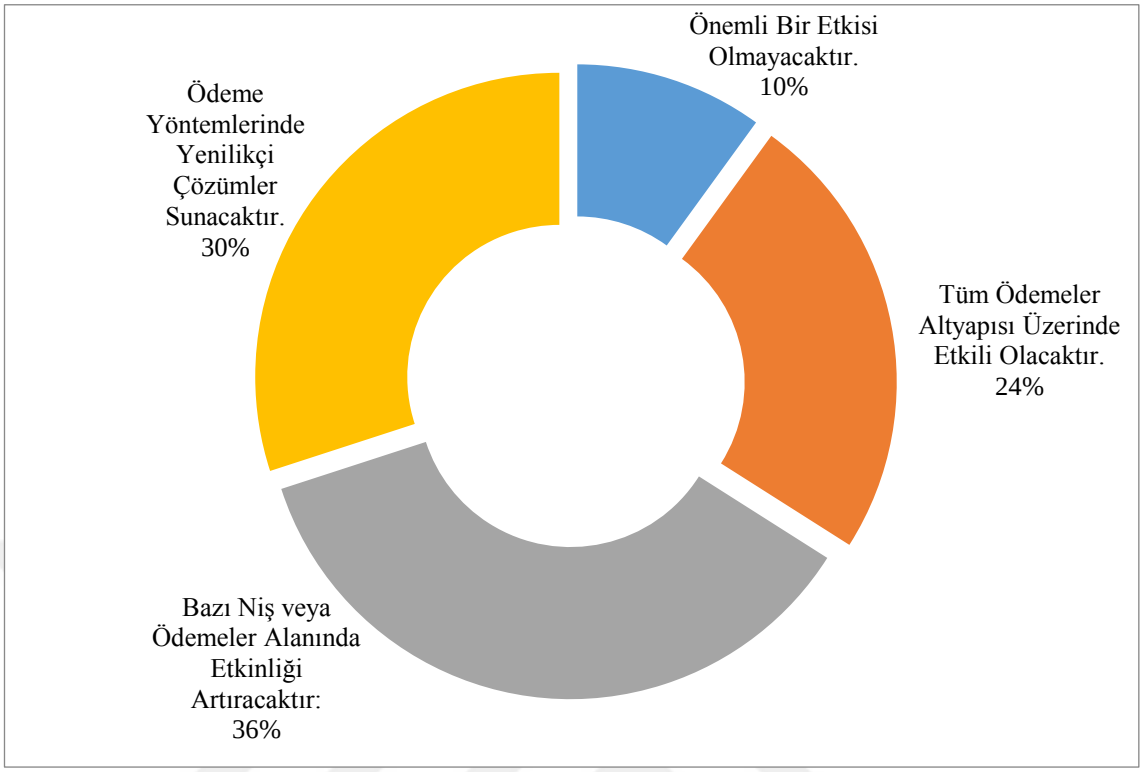
yönetebilmektedir. Veri (bilgi) güvenliği ve gizlilik son yıllarda özellikle önem kazanmıştır. Genel olarak, ödeme sistemleri yenilikçi olmalı, aynı zamanda riskleri ele alarak, finansal istikrarı destekleyerek kamu güvenini sürdürebilmelidir (FED, 2017: 3). Blok zinciri sürdürülebilir gelişmeler için kullanılacak bir araç, teknolojik alt yapı hizmeti sunabilecek bir gelişme olarak görülebilir.

Ödemeler endüstrisi, finansal kurumların başlıca iş alanlarından birini temsil etmektedir. Esas olarak, ödemeler kârlı bir gelir kaynağı değildir, çeşitli hizmetler için çapa ürünüdür ve müşteri verileri açısından da kritik bir unsur olama özelliğindedir. Bankalar için, ödeme bilgileri müşteri hakkında bilgi kaynağı sağlamaktadır. Bankaların kendi iş süreçlerini müşterilerin iş süreçlerine entegre etmek amacıyla kullanabileceği, referans noktaları üretmek için bir fırsattır. Bu nedenle, ödeme işlemlerinin sağladığı kazançların kaybedilmesi bankalar için olumsuz sonuçlar doğurabilir. Küresel olarak akıllı telefonların kullanılması, büyük teknoloji ve telekomünikasyon şirketleri gibi yeni kuruluşların piyasaya girmesini mümkün kılmaktadır. Buna ek olarak finansal hizmetler sektöründe faaliyet göstermekte olan şirketler bilgi teknolojilerine bağımlıdırlar. Uyum ve bilgi teknolojilerine yatırım ihtiyacı her geçen gün artmaktadır. Geleneksel kaynaklardan gelen gelirin erozyonu ve rekabetin artması arasında sıkışan birçok finansal kuruluşun, iş modelleri ve yapıları baskı altındadır (Holotiuk, Pisani ve Moonmann, 2017: 915-916). Eşten eşe gelişen yapılar ekonomik modelleri oldukça kuvvetli etkilemektedir.

Bu bağlamda, blok zinciri teknolojisi, özellikle ödemelerde finansal kurumların üçüncü parti işlevini durdurabileceğinden dikkat çekici bir sistemdir. Aynı zamanda, ödemelerde blok zincir kullanımı ile gerçekleştirilebilecek olan maliyetlerin azaltılması, finans kuruluşlarının blok zincirinin gelişimine yakından bakmasına neden olmaktadır. Blok zinciri teknolojisinin bu umut verici potansiyeli, SWIFT gibi uluslararası ödeme işlemleri sağlayıcıları ve düzenleyicileri mevcut ödeme altyapı operatörleri büyük ilgi göstermektedir. Finansal hizmetler sektörü girişimcileri, blok zinciri tabanlı çözümlerin prototiplerini araştırmakta ve başlatmaktadırlar. Özellikle mevcut şirketler, kurum içi platformlar geliştirmek, blok zinciri şirketlerine doğrudan yatırım yapmak, onlarla ortaklık kurmak veya blok zinciri uygulamalarını keşfetmek için hızlandırıcı hizmetlerden yararlanmak gibi bir dizi stratejiyi uygulayarak iş modellerini savunmaya

çalışmaktadır. Büyük bankalar, global çapta işbirliklerine katılmaya başlamışlardır ve denetim firmalarının yanı sıra neredeyse tüm büyük danışmanlıklar bu alanda uzmanlığını sunarak önde gelen bilgi sağlayıcıları olarak konumlandırılmaya çalışılmaktadırlar (Holotiuk, Pisani ve Moonmann, 2017: 915-916).

Varlıklar her zaman fiili sahiplerine ait olmalı ve varlık sahipleri varlıkların yasal sahipliğini üçüncü kişilere geçirmeden üçüncü taraf uzmanlarının varlıklarını yönetmesine izin vermelidir. Üçüncü taraf, varlık yöneticileri veya depo bankaları, varlıkları sahibinin adına satın alabilir, satabilir ve ödünç verebilirken ihraç edenler, varlık sahiplerine (örneğin, hisse senedi sahiplerine) mesaj veya ödeme göndermeleri gerekiyorsa, ihraççılar bunları doğrudan varlık sahiplerine gönderebilmelidir. Pay sahiplerinin ödemelerin yönetilmesi ve yönlendirilmesi gibi varlık sahipliği görevleri hakkında endişelenmeden, bu düzenleme uyarınca, saklayıcılar, pay sahiplerine katma değerli hizmetler sunabilirler (Hyperledger Fabric, 2017: 103). Blok zinciri teknolojisi hem finansal hem de finansal olmayan geniş alanlarda uygulama fırsatlarına sahiptir. Finansal kurumlar ve bankalar aslında blok zinciri teknolojisini geleneksel ticari modellere yönelik tehdit olarak görmemektedir. Kripto para birimlerinin piyasa değeri, 2017 yılında önemli ölçüde artmış olsa da Avrupa Merkez Bankası Başkanı Mario Draghi'ye göre reel ekonomiye bağlantısının önemli ölçüde güçlendiğini gösteren herhangi bir kanıt bulunmamaktadır. Avrupa Merkez Bankası tarafından raporlarda da iddia edildiği gibi, gelecekte kripto para birimlerinden kaynaklanan risklerin oluşması gerçekleşebilir ve böyle bir durumda finansal istikrar perspektifinden daha doğrudan bir düzenlemeye ihtiyaç duyulabilecektir. Bu düzenleme reaksiyonunun uluslararası düzeyde koordine edilmesinin, muhtemelen daha etkili olacağı belirtilmiştir (ECB, 2017: 1-2). Doğal olarak kripto para yapıları kullanımında bir artışı göz önünde bulundurarak, finansal istikrar perspektifinden kripto para yapılarını takip etmek önemli olacaktır. Dünyanın en büyük bankaları, bu alanda yenilikçi blok zinciri uygulamaları üzerine araştırmalar yaparak yeni fırsatlar aramaktadırlar. Avrupa Ödemeler Konseyi tarafından gerçekleştirilen, "Ödemelerde Blok Zincirinin Etkileri" konulu anket sonuçları Şekil 3.5'de gösterilmiştir. Blok zinciri uygulamalarının finansal alandaki etkileri kesin olarak çizilemese de, özellikle elektronik ödemeler alanında önemli etkileri olacaktır.



Şekil 3.5. Ödemelerde Blok Zincirinin Etkileri Konulu Avrupa Ödemeler Konseyi Anketi Sonuçları

Kaynak: europeanpaymentscouncil.eu (2016)

Avrupa Ödemeler Konseyi (EPC), blok zinciri teknolojisine ilişkin anket sonuçlarında % 90'lık bir kesimin 2025 yılına kadar blok zinciri teknolojisinin ödemelerde önemli bir etkisi olacağını düşünmektedir. Ankete katılanların sadece %10'unun blok zincirinin "önemli bir etkisi olmayacağını" belirtmiştir. Blok zinciri teknolojisinin 2025 yılına kadar Avrupa ödemelerinde önemli bir etkisi olacağını düşünenlerin %36'lık kısmı, bazı niş[43] alanlarda veya ödemeler alanında etkinliği artırabileceğini düşünmektedirler (blok zinciri teknolojisinin belirli amaçlar için benimsendiği kanaatindedirler). Katılımcıların %30'u blok zinciri temelli sistemlerin, ödeme yöntemlerinde yenilikçi çözümler sunacağı kanaatindedir (blok zinciri teknolojisi diğer pek çok önemli modele benzetilmektedir). Katılımcıların %24'ü ise tüm ödemeler altyapısı üzerinde etkili olacağını düşünmektedir (blok zincirinin, teknolojik paradigma kaymasında bir ana sütununa dönüşeceğini düşünmektedirler).

[43]Niş pazar; belirli bir ürün ya da hizmet çeşidi için uygun, pazarın uzmanlaşmış bir bölümü.

Blok zinciri ile ilgili gerçekleştirilen analizler, dağıtık kayıt teknolojisinin, sınır ötesi ödemelere, menkul kıymet ticaretine ve mevzuata uygunluk konularına ilişkin atfedilebilecek bankaların altyapı maliyetlerini 2022 yılına kadar yılda 15-20 Milyar Dolar azaltabileceğini önermektedir (Santander Innoventures, Wyman ve Anthemis, 2015: 15).

Gelişimin ve düzenlemenin kullanılmasını etkileyebilecek faktörleri göz önünde bulundurmak ve bu faktörleri belirtmek önemlidir. Bazı düzenlemeler tek bir grubu veya küçük bir grup birimini etkilemektedir. Diğer düzenlemeler ise yaygın kabul görmeyi gerektirir çünkü potansiyel verimlilik kazançları ve diğer faydalar ağ boyutuna bağlı olabilmektedir. Diğer bir deyişle sektörün herhangi bir potansiyel verimlilik kazanımı gerçekleştirebilmesi için düzenlemeye katılan kritik bir kitleye[44] ihtiyaç duyulabilmektedir. Buna ek olarak uygulamalarda, piyasa sözleşmeleri ve uygulamalarında yapılan değişiklikler de dahil olmak üzere pazarda daha temel ve yapısal değişiklikler gerektirebilir. Bu düzenlemenin oluşturulmasında aşağıda belirtilen çevresel, teknolojik ve mali faktörler, rol oynayabilir. Etkili bir uygulama için kilit faktörler;

• *Çevresel faktörler:* yeni teknolojilerin kurumsal olarak kabul görmesi, boyut, piyasa yapısı ve uygulamaları, düzenleyici, hukuki koşullar ve endüstri koordinasyon seviyesi gibi piyasa faktörlerini kapsamaktadır.

• *Teknolojik faktörler:* teknolojinin olgunluğu, mevcut sistemler ve süreçler ile birlikte çalışabilirliği gibi hususlar, teknolojik adaptasyonda karşılaşılan unsurlardır.

• *Mali faktörler:* Maliyet tasarrufu, gelir potansiyeli veya her ikisi ile daha iyi yatırım getirisi sunan projelerin, kurumlar ve pazarlar tarafından benimsenmesi daha olasıdır (BIS, 2017: 11).

Blok zinciri devrimi bir gecede gerçekleştirilemeyecektir, piyasa katılımcıları, düzenleyiciler ve teknologlar[45] arasında işbirliği gerektirmektedir. Diğer bir deyişle blok zinciri teknolojisinin tam potansiyeli ancak katılımcılar, düzenleyiciler ve teknologlar arasındaki işbirliği yoluyla ortaya çıkarılabilir ve dolayısıyla bu süreç biraz zaman alabilir. Gelişmekte olan ülkelerde bankalar ve diğer finansal piyasa katılımcıları

[44] Kritik kitle; ağ etkisi oluşturmak için gerekli kaynak miktarı.
[45] Teknolog; belirli bir teknoloji alanında uzman.

zorluklar yaşayabilirler. Blok zinciri kullanımı varlıkların sayısallaştırılması, varlıkların yerleştirilmesi, konum takibi ve bilgi işlem gücü gibi konular ile yakından ilgilidir. Bankalar, yasal ve operasyonel protokoller ile pazar zorlukları, piyasaya sürülme, geçiş ve birlikte işlerlikle ilgili sorunların yanı sıra, giderlerin oluşturacağı baskı, teknoloji tasarımı ve kültürel dirençle ilgili engeller ile karşı karşıya kalacaklardır (McKinsey, 2015: 2-3). İlk bakışta, blok zinciri teknolojik uygulamalarının merkezi olmayan, şifrelenmiş, kendi kendini yürüten karakteri ve kendini düzenleyici yaklaşımından dolayı prensip olarak geleneksel yasal araçlar gibi faaliyet göstermesi beklenmektedir. Verilerin akışına rehberlik etmek ve yardımcı olmak için daha az denetim noktası olacaktır. Dağıtılmış kayıtların şu anda sorumlulukları ve yükümlülükleri ile görevlendirilmesi için gerekli olan tüzel kişilikten yoksun olması nedeniyle, akıllı sözleşmelerin yasal uygulanabilirliği, sorumluluk ve hesap verebilirlik konuları gibi dikkate alınması gereken çeşitli hususlar da bulunmaktadır. Bu konu, blok zinciri tabanlı uygulamaların uluslararası faaliyet göstermesi nedeniyle daha da zorlaşmaktadır. Global geçerlilik ve farklı zorluklar nedeniyle akıllı sözleşmeler henüz karmaşık işlemleri gerçekleştiremeyebilir (Boucher, Nascimento ve Kritikos, 2017: 23).

Dünya Ekonomik Forumu (WEF) Yazılım ve Hizmetler alanında Küresel Gündem Konseyi, Mart 2015'te Teknoloji Kırılma Noktaları ve Toplumsal Etki anketi gerçekleştirmiştir. Anket, önceki aylardaki tartışmalara dayanarak, katılımcılardan, 21 kırılma noktası hakkında, belirli teknolojik kaymaların toplum üzerindeki etkileri ile ilgilenmektedir. Anket, iletişim ve bilgi teknolojileri sektöründen 800'den fazla yöneticinin ve uzmanın katıldığı bir topluluğun anlık beklentilerini ve bu kırılma noktalarının ne zaman oluşacağına ilişkin algılarını araştırmayı amaçlamıştır. Toplamda 816 adet yanıt alınmıştır (WEF, 2015: 4).

Blok zinciri teknolojisinde depolanan kıymetlerin değerinin, küresel gayri safi yurtiçi hasılanın (GSYİH) oranının 2027 yılında % 10 olması hakkındaki beklentileri sorulmuş ve katılımcıların% 58'i bu kırılma noktasının 2025 yılında gerçekleşmesini beklediklerini beyan etmişlerdir. Beklentiler, Bitcoin ve dijital para birimlerinde, güvenilir işlemlerin dağılmış biçimde takip edilmesinin bir yöntemi olan "blok zinciri" dağıtılmış güven mekanizması fikrine dayanmaktadır.
Blok zincir sistematiğinin muhtemel olumlu etkileri ise şöyle özetlenebilir:

- Blok zincirindeki finansal hizmetler alanında kritik kitleyi elde ettiğinden, gelişmekte olan piyasalarda finansal katkının artması beklenebilir.
- Mali kurumların aracılıktan çıkarılması, yeni hizmetler ve değer değişimlerinin doğrudan blok zincirinde oluşturulması mümkün olabilir.
- Her çeşit değer değişiminin blok zincirinde gerçekleştirilebilmesi nedeniyle, ticari niteliğe sahip özellikli varlıkların sayısında artış yaşanabilir.
- Gelişmekte olan piyasalarda daha gelişmiş mülkiyet kayıtları ve her şeyi ticarete açık bir varlık olarak kullanma becerisi artabilir.
- Blok zincirinin esas olarak tüm işlemleri saklayan genel bir kayıt olarak şeffaflığı artırması beklenebilir.

Ayrıca, aynı ankete katılan katılımcıların %73'ü bir hükümet tarafından blok zinciri sistemi kullanılarak vergilerin ilk kez 2023 yılında toplanmasını beklemektedir. Blok zinciri, ülkeler için hem fırsatlar hem de zorluklar oluşturmaktadır. Bir yandan, herhangi bir merkez bankası tarafından denetlenmeyen ve denetlenemez olması, para politikası üzerinde daha az kontrol anlamına gelmektedir. Bundan dolayı, merkez bankaları, para politikalarını gözden geçirmek zorunda kalacaklardır. Öte yandan, blok zincirinde yer alacak yeni vergilendirme mekanizmaları (örneğin, küçük bir işlem vergisi) buna olanak sağlayacaktır (WEF, 2015: 23-26).

SONUÇ

Blok zinciri birçok alanda olduğu gibi, özellikle de elektronik ödemeler alanında büyük fırsatlar sunmaktadır. Bununla birlikte, bugünden yarına büyük bir değişim ve piyasa entegrasyonu beklenmemelidir. Elektronik ödemeler alanındaki faydası sadece işlem maliyetlerini azaltması değildir. Blok zinciri, kullanıcıların elektronik ödemelere olan güvenini artırabilir ve transfer işlemlerinin yasal durumunu, merkezi makamların rolünden dolayı belirsiz hale getirilebilir. Dağıtık kayıt teknolojisi, yeni finansal hizmetler altyapısı ve süreçlerinin oluşturulması hususunda, kolaylığı ve verimliliği artırmak için büyük potansiyele sahiptir. Blok zincirinin kullanıldığı her alanda tüm sorunları bertaraf etmesi beklenmemelidir, yeni nesil ademi merkezi ve dağıtık finansal hizmetler altyapısının temelini oluşturacak bir yapı olarak görülmelidir.

Finansal alanda elektronikleşme ya da dijitalleşme, otoriteleri, kuruluşları ve kullanıcıları etkileyen en önemli faktör olarak birçok açıdan önem arz etmektedir. Elektronik ödemeler alanında faaliyet gösteren, pazar payını korumak ve yükseltmek isteyen kuruluşlar yenilik yapma baskısı altında olacaktır. Kripto para yapıları ile blok zinciri bir yeniliğin kabul edilmesi için gerekli argümanları sağlamaktadır. DLT ve blok zinciri teknolojileri bilindik ya da farklı yapılarda, finansal ve diğer piyasalarda kalıcı olarak kullanılacaklardır. Blok zinciri teknolojisine dayalı kripto paralar, yaygın kullanımına rağmen birçok otorite tarafından hala belirgin olarak düzenlenememiştir. Kripto paranın yasal durumu otoriteler tarafından sürekli güncellenirken, kripto paranın kullanımına izin veren ve vermeyen ülkelerin sayısı da her geçen gün artmaktadır.

Önceki para sistemlerinin ve mevcut ekonomik yapıların bir eleştirisi olarak ortaya çıkan blok zinciri sistematiği, önümüzdeki dönemde özellikle elektronik ödeme sistemleri olmak üzere çok farklı alanda önemli teknolojik gelişmelere, değişikliklere ve yeniliklere yol açabilecektir. Elbette her yeni uygulamanın ve gelişmenin beraberinde çok farklı avantajlar ve dezavantajlar getirme potansiyeli yadsınamaz bir gerçektir.

Finans ile teknolojinin etkileşiminin çok disiplinli yapıda olması, üreticiler, kullanıcılar ve düzenleyici otoriteler arasında kuvvetli işbirlikleri gerektirmektedir. Elektronik ödemeler alanında olgunlaşan kripto para ve blok zinciri teknolojisi hakkında yapılacak akademik çalışmalar, bu alanda farkındalığı artırarak finansal okuryazarlığı geliştirecektir. Hükümetler ve uluslararası politikalar açısından gerçekleştirilecek akademik incelemeler, yasal statülerini daha belirgin hale getirecektir. Dünyanın çeşitli üniversitelerinin akademik programlarına dağıtık sistemler ve blok zinciri teknolojisi dahil edilmektedir. Blok zinciri teknolojisinin akademik programlarda yer alması bilgi ve teknolojinin gelişmesini, aktarılmasını, oluşan talebin karşılanması gibi alanlarda fayda sağlayacaktır.

Blok zincirinin kullanımının artması ile ortaya çıkan veriler, ölçülebilmesi ile ekonomik analizler yapılmasını mümkün kılacaktır. Kripto paraların ekonomik etkileri gibi birçok anlamda araştırma imkanı sunmaktadır. Elektronik ödemeler, ICO yapıları ve farklı kullanım alanları üzerine gerçekleştirilebilecek araştırmalar için geniş olanaklar sunacaktır.

KAYNAKÇA

Akel, V. (2006). *Finansal Yenilikler ve Risk Yönetimi Tekniklerinin Finansal Gelişmişlik Üzerine Etkileri*. Kayseri: Erciyes Üniversitesi. Erişim tarihi: Mayıs, 2017, Erişim adresi: http://iibf.erciyes.edu.tr/akademi/mh/vakel/veli_akel/finansal-_yenilik_gelisme.pdf.

Antonopoulos, A. M. (2014). *Mastering Bitcoin* (Early Rele). Sebastopol: O'Reilly Media, Inc.

Arner, D. W. (2016). FinTech: Evolution and Regulation. *Hong Kong: Asian Institute of International Financial Law University of Hong Kong*. Erişim adresi: http://law.unimelb.edu.au/__data/assets/pdf_file/0011/1978256/D-Arner-FinTech-Evolution-Melbourne-June-2016.pdf.

bafin.de. (2017). BaFin - Blockchain technology - Blockchain technology. Erişim tarihi: Ağustos, 2017, Erişim adresi: https://www.bafin.de/EN/Aufsicht/FinTech/-Blockchain/blockchain_artikel_en.html.

Balcısoy, E. (2017). *Yüksek Performanslı Bitcoin Madenciliği İçin Sha256 Özet Algoritmasının Eniyilenmesi*. Ankara: TOBB Ekonomi ve Teknoloji Üniveritesi. Erişim adresi: https://tez.yok.gov.tr/UlusalTezMerkezi/.

Baliga, A. (2017). Understanding Blockchain Consensus Models. *Santa Clara*: *Persistent Systems Ltd.*, (April), 1–14. Erişim adresi: https://www.persistent-.com/wpcontent/uploads/2017/04/WP-Understanding-Bloc-kchain-Consensus-Models.pdf.

Bank of England. (2017). Digital Currencies | Bank of England. Erişim tarihi: Haziran, 2017, Erişim adresi: http://www.bankofengland.co.uk/research/Pages/onebank/-cbdc.aspx.

Baran, P. (1962). *On Distributed Cominications Networks*. *The Rand Corporation* (Vol. 1). Santa Monica. Erişim adresi: http://pages.cs.wisc.edu/~akella/CS740/F08/740-Papers/Bar64.pdf.

Barberis, J., vd. (2016). *The FinTech Book*. (J. Barberis & S. Christi, Eds.) (1. Baskı). Cornwall: Wiley's ebook EULA.

Baron, J., Mahony, A. O., Manheim, D., & Dion-schwarz, C. (2015). *National Security Implications of Virtual Currency*. Santa Monica: RAND Corporation.

Bech, M., & Garratt, R. (2017). Central Bank Cryptocurrencies. *BIS Quarterly Review*, 16. Basel: BIS Media. Erişim adresi: http://www.bis.org/publ/qtrpdf/r_qt1709f.-htm#d1.

Biondi, D., Hetterscheidt, T., & Obermeier, B. (2016). *Blockchain in the financial services industry*. Erişim adresi: https://www.hpe.com/h20195/v2/GetPDF.a-spx/4AA6-5864ENW.pdf.

BIS, & Committee on Payments and Market Infrastructures Statistics on Payment, C. and S. S. in the C. countries. (2015). Digital currencies, (December). Basel: BIS Media. Erişim adresi: http://www.bis.org/cpmi/publ/d137.htm.

BIS, & Committee on Payments and Market Infrastructures. (2017). Distributed Ledger Technology in Payment, Clearing And Settlement: An analytical framework, (February), 29. Basel: BIS Media.

bitcoin.it. (2017). Blockchain – Bitcoin Wiki. Erişim tarihi: Haziran, 2017, Erişim adresi: https://bitcoin.it/wiki/Main_Page.

bitcoincore.org. (2017). Bitcoin Core :: Bitcoin. Erişim tarihi: Ağustos, 2017, Erişim adresi: https://bitcoincore.org/.

bitcoin.org. (2009). Bitcoin - Open Source P2P Money. Erişim tarihi: Haziran, 2017, Erişim adresi: https://bitcoin.org/.

bitnodes.21.co. (2017). Global Bitcoin Nodes Distribution - Bitnodes. Erişim tarihi: Ağustos, 2017, Erişim adresi: https://bitnodes.21.co/.

blockchain.info. (2017). Erişim tarihi: Mayıs, 2017, Erişim adresi: https://-blockchain.info/charts.

blockgeeks.com. (2015). Guides Archive - Blockgeeks. Erişim tarihi: Haziran, 2017, Erişim adresi: https://blockgeeks.com/guides/.

Boucher, P., Nascimento, S., & Kritikos, M. (2017). How blockchain technology could change our lives, 28. Brussels: European Parliamentary Research Service. Erişim adresi: https://doi.org/10.2861/926645.

Buterin, V. (2014). Vitalik Buterin - Ethereum Blog. Erişim tarihi: Ağustos, 2017, Erişim adresi: https://blog.ethereum.org/author/vitalik-buterin/.

Buterin, V. (2014). Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform. *Etherum*, (January), 1–36. Erişim tarihi: Haziran, 2017, Erişim adresi: https://github.com/ethereum/wiki/wiki/White-Paper.

Cangürel, O., Güngör, S., Sevinç, V. U., Kayci, I., & Atalay, S. (2010). Sorularla Basel III. İstanbul: BDDK Risk Yönetimi Dairesi. Erişim adresi: www.bddk.org.tr.

coinatmradar.com. (2017). Bitcoin ATM Map – Find Bitcoin ATM, Online Rates. Erişim tarihi: Ağustos, 2017, Erişim adresi: https://coinatmradar.com.

coinhills.com. (2017). CNY Strength vs USD - Statistics - Coinhills. Erişim tarihi: Ağustos, 2017, Erişim adresi: https://www.coinhills.com/statistics/volume-cny-strength/.

coinmarketcap.com. (2017). CryptoCurrency Market Capitalizations. Erişim tarihi: Haziran, 2017, Erişim adresi: https://coinmarketcap.com/.

computinghistory.org.uk. (2017). Computing History - The UK Computer Museum - Cambridge. Erişim tarihi: Ağustos, 2017, Erişim adresi: http://www.computing-history.org.uk/.

Czepluch, Lollike, Beck, & Malone. (2016). Blockchain – the Gateway To Trust-Free Cryptographıc Transactıons. In Czepluch & Lollike (Eds.), *Twenty-Fourth European Conference on Information Systems (ECIS)* (pp. 0–14). İstanbul: Researchgate. Erişim adresi: https://www.researchgate.net/publication/302589-859_Blockchaın_-_The_Gateway_To_Trust-Free_Cryptographıc_Transacti ons?enrichId=rgreq-7799d9d300fcd0bbef33c0b9d0-6d2d2dXXX&enrichSource=-

Y292ZXJQYWdlOzMwMjU4OTg1OTtBUzozNjAxNjQxNDMxOTAwMThAMTQ2Mjg4MTIzMTYyMg%3D.

Çarkacıoğlu, A. (2016). Kripto-Para Bitcoin. Ankara: Sermaye Piyasası Kurulu Araştırma Dairesi Araştırma Raporu. Erişim tarihi: Mayıs, 2017, Erişim adresi: http://spk.gov.tr/yayingoster.aspx?yid=1130&ct=f&action=down-loadfile.

digiconomist.net. (2017). Bitcoin Energy Consumption Index - Digiconomist. Retrieved October 9, 2017, Erişim tarihi: Eylül, 2017, Erişim adresi: https://digiconomist.-net/bitcoin-energy-consumption#assumptions.

EBA, & Authority, E. B. (2014). EBA Opinion on Virtual Currencies. *European Banking Authority*, (EBA/Op/2014/08). Erişim tarihi: Mayıs, 2017, Erişim adresi: https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion-+on+Virtual+Currencies.pdf.

ECB, (2012). *Virtual Currency Schemes*. *European Central Bank*. Frankfurt am Main: European Central Bank. Erişim adresi: https://doi.org/ISBN: 978-92-899-0862-7.

ECB, (2015). *Virtual Currency Schemes – A Further Analysis*. Frankfurt am Main: European Central B. Erişim adresi: https://doi.org/http://doi.org/10.2866/662172.

ECB, & Draghi, M. (2017). Letter from the ECB President to Mrs Paloma López Bermejo and Mr Manuel Viegas, MEPs, on Virtual Currency Schemes, 2. Erişim tarihi: Temmuz, 2017, Erişim adresi: https://www.ecb.europa.eu/pub/pdf/-other/ecb.mepletter170720_bermejo_viegas.en.pdf?058f01ea6d1274e17f44c32ab8c084dd.

ecb.europa.eu, (2015). What is Money?. Erişim tarihi: Ağustos, 2017, Erişim adresi: https://www.ecb.europa.eu/explainers/tell-me-more/html/what_is_money.en.html.

ESMA, & European Securities and Markets Authority. (2016). *The Distributed Ledger Technology Applied to Securities Markets* (2016 No. 773). Paris.

ethereum.org. (2017). What is Ether. Erişim tarihi: Ağustos, 2017, Erişim adresi: https://ethereum.org/ether.

etherscan.io. (2017). Ethereum Average BlockTime Chart. Erişim tarihi: Haziran, 2017, Erişim adresi: https://etherscan.io/chart/blocktime.

European Comission, & Union, T. E. P. A. T. C. O. T. E. (2009). Directive 2009/110/EC (E-Money Directive). *Strasbourg: Official Journal of the European Union*, 7–17.

europeanpaymentscouncil.eu. EPC, (2016). Results of the EPC Poll on the Impact of Blockchain on Payments | European Payments Council. Retrieved September 14, 2017, Erişim adresi: https:-//www.europeanpaymentscouncil.eu/newsinsights-/news/results-epc-poll-impact-blockchain-payments.

FED, & Powell, J. H. (2017). *Innovation, Technology, and the Payments System*. New Haven: Board of Governors of the Federal Reserve System at Blockchain: The Future of Finance and Capital Markets? The Yale Law School Center for the Study

of Corporate Law Weil, Gotshal & Manges Roundtable Yale University. Erişim adresi: https://www.federalreserve.gov/newsevents/speech/powell-20170303a.htm.

Firpo, J. (2009). E-Money – Mobile Money – Mobile Banking – What's the Difference? | Private Sector Development. Erişim tarihi: Mayıs, 2017, Erişim adresi: http://-blogs.worldbank.org/psd/e-money-mobile-money-mobile-banking-what-s-the-difference

Geiling, L. (2016). BaFin - Expert Article: Distributed Ledger - The technology behind virtual …. *BaFin*. Bonn: BaFin Journal. Erişim adresi: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2016/fa_bj_1602_blockchain_en.html;jsessionid=3C3E7EEFDCFCB24FF06EDD830CB4D35D.1_cid381?nn=8249098#doc7860066bodyText2.

GOS, (Government Office of Science), (2015). Distributed Ledger Technology: Beyond Block Chain. London: *Government Office for Science*, 1–88. Erişim adresi: https://www.gov.uk-/government/publications/distributed-ledger-technology-blackett-review.

Gronbaek, H. (2016). *Blockchain 2.0, Smart Contracts and Challenges* (June/July 2016). Erişim adresi: https://www.twobirds.com/en/news/articles/2016/uk/blockchain-2-0--smart-contracts-and-challenges.

Guo, Y., & Liang, C. (2016). Blockchain Application and Outlook in The Banking İndustry. *Financial Innovation, 2*(1), 12. Xiamen: Xiamen University School of Economics. Erişim adresi: https://doi.org/10.1186/-s40854-016-0034-9.

Gupta, V. (2017). A Brief History of Blockchain. Brighton: Harvard Business School Publishing. Erişim tarihi: Haziran, 2017, Erişim adresi: https://hbr.org/2017/02/a-brief-history-of-blockchain.

Harm, J., Obregon, J., & Stubbendick, J. (2016). *Ethereum vs. Bitcoin*. Omaha: Creighton University.

hashgenerator.de. (2017). hashgenerator.de - Generate Md4 Md5 Sha1 Sha256 Sha512 Ripemd and Whirlpool Hashes on the Fly. Erişim tarihi: Mayıs, 2017, Erişim adresi: http://hashgenerator.de.

Holotiuk, F., Pisani, F., & Moormann, J. (2017). *The Impact of Blockchain Technology on Business Models in the Payments Industry*. *WI 2017 Proceedings*. Frankfurt am Main: Frankfurt School of Finance & Management ProcessLab.

Hong Kong Monetary Authority. (2016). *Whitepaper On Distributed Ledger Technology*. Hong Kong: Hong Kong Monetary Authority. Erişim adresi: http://www.hkma.gov.hk/media/eng/doc/-key-functions/finanicalinfrastructure/-Whitepaper_On_Distributed_Ledger_-Technology.pdf.

HSBC, (2017). *Trust in Technology*. *Journal of Interactive Marketing*. Erişim adresi: http://www.hsbc.com/~/media/hsbc-com/newsroomassets/2017-/pdfs/170609-updated-trust-in-technology-final-report.pdf.

Hyperledger Whitepaper, & Linux Fundation. (2016). *Hyperledger Whitepaper v2.0.0*. Erişim adresi: https://github.com/hyperledger/hyperledger/wiki/Whitepaper-WG.

hyperledger.org. (2016). Hyperledger – Blockchain Technologies for Business. Erişim tarihi: Ağustos, 2017, Erişim adresi: http://hyperledger.org/.

Hyperledger Fabric, (2017). *hyperledger-fabricdocs Documentation* (v0.6). Erişim tarihi: Ağustos, 2017, Erişim adresi: http://hyperledger.org/.

Iansiti, M., & Lakhani, K. R. (2017). The Truth About Blockchain. Brighton: Harvard Business School Publishing. Erişim tarihi: Haziran, 2017, Erişim adresi: https://hbr.org/2017/01/the-truth-about-blockchain.

IMF, IMF Staff., He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., … Jagatsing, K. (2016). Virtual Currencies and Beyond: Initial Considerations Internatıonal Monetary Fund Monetary and Capital Markets, Legal, and Strategy and Policy Review Departments Virtual Currencies and Beyond: Initial Considerations. *IMF*. Erişim adresi: https://www.imf.org/external-/pubs/ft/sdn/2016/sdn1603.pdf.

imf.org. (2017). Special Drawing Right SDR. Erişim tarihi: Ağustos, 2017, Erişim adresi: http://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/14/51/Special-Drawing-Right-SDR.

info.cern.ch/. (1991). info.cern.ch. Erişim tarihi: Ağustos, 2017, Erişim adresi: http://info.cern.ch/.

Kar, A. K. & Dey, S.K. (2014). Cryptography in the Banking Industry. *Researchergate*, *1*(1), 1–7. Erişim adresi: https://doi.org/10.13140/2.1.2289.8242.

Kuzu, Y. (2003). *Türkiye Cumhuriyet Merkez Bankaslnda Uluslararasl Elektronik Finansal İletişim & Yurt Dlşl Ödeme Sistemleri İle İlişkiler*. Ankara: TCMB Genel Md. Erişim adresi: http://www3.tcmb.gov.tr/kutuphane/TURKCE/tezler/yasemin-kuzu .pdf.

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, *4*(3), 382–401. Erişim adresi: https://doi.org/10.1145/357172.357176.

Lanka Business Online, Akmeemana, C. & Stubbs, E. (2016). Opinion: Blockchain, Cryptoeconomics, and the Disintermediation of Trust – Lanka Business Online. Erişim tarihi: Haziran, 2017, Erişim adresi: http://www.lankabusinessonline.com-/opinion-blockchain-cryptoeceonomics-and-the-disintermediation-of-trust/.

ledracapital.com. (2017). Bitcoin Series 24: The Mega-Master Blockchain List — Ledra Capital. Erişim tarihi: July, 2017, Erişim adresi: http://ledracapital.com/-blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list.

McKinsey & Company, Buehler, K., Chiarella, D., Akash, L., Lemerle, M., Moon, J., & Heidegger, H. (2015). *Beyond the Hype : Blockchains in Capital Markets* (No. 12). *McKinsey & Company*. New York: *McKinsey & Company* Global Corporate & Investment Banking Practice.

METI. (2017). Evaluation Forms for Blockchain-Based Systems. *Information Economy Division Commerce and Information Policy Bureau*, (April 2017), 0–21. Tokyo: Ministry of Economy, Trade and Industry.

Mills, D., Wang, K., Malone, B., Ravi, A., Marquardt, J., Chen, C., … Baird, M. (2016). Distributed Ledger Technology in Payments, Clearing, and Settlement.

Finance and Economics Discussion Series, *2016*(95), 1–36. Washington: Board of Governors of the Federal Reserve System, Erişim adresi: https://doi.org/10.17016/FEDS.2016.095.

Mises, L. Von. (1912). *The Theory of Money and Credit*. New Heawen: *Yale University Press*. Erişim adresi: https://mises.org/sites/.../The Theory of Money and Credit_3.pdf.

Moore, G. (1991). *Crossing The Chasm*. *HarperCollins Publishers PerfectBound™*. (Vol. 1). HarperCollins & Publishers PerfectBound™. Erişim adresi: https://doi.org/10.1073/pnas.0703993104.

Mougayar, W. (2015). Understanding the Blockchain. Sebastopol: O'Reilly Media, Inc. Erişim tarihi: Haziran, 2017, Erişim adresi: https://www.oreilly.com/-ideas/understanding-the-blockchain.

Müller, C., & Hasic, D. (2016). *Blockchain : Technology and Applications*. Salzburg: University of Salzburg Department of Computer Sciences.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. *Journal for General Philosophy of Science*. Erişim adresi: https://bitcoin.org/bitcoin.pdf.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2015). *Bitcoin and Cryptocurrency Technologies*. *Princeton University*. Princeton: Princeton University. Erişim adresi: http://www.the-blockchain.com/docs/Princeton Bitcoin and Cryptocurrency Technologies Course.pdf.

Network Associates, (1999). *An Introduction to Cryptography*. *Network Associates, Inc.* (1st ed., Vol. 1). Santa Clara: Network Associates, Inc. Erişim adresi: https://courses.cs.vt.edu/cs5204/fall09kafura/Papers/Security/IntroToCryptography.pdf.

OECD, (2016). *OECD Science, Technology and Innovation Outlook 2016*. Paris: OECD Publishing. Erişim adresi: https://doi.org/http://dx.doi.org/10.1787/sti_in_outlook-2016-en.

oxforddictionaries.com. & Oxford University Press. (2017). English Dictionary, Thesaurus, & Grammar Help | Oxford Dictionaries. Erişim tarihi: Haziran, 2017, Erişim adresi: https://en.oxforddictionaries.com/.

Parasız, I. (2005). *Para Banka & Finansal Piyasalar* (8. Baskı.). Bursa: Ezgi Kitabevi.

Pinna, A., & Ruttenberg, W. (2016). *Distributed Ledger Technologies in Securites Post-Trading*. *European Central Bank: Occasional Paper Series*. Frankfurt am Main. https://doi.org/10.2866/270533.

Resmî Gazete. (2013). Başbakanlık Mevzuatı Geliştirme & Yayın Genel Müdürlüğü Ödeme & Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri & Elektronik Para Kuruluşları Kanun No. 6493. 27 Haziran 2013 Tarihli ve 28690 Sayılı Resmî Gazete. Erişim tarihi: Haziran, 2017, Erişim adresi: http://www.resmigazete.gov.tr-/-eskiler/2013/06/20130627-14.htm.

Ripple, Rapoport, P., Leal, R., Griffin, P., & Scully, W. (2014). Ripple Protocol: A Deep Dive for Finance Professionals, (November), 1–47. San Francisco: Ripple Labs. Erişim adresi: http://www.the-blockchain.com/docs/Ripple Protocol - Deep Dive For Financial Professionals.pdf.

Santander Innoventures, Wyman, & Anthemis. (2015). The Fintech 2.0 Paper: rebooting financial services, 20. Erişim adresi: http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf.

shattered.io. (2017). SHAttered. Erişim tarihi: Haziran, 2017, Erişim adresi: shattered.io.

Statista & The Radicati Group, I. (2017). Number of Active E-Mail Accounts Worldwide 2019. Statistic. Erişim tarihi: Ağustos, 2017, Erişim adresi: https://www.statista.-com/statistics/456519/forecast-number-of-active-email-accounts-worldwide/.

Statista.com. (2017). Statista - The Statistics Portal for Market Data, Market Research and Market Studies. Erişim tarihi: Ağustos, 2017, Erişim adresi: https://www.-statista.com/.

Stevens, M., Bursztein, E., Karpman, P., Albertini, A., & Markov, Y. (2017). The First Collision for Full SHA-1, 1–23. Erişim adresi: https://doi.org/10.1007/978-3-319-63688-7_19.

Swan, M. (2015). *Blockchain Blueprınt For A New Economy*. (Tim McGovern, Ed.) (1. Baskı). Sebastopol: O'Reilly Media, Inc.

SWIFT Institute, Mainelli, M., & Milne, A. (2016). *The Impact and Potential of Block chain on the Securities Transaction Lifecycle* (No. 2015–007 THE). *Swift Institute Working Paper* (Vol. 2015–7).

swift.com. (2017). 22 Additional Global Banks Join the SWIFT Gpi Blockchain Proof of Concept | SWIFT. Erişim tarihi: Haziran, 2017, Erişim adresi: https://www.swift.com/news-events/press-releases/22-additional-global-banks-join-the-swift-gpi-blockchain-proof-of-concept.

T.C. Dışişleri Bakanlığı Tercüme Dairesi Başkanlığı. (2015). *Economy & Fınance Terms, Ekonomi & Maliye Terimleri*. Ankara: T.C. Dışişleri Bakanlığı. Erişim tarihi: Mayıs, 2017, Erişim adresi: http://www.mfa.gov.tr/data/Terminoloji/-ekonomi-ve-maliye-terimleri-listesi-110615.pdf.

TCMB. *Terimler Sözlüğü*. Ankara:TCMB. Erişim tarihi: Mayıs, 2017, Erişim adresi: http://www.tcmb.gov.tr/wps/wcm/connect/TCMB+TR/TCMB+TR/Bottom+Menu/Egitim-Akademik/Terimler+Sozlugu/.

TCMB. (2014). *Ödeme Sistemleri Türkiye'de Ödeme Sistemleri* (1st ed.). Ankara: Türkiye Cumhuriyet Merkez Bankası İdare Merkezi. Erişim adresi: tcmb.gov.tr.

tcmb.gov.tr. (2017). TCMB. Erişim tarihi: Haziran, 2017, Erişim adresi: http://www.tcmb.gov.tr/wps/wcm/connect/tcmb+tr/tcmb+tr.

The Economist. (2015). The Trust Machine. New York: The Economist Online. Erişim tarihi: Haziran, 2017, Erişim adresi: https://www.economist.com/news/leaders-/21677-198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine.

tradingview.com. (2017). Tradingview - Canlı Borsa & Forex Grafikler. Erişim tarihi: Ağustos, 2017, Erişim adresi: https://tr.tradingview.com/.

thecenter.org. (2016). How encryption works - The Center for Innovative Justice and Technology. Erişim tarihi: Haziran, 2017, Erişim adresi: http://www.thecenter-.org/how -encryption-works/

TDK. (2014). Türk Dil Kurumu. Erişim tarihi: Mayıs, 2017, Erişim adresi: www.tdk.gov.tr.

Uysal, B., Tanrısever, N. H., & Düzel, O. (2003). *Avrupa Birliği Temel Terimler Sözlüğü*. Ankara: Avrupa Birliği Genel Sekreterliği. Erişim adresi: https://-6aafda01-a-2128149d-s-sites.googlegroups.com/a/yuret.com/deniz/turkish/-SOZLUK_BASKI.pdf?attachauth=ANoY7cqxRINb5CUWyZl8sHe3UznYL-ORW_FO_jItR7eB3QDbJYQ0eacsAYW2SuFPMyGqLKgMrjElXZz-f0Lcb0MPm8cHlkNWTOmPZDt7vAu1p-TI53D2qbN5_3qo-zeTzumlX1Yref-xm2SoAgu2_.

Visa Inc. (2017). Visa Inc . Facts & Figures, *Visa Inc.*, *2017*(Ocak). Erişim adresi: https://usa.visa.com/dam/VCOM/global/about-visa/documents/visa-facts-figures-jan-2017.pdf.

WEF, (2015). WEF Survey Report, *Deep Shift: Technology Tipping Points and Societal Impact*. Geneva: World Economic Forum. Erişim adresi: http://www3.weforum-.org/docs/WEF_GAC15_Technological_Tipping_-Points_report_2015.pdf.

WEF, (2016). The Future of Financial Infrastructure. *Part of the Future of Financial Services Series August 2016*, Erişim tarihi: Mayıs, 2017, Erişim adresi: https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitio us -look-at-how-blockchain-can-reshape-financial-services.

WEF White Paper, Tapscott, D., & Tapscott, A. (2017). *Realizing the Potential of Blockchain A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies*. Geneva: World Economic Forum. Erişim adresi: www.-weforum.org.

Wood, G. (2014). *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. *Ethereum Project Yellow Paper*. Erişim adresi: https://doi.org/10.1017/CBO-9781107415324.004.

Lin, J., Fardoust, S., & Rosenblatt, D. (2012). Reform of the International Monetary System: A Jagged History and Uncertain Prospects. *World Bank Policy Research …*, (Mayıs). Erişim adresi: http://papers.ssrn.com/sol3/papers.cfm?-abstract_id=2060827.

Zimmerman, E. (2016). The Evolution of Fintech - The New York Times. Erişim tarihi: Haziran, 2017, Erişim adresi: https://www.nytimes.com/2016/04/07/-business/dealbook/the-evolution-of-fintech.html?mcubz=1.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı, Soyadı: İmparator S. Karaköse

Email: imparatorkarakose@gmail.com

EĞİTİM

Derece	Kurum	Mezuniyet Tarihi
Yüksek Lisans	Erciyes Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı	2017
Lisans	Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi İşletme Bölümü	2015

Yabancı Dil

Almanca, İngilizce