



T.C.

BARTIN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
İŞLETME ANABİLİM DALI

YÜKSEK LİSANS TEZİ

FİNANSTA DAĞITIK DEFTER TEKNOLOJİSİ UYGULAMALARI:
ENGELLER VE FIRSATLAR

BICHARA TOIHA

DANIŞMAN

DR. ÖĞR. ÜYESİ İSMAİL FATİH CEYHAN

BARTIN-2024



T.C.

**BARTIN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
İŞLETME ANABİLİM DALI**

**FİNANSTA DAĞITIK DEFTER TEKNOLOJİSİ UYGULAMALARI: ENGELLER
VE FIRSATLAR**

YÜKSEK LİSANS TEZİ

Bichara TOIHA

JÜRİ ÜYELERİ

Danışman

Üye :

Üye :

BARTIN-2024



BEYANNAME

Bartın Üniversitesi Lisansüstü Eğitim Enstitüsü tez yazım kılavuzuna göre Dr. Öğr. Üyesi İsmail Fatih CEYHAN danışmanlığında hazırlamış olduğum “FİNANSTA DAĞITIK DEFTER TEKNOLOJİSİ UYGULAMALARI: ENGELLER VE FIRSATLAR ” başlıklı yüksek lisans tezimin bilimsel etik değerlere ve kurallara uygun, özgün bir çalışma olduğunu, aksinin tespit edilmesi halinde her türlü yasal yaptırımını kabul edeceğimi beyan ederim.

01.07.2024

Bichara TOIHA



ÖN SÖZ

Bu tez, "Finans Alanında Dağıtık Defter Teknolojisi Uygulamaları: Engeller ve Fırsatlar" konusunu derinlemesine incelemektedir. Bu çalışma boyunca bana destek olan herkese en içten şükranlarımı sunarım.

Öncelikle tez danışmanım İsmail Fatih CEYHAN'a sonsuz teşekkürlerimi sunarım. Kendisinin sabrı, tavsiyeleri ve değerli rehberliği olmasaydı bu çalışmayı tamamlamam mümkün olmazdı. Kendisinin desteği ve uzmanlığı, bu projeyi tamamlamamda ve uzun ve zorlu bir süreç olan bu çalışmanın zorluklarını aşmamda büyük önem taşımaktadır.

Son olarak, iki sevgili anneme, aileme, arkadaşlarıma ve sevdiklerime sonsuz şükranlarımı sunarım. Onların manevi desteği ve anlayışı bu süreç boyunca benim için çok değerliydi.



Bichara TOIHA

ÖZET

Yüksek Lisans Tezi

FİNANSTA DAĞITIK DEFTER TEKNOLOJİSİ UYGULAMALARI: ENGELLER VE FIRSATLAR

Bichara TOIHA

Bartın Üniversitesi

Lisansüstü Eğitim Enstitüsü

İşletme Anabilim Dalı

Tez Danışmanı: Dr. Öğr. Üyesi İsmail Fatih CEYHAN

Bartın-2024, sayfa: 107

İlk uygulamaları yaygın olarak blok zinciri ile olarak bilinen Dağıtık Defter Teknolojisi (DLT), bilginin ağlar arasında nasıl toplandığı, depolandığı ve paylaşıldığı konusunda bir paradigma değişikliğini temsil etmektedir. Ademi merkezîyetçilik, şeffaflık ve güvenlik ile karakterize edilen bu teknoloji, kripto para birimleri ile olan ilişkisini çoktan aşmış ve çeşitli sektörlerde büyük fırsatlar ve önemli zorluklar getirmiştir. DLT tarafından sunulan fırsatlar çok yönlü ve potansiyel olarak dönüştürücüdür. Finans alanında, işlemleri kolaylaştırmayı, maliyetleri düşürmeyi, şeffaflığı ve güvenliğini artırmayı ve potansiyel olarak dünya çapında finansal hizmetlere erişimi vaat etmektedir. Ancak bu fırsatlar karmaşık zorluklarla iç içe geçmiştir. Teknolojik açıdan ölçeklenebilirlik, enerji tüketimi ve mevcut sistemlerle entegrasyon vb. önemli engeller mevcuttur. Özellikle yüksek işlem hacimleri nedeniyle ölçeklenebilirlik sorunları kritik bir zorluk olmaya devam etmektedir. Bazı DLT uygulamalarının, özellikle de iş kanıtı (proof of work) blok zincirlerinin önemli ölçüde enerji tüketimi çevresel kaygıları artırmaktadır. Ayrıca, DLT'yi eski sistemlerle entegre etmek önemli yatırımlar gerektirmekte ve operasyonel zorluklar ortaya çıkarmaktadır.

Düzenleyici kurumların açısından bakıldığında, DLT'nin merkezi olmayan yapısı, tüketicileri korumayı ve yeniliği engellemeden finansal istikrarı sağlamayı amaçlayan yasa koyucular ve düzenleyiciler için karmaşık bir zorluk teşkil etmektedir. Yasal çerçevelerin,

DLT'nin risklerini azaltırken yargı yetkisi, veri gizliliği ve standardizasyon konularını ele alacak şekilde geliştirilmesi gerekir.

Bu araştırma, şeffaflığı, verimliliği ve güvenliğini artırmak için sunduğu derin fırsatları araştırarak, DLT'nin finans sektöründeki çeşitli uygulamalarını incelemektedir. Aynı zamanda, DLT'nin yaygın olarak benimsenmesinin doğasında bulunan teknolojik ve düzenleyici zorlukları eleştirel bir şekilde analiz ederek, bu çığır açan teknolojinin gelecekteki potansiyeline dair görüşler sunmaktadır. Bu araştırma mevcut ve potansiyel uygulamaların kapsamlı bir biçimde incelenmesi ile dengeli bir DLT görünümünü sağlarken karşılaşılan engellerin farkında olmayı amaçlamaktadır.

Anahtar Kelimeler: Blok zinciri, dağıtık defter teknolojisi, engeller ve fırsatlar, finans sektörü, finansal hizmetler, kripto para.

ABSTRACT

M.A. Thesis

DISTRIBUTED LEDGER TECHNOLOGY APPLICATIONS IN FINANCE: CHALLENGES AND OPPORTUNITIES

Bichara TOIHA

Bartın University

Graduate School

Department of Business Administration

Thesis Advisor: Assist. Prof. Dr. İsmail Fatih CEYHAN

Bartın-2024, pp: 107

Distributed Ledger Technology (DLT), commonly known as blockchain, represents a paradigm shift in how information is collected, stored and shared across networks. Characterized by decentralization, transparency and security, this technology has already transcended its association with cryptocurrencies and has brought great opportunities and significant challenges in various sectors. The opportunities offered by DLT are multifaceted and potentially transformative. In finance, it promises to streamline transactions, reduce costs, increase transparency and security, and potentially provide access to financial services worldwide. However, these opportunities are intertwined with complex challenges. From a technological point of view, there are significant barriers such as scalability, energy consumption and integration with existing systems. Scalability issues remain a critical challenge, especially due to high transaction volumes. The significant energy consumption of some DLT applications, especially proof of work blockchains, raises environmental concerns. Furthermore, integrating DLT with legacy systems requires significant investments and poses operational challenges.

From the perspective of regulators, the decentralized nature of DLT poses a complex challenge for legislators and regulators aiming to protect consumers and ensure financial stability without hindering innovation. Legal frameworks need to be developed to address

issues of jurisdiction, data privacy and standardization while mitigating the risks of DLT.

This research examines various applications of DLT in the financial sector, exploring the profound opportunities it offers to enhance transparency, efficiency, and security. It also offers insights into the future potential of this groundbreaking technology by critically analyzing the technological and regulatory challenges inherent in the widespread adoption of DLT. Through a comprehensive examination of current and potential applications, this research aims to raise awareness of the obstacles encountered while ensuring a balanced view of DLT.

Keywords: Barriers and opportunities, blockchain, cryptocurrency, distributed ledger technology, financial sector, financial services.



İÇİNDEKİLER

BEYANNAME	iii
ÖN SÖZ	iv
ÖZET	v
ABSTRACT	vii
İÇİNDEKİLER.....	ix
ŞEKİLLER DİZİNİ.....	xi
TABLOLAR DİZİNİ.....	xii
KISALTMALAR.....	xiii
1. GİRİŞ.....	1
2. LİTERATÜR ÖZETİ.....	3
3. BLOK ZİNCİRİ: ORTAYA ÇIKIŞI VE TEKNOLOJİLERİ.....	17
3.1. Blok Zincirinin Ortaya Çıkışı	17
3.1.1 Bitcoin'in Kökeni	17
3.1.2 Güven Krizi	19
3.2.1 Blok Zinciri: İnternet Üzerinde Değer İşlemlerinin Yeniden Tanımlanması.....	21
3.2.2 Mutabakat Algoritması: İşlem Doğrulama Süreci.....	23
3.2.3 Kriptografi: İşlemleri Güvence Altına Alma Süreci.....	25
3.2.4 Dağıtık Defterlerde Bilgi Paylaşım Süreci	26
3.2.5 Halka Açık Blok Zincirleri ve Özel Blok Zincirleri.....	27
3.2.6 Akıllı Sözleşmeler	29
3.3.1 Blok Zincirlerin Desteklediği Ekonomik İlkeler	32
3.3.2 Blok Zincirlerin Desteklediği Ana İşlevler	33
3.3.3 Blok Zincirinin Faydaları ve Sınırlamaları	34
4. BLOK ZİNCİRİ TEKNOLOJİSİNİN FİNANSAL SİSTEMDEKİ POTANSİYELİ.....	36
4.1 Finansal Piyasalarda Blok Zinciri Uygulamaları	36
4.1.1 Blok Zinciri Tabanlı Bankalar Arası Mutabakatlar	37
4.1.2 Sermaye Piyasalarında Blok Zincirleri.....	44

4.1.3 Gayrimenkulde Blok Zincirleri	51
4.1.4 Ticaret Finansmanında blok Zincirleri.....	58
4.1.5 Blok Zincirle Ticaret Finansman Sistemlerini Geliştirme Örnekleri	63
5. FİNANS ALANINDA BLOK ZİNCİRİ TEKNOLOJİSİ KULLANIMI İLE	
İLGİLİ BAŞLICA ENGELLER VE KISITLAR.....	66
5.1 Blok Zinciri Yanılsaması	67
5.1.1 Blok Zinciri Teknolojisinin Ölçeklenebilirliği ve Performansı.....	69
5.1.2 Gizlilik	73
5.1.3 Birlikte Çalışabilirlik	79
5.1.4 Enerji Tüketimi	80
5.2 Blok Zinciri'nin Güvenlik Eksikliği	84
5.3 Halka Açık Blok Zincirinin Güçsüz Olmasının Nedenleri.....	85
5.3.1 Çözülememiş Problemler	85
5.3.2 Sürdürülebilir Olmayan Bir Ekonomi Modeli	86
5.3.3 Yasalardaki Belirsizlik.....	87
5.4 Düzenlemelere Yönelik Çıkarımlar	87
5.4.1 Düzenleyici Kurumların Endişeleri.....	89
5.5 Geleceğin Teknolojileri Kapsamında Blok Zincirinin Potansiyeli	91
5.5.1 Dağıtık Defter Teknolojisinin Gelecekteki Üç Uygulaması.....	92
6. SONUÇ VE TARTIŞMALAR.....	94
KAYNAKLAR.....	101

ŞEKİLLER DİZİNİ

Şekil	Sayfa
<u>No</u>	<u>No</u>
3.1: Blok zinciri nedir?	23
3.2: Kriptografik güvenliğin açıklaması.....	26
4.1: Ticaret finansmanı;.....	61
5.1: Blok zinciri: öncüllük aşaması	69
5.2: DCS üçgeni	72
5.3: Ülke grafiğine göre enerji tüketimi	82
5.4: Bitcoin ve Visa ağının ortalama tüketimi.....	83



TABLÖLAR DİZİNİ

Tablo	Sayfa
<u>No</u>	<u>No</u>
2.1: Literatür Tablosu	15



KISALTMALAR

ABD	: Amerika Birleşik Devletler
AML	: Kara para aklamayı önleme
BHT	: Byzantine Fault Tolerance (Bizans hata toleransı)
CLS	: Conctinuous Linked Settlement system (Bağlantılı Uzlaştırma Sistemi)
CME	: Chicago Mercantile Exchange
CPU	: Central Proceesing Unity (Merkezi işlem birimi)
DAO	: Decentralized Autonomous Organization (merkezi olmayan otonom bir organizasyon)
DLT	: Distributed Ledger Technology (Dağıtık Defter Teknolojisi)
GAFAM	: Google, Apple, Facebook, Amazon, Microsoft
GDPR	: Genel Veri Koruma Yönetmelik
IBM	: International Business Machines (Uluslararası İş Makineleri)
ICO	: İnitial Coin Offering (İlk Para Arzı teklifi)
IIN	: Interbank Information Network (Bankalararası Bilgi Ağı)
IOTA	: Internet of Things (Nesnelerin İnterneti)
JPM	: John Pierpont Morgan
KYC	: Know Your Customer (Müşterinizi Tanıyın)
NSA	: National Security Agency (Ulusal Güvenlik Dairesi)
P2P	: Peer to Peer (Uçtan Uça Ödeme)
PoW	: Proof of Work (İş İspatı)

1. GİRİŞ

Büyük kâğıt kitapların yaratılmasından bu yana bin yıldan fazla zaman geçmiştir. Yirminci yüzyılın sonunda bilgisayarların kullanılmaya başlanması, kitapların dijitalleştirilmesine yol açmıştır. Sofistike algoritmik sistemlerin ve yüksek hesaplama kapasitelerinin geliştirilmesi sayesinde, kriptografi gibi sistemler sayesinde dağıtılmış defterler gibi daha güvenilir arşivleme sistemleri artık mümkündür (actualitinformatique, 2020). Son yıllarda dağıtık defter teknolojisinin (DLT) ortaya çıkmasıyla birlikte finans sektörü büyük bir dönüşüm geçirmiştir. Yaygın olarak blok zinciri olarak bilinen DLT, finansal işlemlerin kaydedilmesi ve paylaşılması için güvenli ve merkezi olmayan bir yol sunmaktadır (Yves ve Serge, 2016). Bu durum, DLT'nin finans alanındaki uygulamalarına ve bu uygulamaların beraberinde getirdiği zorluklara ve fırsatlara olan ilginin artmasına yol açmıştır.

Geleneksel üçüncü taraflara ve aracılara, kurumlara, bankalara ve hükümetlere karşı güven ve memnuniyetsizlik krizinin yaşandığı bir dönemde, aracılıktan çıkarma ve şeffaflık vaatleriyle blok zinciri teknolojisi baştan çıkarıcı ve ilgi çekicidir (Pignel, 2019). Yıkıcı bir yenilik olan bu teknoloji, güvenilir üçüncü tarafları ortadan kaldırma kabiliyeti nedeniyle küresel bir çılgınlık yaratmakta ve bazen yeni bir dünyanın ideolojik vizyonlarına yol açmaktadır. Dağıtık defter teknolojisine yönelik bu çılgınlığın temelinde, ilkeleri Satoshi Nakamoto'nun beyaz kâğıdına dayanan bu teknolojinin mümkün kıldığı yeni merkezi olmayan işlem modeli yatmaktadır (Nakamoto, 2008).

DLT'nin finans alanındaki potansiyel faydaları sayısızdır. Bir yandan, DLT şeffaf, sahteciliğe karşı dayanıklı bir işlem kaydı oluşturarak dolandırıcılığı ve aracılara olan ihtiyacı azaltır. Bu sonuçta finansal kurumlar için maliyet tasarrufu ve bireyler için daha güvenli işlemlere yol açabilir. Ek olarak, DLT, uzlaştırma ve ticaret mutabakatı gibi süreçleri kolaylaştırma ve otomatikleştirme potansiyeline sahiptir, bu da verimliliğin artmasına ve operasyonel risklerin azalmasına neden olur (Collomb ve Sok, 2017).

Bununla birlikte, DLT'yi finans alanında uygulamak zorlukları olmadan değildir. DLT'yi çevreleyen düzenleyici ortam, düzenleyiciler merkezi olmayan bir şekilde çalışan bir teknolojiyi nasıl denetleyeceklerini merak ettikleri için büyük bir engeldir. Ek olarak, DLT ağlarının yüksek işlem hacimlerini idare edebilmesi ve mevcut finansal sistemlerle sorunsuz

bir şekilde çalışabilmesi gerektiğinden, ölçeklenebilirlik ve birlikte çalışabilirlik konusunda endişeler vardır (URL-7, 2018).

Bu zorluklara rağmen, DLT'nin finans sektöründe sunduğu potansiyel fırsatlar göz ardı edilemeyecek kadar önemlidir. Doğru düzenleyici çerçeveler ve teknolojik çözümler ile DLT, finansal işlemlerin gerçekleştirilme biçiminde devrim yaratma potansiyeline sahiptir. Bu çalışmanın ilk bölümünde blok zinciri teknolojisinin kendisini inceleyeceğiz: ortaya çıkışı, özellikleri, işleyişi ve riskleri; daha sonra finansal sistemdeki blok zinciri teknolojisinin potansiyeline bakacağız ve son bölümde, blok zinciri teknolojisinin sınırlarını ve zorluklarını inceleyeceğiz. Bu sayede, bu teknolojinin finans sektörünün geleceğini nasıl şekillendirebileceğini daha iyi anlayabilmemiz mümkün olacaktır.

Dağıtık defter teknolojisinin çok yakın zamanda ortaya çıkmasından dolayı kullanımıyla ilgili veriler sınırlıdır. Bu nedenle araştırmada bu konuda yapılmış çalışmaların derlenmesi ve düzenli bir sonuca ulaşılması hedeflenmiştir.

Bu araştırmanın veri toplama tekniği dokümantasyondur, yani makalelerden, kitaplardan, web sitelerinden elde edilen kaynaklar kullanılarak tezin amacına yönelik sonuçlar derlenmiştir.

Çalışma literatür bölümünden sonra üç ana bölümden oluşmaktadır:

Birinci bölüm: Blok zinciri: ortaya çıkışı ve teknolojileri

İkinci bölüm: Blok zinciri teknolojisinin finansal sistemdeki potansiyeli

Üçüncü bölüm: Blok zinciri teknolojisi ile ilgili başlıca engeller ve kısıtlar

2. LİTERATÜR ÖZETİ

Birçok dijital kripto para biriminin altında yatan teknolojiye blok zinciri denir. Blok zinciri, verileri dijital imzalarla birlikte depolamak için kullanılan dağıtılmış, merkezi olmayan bir blok ağıdır. Blok zincirinin ademi merkeziyetçilik, değişmezlik, şeffaflık ve denetlenebilirlik gibi özellikleri sayesinde işlemler daha güvenli ve aşılmazdır. Blok zinciri teknolojisi, risk yönetimi, sağlık tesisleri, finansal ve sosyal hizmetler ve daha fazlası dahil olmak üzere kripto para biriminin ötesinde uygulamalara sahiptir. Çok sayıda araştırma çalışması, blok zincirinin bir dizi uygulama alanında sunduğu potansiyele odaklanmaktadır. Bu çalışmada, blok zinciri teknolojisinin taksonomisi ve mimarisinin açıklanmasının yanı sıra, çeşitli mutabakat mekanizmalarının ödünleşimleri karşılaştırılmakta ve ölçeklenebilirlik, gizlilik, birlikte çalışabilirlik, enerji tüketimi ve düzenleyici konular gibi çeşitli zorluklar ele alınmaktadır. Bu çalışma aynı zamanda blok zinciri teknolojisinin potansiyel uygulamalarını da tartışmaktadır (Monrat vd., 2019).

Blok zinciri teknolojisi, geleneksel iş modellerinde ve ticari işlemlere yönelik iş akışlarında devrim yaratan yıkıcı bir teknolojidir. Aynı zamanda iş değerinin birlikte yaratılması için bir olasılıklar dünyası açmıştır. Blok zinciri, bankacılık ve finans sektörü en iyi bilinenlerden biri olmak üzere bir dizi işletme ve sektörü alt üst etme potansiyeline sahiptir. Bu nitel çalışmada bankacılık ve finans sektöründeki en yeni blok zinciri araştırmaları ve teknolojileri incelenmiştir. İlk olarak, 2016-2020 yılları arasında bankacılık ve finans sektöründeki 76 adet literatürü seçip analiz ederek çalışma grubunun eleştirel bir bibliyometrik incelemesini yapılmıştır. En önemli araştırma konularını, beş olası iş avantajını ve bankacılık ve finans sektöründe blok zinciri teknolojisinin uygulanmasıyla ilişkili üç olası zorluk türünü sistematik olarak belirlemek için, ikinci olarak yaygın olarak tanınan tema analizi metodolojisini kullandık. Sonuç bölümünde çalışmanın sınırlılıklarını özetledik ve ardından gelecekteki araştırmalar için alanlar önerdik. Yazarların bildiği kadarıyla, diğer alanlardaki çok sayıda çalışmaya rağmen, bu alandaki blok zinciri uygulamasına ilişkin araştırmaları derleyen kapsamlı bir inceleme bulunmamaktadır. Dolayısıyla bu çalışma gelecekteki araştırmalar için bir temel teşkil etmekte ve akademisyenler ile sektördeki uygulayıcıların işini kolaylaştırmaktadır (Gang vd., 2021).

Yenilikçi blok zinciri teknolojisinin kullanımı, işlem kapasitesinin genişlemesi ve çoklu

kullanımları nedeniyle mümkündür. Bu çalışmanın amacı, finans sektörünün blok zinciri teknolojisini benimsemesinin önündeki engelleri anlamak, metodik çözüm için sınıflandırmak ve bir model halinde düzenlemektir. Blok zinciri benimseme sorunlarını hiyerarşik olarak yapılandırmak ve daha iyi ele almak için Yorumlayıcı Yapısal Modelleme (ISM) ve MICMAC (Matrice d'Impacts Croisés Multiplication Appliquée a un Classement/ Cross Impact Matrix Multiplication Applied to Classification) analizi kullanılmıştır. Zorluklar dört sınıfa ayrılmıştır: özerk, bağımlı, bağlantılı ve bağımsız. Bu çalışmada içerik analizi için NVivo yazılımı da kullanılmıştır. Hiyerarşik zorluk modeli digraf ile temsil edilmektedir. Bağımlı değişkenler, finansal suçlar ve aksaklıklar, gizlilik endişeleri ve jeopolitik gerilimlere karşı sınır ötesi işlem kırılganlıklarıdır. Yeni finansal araçlara duyulan ihtiyaç, denetimin zorluğu, karmaşık mimariyi anlama, kodlama ve düzeltmenin karmaşıklığı ve kurumlar ve düzenleyiciler arasında birleşik yönetim ve koordinasyonun olmaması bağımsız değişkenlerdir. Finans alanında blok zinciri teknolojisinin olumlu bir şekilde benimsenmesini teşvik etmek için paydaşlar, nitel içerik analizi ve digraf tarafından desteklendiği üzere, teknolojinin uygulanmasıyla birlikte gelen birbiriyle ilişkili zorlukları metodik olarak ele almalıdır. Blok zinciri teknolojisini çeşitli finansal alanlarda uygulamak için benimseme engellerinin aşılması gerekmektedir. Bu çalışmayı kullanarak, kuruluşlar kaynaklarını planlayabilir ve blok zinciri teknolojisinin faydalarından tam olarak yararlanmak için bu sorunları sistematik bir şekilde ele alabilirler. Mevcut çalışmanın bulguları, daha hızlı, daha uygun fiyatlı, şeffaf ve güvenli finansal işlemleri kolaylaştıran blok zinciri teknolojisinin yayılmasını destekleyebilir. Ayrıca ekonomiyi canlandıran yeni ve yaratıcı iş modellerinin geliştirilmesini de destekleyebilir. Finans sektörü, teknolojik gelişmelerin bir sonucu olarak muazzam bir dönüşüm geçirmiştir. Blok zinciri teknolojisinin amacı işlem güvenliğini ve şeffaflığını artırmaktır. Finans sektörü kritik blok zinciri zorluklarıyla karşı karşıyadır, ancak hiçbir araştırma bunları hiyerarşik bir şekilde düzenlemek ve kategorize etmek için ISM-MICMAC kullanmamıştır. Buna ek olarak, çalışmada ISM-MICMAC kullanıldığında nadir görülen içerik analizi kullanılmıştır (Banerjee, 2022).

Diğer bir makalenin amacı, Amerika Birleşik Devletleri ve Avrupa Birliği'nin (AB) en yeni dağıtık teknolojiler olan blok zincirleri ile ilgili olarak karşı karşıya olduğu temel düzenleyici sorunları analiz etmektir. Araştırma nitel bir bakış açısına dayanmaktadır. Bu çalışmada, ilgili vaka çalışması içgörülerini de dahil olmak üzere kamusal alandan ikincil veriler ve ilgili tüzüklerden birincil veriler kullanılmaktadır. AB ve ABD, blok zincirlerinin gelecekte

finansal hizmetlere ve ilgili sektörlere yapacağı yenilikçi katkıların yanı sıra daha fazla finansal kapsayıcılık için çoğunlukla iyi bir işaret olan akıllı bir düzenleyici yaklaşım benimsemiştir. Çalışmanın sonuçları, özellikle finansal hizmetler için katma değer ve verimliliği artırmak amacıyla mümkün olan en az düzenleyici kısıtlama ile blok zinciri teknolojisinin ilerlemesini desteklemektedir. Bu da erişilebilirliği ve dolayısıyla finansal kapsayıcılığı artıracaktır. Bu çalışma, sanal para birimlerinin altında yatan teknolojiyi vurgulayarak bu konudaki farkındalığın artırılmasına katkıda bulunmaktadır. Ayrıca blok zinciri gelişiminden kaynaklanan ek finansal fırsatlara da dikkat çekmektedir (Yeoh, 2017).

Bitcoin kripto para birimi, binlerce düğüm arasında dünya çapında mutabakatın değerini göstererek dijital işlemlerin manzarasını tamamen değiştirmiştir. Blok zincirinin ya da olasılıksal iş kanıtı (PoW) tabanlı mutabakat yapısının performansı ilk başlarda Bitcoin için büyük bir problem oluşturmamıştır. Yaklaşık bir saatlik mutabakat gecikmelerine ve saniyede sadece yedi işlemlik teorik zirve verimine rağmen, Bitcoin bir başarı hikayesi haline gelmiştir. Mevcut senaryo geçmişten büyük ölçüde farklıdır ve ilk PoW blok zincirlerinin düşük performansı ve ölçeklenebilirliği artık rasyonel değildir. Daha spesifik olarak, Ethereum gibi kripto para platformlarındaki mevcut eğilim, önemli ölçüde daha yüksek performans gerektiren herhangi bir dağıtılmış uygulamanın bir blok zinciri dokusu üzerinde yürütülmesini sağlamaktır. Bununla birlikte, bu strateji kripto para platformlarını kullanım amaçlarından sapmaya ve veri tabanı replikasyon protokolleri alanına, özellikle de geleneksel durum-makine replikasyonu ve bunun Bizans hata toleranslı (BFT) varyasyonlarına girmeye zorlamaktadır. Ölçeklenebilirlik kısıtlamalarına vurgu yaparak, bu makalede PoW tabanlı blok zincirlerini BFT durum makinesi replikasyonuna dayalı olanlarla karşılaştırmaktadır. "Nihai" blok zinciri yapısının arayışında, çözülmemiş önemli sorunları da özetliyor ve bu ölçeklenebilirlik sınırlarını aşmak için son önerilerden bahsetmektedir (Vukolic, 2016).

Blok zinciri paradigması, birçok kişi tarafından BT alanında birkaç örnek ve zarif dönüşüm getirebilecek yenilikçi ve yıkıcı bir paradigma olarak lanse edilmektedir. İş operasyonları ve teklifleri, BT alanındaki çeşitli önemli başarılar ve ilerlemeler sayesinde büyük ölçüde etkinleştirildiğinden, dünyanın dört bir yanındaki işletme yöneticileri, bir dizi ticari fayda elde etmek için bu yeni ve fütüristik teknolojiyi denemeye ve benimsemeye eşit derecede isteklidir. İlginç bir şekilde, blok zinciri, çeşitli endüstri dikeyleri için stratejik olarak sağlam bir dizi sonuç getirme potansiyeline ve vaadine sahiptir. Kripto para birimi, blok zinciri

teknolojisinin en iyi ve en önde gelen uygulamalarından biridir. Tedarik zinciri alanı, bazı önemli avantajları gerçekleştirmek için bu yeni fenomeni araştırıyor. Lot disiplini, blok zinciri alanında gerçekleştirilen tüm trend belirleyici iyileştirmelerden bir dizi farklı fayda elde edebilen bir diğer disiplindir (Kumar vd., 2021).

Siber uzayın genişlemesinin ilk aşamalarında iki ana faktör birçok insanın interneti kullanma konusunda isteksiz olmasına neden olmuştur: şüphecilik ve belirsizlik. Ancak internet hızla gelişerek, veri bütünlüğü ve gizliliği gibi sorunların ele alınması ihtiyacının çok önemli hale geldiği çeşitli sektörler için tek durak noktası haline geldi. 2008 yılında anonim bir geliştirici ya da geliştirici topluluğu olan Satoshi Nakamoto tarafından yaratılan çevrimiçi bir para birimi olan Bitcoin piyasaya çıkmıştır. Bitcoin'in fiyat ya da devlet tarafından çıkarılan para için iyi bir ikame olabileceğine karar verilmiştir. İşlem verilerinin depolanacağı ve anında işleneceği düğümleri veya "blokları" içeren bir cihaz uygulaması veya basitçe "cüzdan" şeklindeki kullanım kolaylığı ve bunun yanı sıra insanlara işlemlerinin tam sahipliğini verecek ve güvenlik ihlallerine maruz kalmayacak güvenilir bir nakit sistemi yaratma hedefi, Bitcoin'i ünlü ve kolayca uyarlanabilir kılan şeydir. Bitcoin'in tanıtımı ve popüleritesiyle birlikte, Ethereum ve Litecoin gibi diğer kripto para birimlerinin ve dijital varlıkların geliştirilmesi için yeni yollar açılmıştır. Güvene dayalı paranın aksine, anonimliği korunacak herhangi iki taraf arasında dijitalleştirilmiş para alışverişinin kapsamlı ve şeffaf bir kaydın sürdürülebilirliğini gerektireceği belirtilmiştir. Sonunda bu bir dönüm noktası oldu ve zaman damgaları ve karma algoritmalarla güçlendirilen sağlam ve karmaşık kriptografik temeli sayesinde güvenli işlemleri garanti eden dağıtılmış bir defter sistemi olarak çalışan blok zinciri teknolojisinin doğuşunu sağladı. Uygulamanın bir parçası olarak Nakamoto ilk blok zinciri veri tabanı da oluşturdu. Bu teknoloji, tüm işlemlerin bankalar veya ödeme işleme şirketleri gibi aracılara ihtiyaç duymadan eşler arası bir ağda (P2P) birden fazla coğrafya arasında senkronize edilmesine olanak tanıdı. Büyük ilgi gören blok zincirleri, işlemlerin bloklar halinde gruplandırılması ve dağıtık bir ortamda, düğümlerden oluşan bir ağın bu işlemleri fikir birliği ile birbirleriyle değiştirmesi ve doğrulaması temel fikrine dayanmaktadır. Dağıtık bir ağda defter tutarlılığını ve kullanıcı güvenliğini garanti etmek için mutabakat algoritmaları kullanılır. Bu teknolojinin kullanımı zaman içinde sanal para birimlerinin yönetiminin ötesine geçmiştir. Blok zinciri, büyük miktarlardaki kayıt organizasyonu ve depolama sorunlarını ortadan kaldırma ve tedarik zincirlerini optimize etme konusunda akıl almaz bir potansiyel ortaya koyduğu için kesinlikle yapay zekadan bu yana en önemli icattır (Rao ve Saritha, 2022).

Blok zinciri, çevreye dağılmış olan ve yaygın olarak kullanılan bir kamu defteridir. En popüler kullanım alanı Bitcoin'dir. Sistemi tüm saldırılardan koruyan Bitcoin'in Mutabakat mekanizması, başarısının anahtarıdır. Bu, dürüst olmayan hiçbir madencinin zinciri etkileyemeyeceği ve kendi ihtiyaçlarına göre değiştiremeyeceği anlamına gelir. Ayrıca, bu ağda üçüncü bir tarafa güvenmeye gerek yoktur ve çifte harcama sorunu yoktur. Yalnızca madencilerin işlem kapasitesine dayanan Proof-of-Work (PoW), Bitcoin teknolojisinde en yaygın kullanılan mutabakat algoritmasıdır. Uygulamaya Özel Entegre Devreler (ASIC) tam da bu bağımlılık nedeniyle Bitcoin madenciliği için üretilmiştir. O zamandan beri, yeni blokların doğrulanmasını tekeline aldı ve sistemin merkezi olmayan doğası için bir tehdit haline gelmiştir. ASIC tabanlı cihazların üretimi tehlikede olsa bile, merkezi olmayan uygulamaları etkilediği için durdurulamazdır. Bu tehdidi azaltmak için çeşitli mutabakat protokolleri önerilmiştir, ancak hepsi bu tehdidi tamamen ortadan kaldırmakta yetersiz kalmıştır. ASIC cihazlarının yüksek maliyeti nedeniyle, yalnızca az sayıda madenci blok zinciri ağını tekeline alabilmektedir. Gelecekte ASIC'e dayanıklı bir mutabakat protokolü oluşturmak için Filtrelenmiş İş İspatını (FPoW) öneriyor ve değerlendirmektedir (Ashik vd., 2020).

Blok zinciri tasarımında pek çok ödünleşme söz konusudur ve blok boyutu gibi ölçeklendirme parametrelerine ilişkin ödünleşmeler pek çok tartışmaya konu olmaktadır. Bu konuyu çevreleyen bazı karışıklıkları gidermek amacıyla DCS Üçgeninin bir olasılık kanıtını sunuyoruz. Bu üçgeni, blok zincirleri gibi merkezi olmayan mutabakat sistemlerinin ölçek, merkezi olmama ve mutabakat özelliklerine sahip olduğunu ancak bu üç özelliğe aynı anda sahip olamayacağını göstermek için kullanıyoruz. Daha sonra, üçgenin önerdiği kısıtlamaların üstesinden gelmek için iki stratejiyi açıklamaktadır (Slepek ve Petrova, 2017).

Bu teknik belge gizlilik, güvenlik ve egemenlik sunan bir kimlik sisteminin temel niteliklerini ana hatlarıyla belirlemeyi amaçlamaktadır. Bu durumda kimliğin tanımı, kimlik sisteminin niteliklerinden veya kimlik sisteminin sunduklarından kaynaklanmaktadır. Bu teknik dokümanda bir kimlik sistemi tanımlanmakta ve ardından kimliğin apriori olarak tanımlanmasının aksine bu kimlik sistemi çerçevesinde kimlik tanımlanmaktadır. Kimlik sisteminin birçok yönü Açık İtibar gibi diğer önerilen sistemleri etkilemiş ve motive etmiştir. Bu çalışma, dağıtık mutabakat protokolleri ve en son kriptografi tekniklerini kullanan açık bir platformun, aynı anda yüksek düzeyde egemenlik, güvenlik ve gizlilik sunan bir kimlik sistemi oluşturmanın en etkili yolu olduğunu ortaya koymaktadır (Smith ve Khovratovich,

2016).

Bitcoin gibi kripto para birimlerinin benimsenmesinin ardındaki başlıca itici güçlerden biri, kriptografi ve ademi merkeziyetçiliğin birleşimiyle mümkün olan gizliliklerdir. Ne yazık ki, Bitcoin'in sunduğu iddia edilen anonimliğin aldatıcı olduğu ortaya çıktı ve gizlilik odaklı blok zincirlerine olan ilgi artıyor olsa da çoğu blok zinciri kullanıcısı, kullanıcılar blok zincirleriyle etkileşime girdiğinde ağ katmanı verilerinden ve sızdıran erişim modellerinden yararlanan gizlilik saldırılarına karşı hala savunmasızdır. Blok zinciri tabanlı uygulamaların güçlü gizlilik garantileri sunup sunamayacağını ve nasıl sunabileceğini belirleme ihtiyacı giderek daha acil hale gelmektedir. Gizli erişim sağlamak için birçok araştırmacı Tor gibi anonim iletişim ağlarının kullanılmasını önermektedir. Bu yöntem endişelere yol açmakta ve anonim olmayan kullanıcıların IP adresleri veya diğer işlemlerle ilişkilendirilemeyen işlemleri yayınlamalarına ve hangilerini aradıklarını ifşa etmeden belirli işlemler hakkında bilgi almalarına olanak tanıyan mekanizmalara duyulan ihtiyacı vurgulamaktadır (Henry vd., 2018).

Bit Coin ile işlemler eşler arası bir ağ üzerinden yayılır ve madeni paralar dağıtılmış bir madenci grubu tarafından üretilir. Bitcoin merkezi olmayan bir P2P dijital para birimidir. Kullanıcıların rastgele oluşturulmuş sınırsız sayıda Bit Coin adresine sahip olmalarına izin vererek, Bit Coin bir miktar anonimlik ya da daha doğrusu takma ad sunar, ancak yeni araştırmalar bu anonimlik seviyesinin aslında oldukça düşük olduğunu göstermektedir. Sonuç olarak, geliştiriciler iyi bilinen mobil SPV istemcilerine varsayılan Tor işlevselliği eklemek ve kullanıcıları anonimleştiriciler veya Tor aracılığıyla Bit Coin ağına bağlamak için motive olmaktadır. Bu çalışmada, Bit Coin'in Tor ile birleştirilmesinin nasıl yeni bir saldırı vektörü oluşturduğunu gösteriyoruz. Tor yerine Bit Coin kullanmayı tercih eden herhangi bir kişi, saldırgan için hiçbir maliyeti olmadan diğer kullanıcılar arasındaki bilgi akışları üzerinde tam kontrole sahip olabilir. Özellikle, saldırgan kullanıcıya hangi Bit Coin bloklarının ve işlemlerinin gönderileceğini kontrol edebilir, kullanıcı işlemlerini ve bloklarını geciktirebilir veya atabilir ve kullanılan takma adlardan bağımsız olarak kullanıcı işlemlerini birbirine bağlayabilir. Ek olarak, bir bilgisayar korsanının Bit coin ağına doğrudan bağlantı kurmayı seçtiklerinde bir kullanıcıyı tanımlamak ve IP adreslerini elde etmek için kullanıcının parmak izlerini nasıl kullanabileceğini göstermektedir (Biryukov ve Pustogarov, 2015).

Merkezi olmayan bir para birimi ağı olan Bitcoin, uluslararası finansal işlemlerin gerçekleştirilmesi için olası bir alternatif olarak popülerlik kazanmaya başlıyor. Birçok kullanıcısı için, kullanıcıların gizliliğini korumak için takma adlar kullanması bir satış noktası olmuştur. Bununla birlikte, Bitcoin işlem defterinin kendine özgü kamusal doğası nedeniyle kullanıcıların gizliliği, bağlanabilir anonimlikle ciddi şekilde sınırlıdır ve şimdiye kadar birkaç işlem anonimleştirme saldırısı belgelenmiştir. Bu makalede, kullanıcıların Bitcoin'i tamamen anonim bir şekilde kullanmalarını sağlayan tamamen merkezi olmayan bir Bitcoin karıştırma protokolü olan CoinShuffle fikri sunulmaktadır. Sorumlu, anonim grup iletişim protokolü Dissent'ten esinlenen CoinShuffle, kendisinden önce gelen Bitcoin karıştırma protokollerine göre bir dizi avantaja sahiptir. Mevcut Bitcoin sistemiyle kusursuz bir şekilde çalışır ve güvenilir, sorumlu ya da güvenilmeyen herhangi bir üçüncü taraf gerektirmez. CoinShuffle ile kullanıcılar iletişim ek yükünde yalnızca hafif bir artış yaşarken, Bitcoin sisteminin geri kalanı minimum hesaplama ve iletişim ek yükü yaşar ve tüm bunlar ek anonimleştirme ücretlerinden tamamen kaçınır (Ruffing vd., 2014).

Bitcoin'in 2008 yılında piyasaya sürülmesinden bu yana kripto para birimlerinin etkileyici bir şekilde benimsenmesine rağmen, bu benimsemeyi teşvik etmede kişiler arası güvenin rolüne çok az akademik ilgi gösterilmiştir. Bu makalede, Dünya Değerler Araştırması'nın 7. dalgasından, Twitter'dan ve Google Trends'ten elde edilen verileri kullanarak, kişiler arası güvenin piyasa değerine göre en büyük üç kripto para birimine (Bitcoin, Ethereum ve Litecoin) olan ilgi ve bunların benimsenmesi üzerindeki etkisini ölçüyoruz. Sonuçlarımız, güvenin kripto paralara olan ilgi ve kripto paraların benimsenmesi üzerinde pozitif ve istatistiksel olarak anlamlı bir etkisi olduğunu göstermekte ve finansal piyasaların büyümesinde güvenin önemini teyit etmektedir (Jalan vd., 2023).

Bitcoin olarak bilinen dijital para birimi halkın büyük ilgisini çekmiştir. Bu durum hem değer patlamalarına hem de madeni parayla işlem yapan borsaların çökmesine neden oldu. Bitcoin'in temel fikirlerinden biri, ödül olarak Bitcoin yaratmak için, tüm finansal işlemleri doğrulamak üzere madencilik olarak bilinen emeğin yapılması gerektiğidir. Bu makalede Bitcoin madenciliği ile ilişkili enerji kullanımını inceliyoruz. Madenciliğin enerji maliyeti ile ilişkili olarak Bitcoin madenciliğinin karlı olup olmadığını ve ne zaman karlı olduğunu inceliyor ve madenciliği karlı hale getirmek için genellikle özel donanımlara ihtiyaç duyulduğu sonucuna varıyoruz. Ayrıca mevcut Bitcoin madenciliği güç tüketiminin İrlanda'nın elektrik tüketimine benzer olduğunu göstermektedir (O'Dwyert ve Malone,

2018).

Genel olarak konuşmak gerekirse, blok zinciri teknolojisinin üniversitelerde, işletmelerde ve toplumda yüksek enerji tüketimine neden olduğu iddiası hakkında hala çok sayıda genelleme yapılmaktadır. Blok zinciri teknolojisinin benimsenmesi, kaçınılmaz olarak sürekli kullanımına ilişkin endişeleri artıran bu algı nedeniyle engellenmektedir. Blok zinciri teknolojisi yaygın olarak yıkıcı ve çığır açan bir yenilik olarak kabul edilmektedir. Blok zinciri teknolojisinin enerji tüketimine ilişkin genellemeleri değerlendirirken dikkatli olmak önemlidir, çünkü bu tüketim tek tip olmaktan uzaktır. Bu makale, şimdiye kadarki tartışmalara hakim olan yalnızca Bitcoin'in enerji tüketimine odaklanmak yerine, konuya kapsamlı bir şekilde açıklık getirmeyi amaçlamaktadır (Seldmeir vd., 2020).

Bitcoin kripto para birimi tarafından kullanılan halka açık bir defter olan blok zinciri, tüm işlemlerinin kaydını tutar. Blok zincirinin madenciler olarak bilinen kullanıcılar tarafından yönetilen dağıtılmış protokolü, güvenliği için hayati önem taşımaktadır. Geleneksel görüşe göre, madencilik protokolü madencileri belirlenen kurallara uymaya teşvik eder ve hem teşvik uyumludur hem de gizli anlaşma yapan azınlık gruplarına karşı güvenlidir. Gösterdiğimiz gibi, Bitcoin madencilik protokolünde bir teşvik çatışması vardır. Gizli anlaşma yapan madencilerin elde ettiği gelirin adil tazminatlarını aştığı bir saldırı başlatır. Gizli anlaşma grubu, çoğunluk haline gelene kadar büyüyecek ve rasyonel madenciler saldırganlara katılmayı seçecektir. Bunlar saldırının Bitcoin üzerindeki potansiyel büyük etkilerinden sadece ikisidir. Bu noktada, Bitcoin sisteminin merkezi olmayan yapısı kaybolur. Belirli koşullar sağlandığı takdirde, herhangi bir koalisyon büyüklüğündeki madenciler bencil madencilik yapabilirler. Genel durumda, Bitcoin protokolünde Bitcoin'i koruyan uygulanabilir bir değişiklik önermektedir. Bu değişiklik, kaynakların dörtte birinden daha azını kontrol eden bir koalisyonun açgözlü madencilik yapmasını yasaklamaktadır. Bu eşik, yanlış olarak varsayılan 1/2 sınırı kadar güçlü değildir, ancak yine de herhangi bir büyüklükteki koalisyonun sistemi baltalayabildiği mevcut durumdan daha güçlüdür (Eyal ve Sirer, 2018).

Bu çalışmada madencilik stratejisi uzayı, geniş bir parametre yelpazesi için madencinin gelirini artıran yeni "inatçı" stratejilerle genişletilmiştir. Bu şekilde, kendine hizmet eden madencilik saldırısının (genellikle) en iyisi olmadığını gösterir. Ayrıca, bir madencinin kazancını daha da artırmak için madencilik dışı saldırıları ağ düzeyinde tutulma saldırılarıyla

nasıl birleştirebileceğini gösterir. Şaşırtıcı bir şekilde, bazı durumlarda, saldırganın mümkün olan en iyi planı kullanması koşuluyla, bir tutulma saldırısının kurbanlarının tutulmaktan bile fayda sağlayabileceğini gösterir (Nayak vd., 2016).

Yeni oluşturulan blokların hızlı bir şekilde dağıtılması, Bitcoin protokolünün düğümler için bir gerekliliğidir. Ancak güçlü düğümler, oluşturdukları blokların yayınlanmasını seçici olarak geciktirerek daha büyük kazançlar elde edebilirler. Eyal ve Sirer bu tür bencil madencilik saldırılarının varlığını rapor eden ilk kişilerdir ve özellikle standart protokolden nasıl sapılacağını göstermişlerdir (SM1 olarak adlandırdığımız bir strateji) (Eyal ve Sirer, 2018). Kâr eşiği kârlı bir saldırı için gereken en düşük kaynak yüzdesi bu makaledeki araştırmamızın konusudur. Analizimiz, sistemin bu tür saldırılara karşı güvende olduğu bir eşik belirlemektedir. Çeşitli varyasyonlar altında en iyi saldırı stratejisini belirleyerek, yöntemlerimiz protokoldeki değişikliklere uyum sağlayacak ve bencil madencilığe karşı savunmasızlığını değerlendirecek şekilde değiştirilebilir. Kar eşiğinin aslında SM1 şemasının neden olduğu eşikten kesinlikle daha küçük olduğu belirlenmiştir. Algoritmamız, saldırıdan çekilmeleri daha iyi düzenleyen ve SM1'e baskın hale getiren politikalar üretmektedir. Daha önce önerilen bazı karşı önlemleri daha ayrıntılı olarak değerlendiriyoruz ve etkinliklerinin daha önce varsayılandan daha düşük olduğunu bulmaktadır. Algoritmamız aracılığıyla, Eyal ve Sirer tarafından bencil madencilığe karşı önerilen karşı önlemin daha önce varsayılandan marjinal olarak daha az etkili olduğunu göstermektedir. Bundan sonra, iletişim gecikmeleri meydana geldiğinde bencil madencilik hakkında daha fazla bilgi ediniyoruz ve küçük saldırganların bile gecikme muhasebesi modeli altında kar eşiği ortadan kalktığında zaman zaman protokolü ihlal etme teşviki olduğunu göstermektedir. Bencil madencilik ile çifte harcama saldırılarının gücü hakkında bazı son düşünceler sunar (Sapirshtein vd., 2015).

Modern finansın mevcut örgütlenme biçimine potansiyel olarak cazip bir alternatif, Bitcoin ve diğer kripto para birimlerine güç veren merkezi olmayan çoğaltılmış defter teknolojisi olan blok zinciri teknolojisi tarafından sağlanmaktadır. Finansal sistem şu anda menkul kıymet mutabakatı için merkezi menkul kıymet depoları (CSD'ler), döviz işlem mutabakatı için CLS Bank, muhabir bankacılığa hakim az sayıda banka ve büyük yatırım kurumları için küresel para transferlerini gerçekleştiren bir avuç banka dahil olmak üzere bir dizi merkezi güvenilir aracıya dayanmaktadır. On yıl öncesine kadar bu merkezlerin güçlü mali yapıları ve yetkin yönetimleri sayesinde başarısız olma ihtimallerinin son derece düşük olduğuna

inanılıyordu. Daha da önemlisi, batamayacak kadar büyük (TBTF) olduklarına, yani batmaları halinde hükümetin müdahale ederek ihtiyaçlarını karşılayacağına inanılmaktadır. Bu varsayımlar, dünyanın en gelişmiş ekonomilerindeki çok sayıda büyük bankanın ya battığı ya da gönülsüzce kurtarıldığı 2007-2008 Küresel Finansal Krizi ile altüst olmuştur. 2010-2012 avro Bölgesi Krizi, insanların zengin devletlerin taahhütlerini yerine getiremeyebilecekleri yönündeki endişelerini arttırmıştır. Büyük finans kuruluşlarının bilgisayarlarının defalarca saldırıya uğraması da güveni aşındıran bir başka unsurdur. Bu tür bir güvene duyulan ihtiyacı azaltan blok zinciri gibi merkezi olmayan sistemler, finansın merkezi merkezlerine duyulan güvenin giderek daha fazla sorgulanması nedeniyle cazip hale gelmektedir (Varma, 2019).

Blok zinciri, güven ve güvenlik endişelerini, yüksek bakım maliyeti sorunlarını ve benzerlerini ele alabilen merkezi olmayan ağlar için önemli çözümler sağladığından IoT için umut verici bir teknoloji olarak kabul edilmiştir. Blok zinciri tarafından sağlanan ademi merkeziyetçilik, büyük ölçüde, herhangi bir üçüncü tarafın katılımı olmadan dağıtılmış bir şekilde eşler arası ticarete olanak tanıyan bir fikir birliği mekanizmasının kullanımına bağlanabilir. Bu makale, temel blok zinciri kavramını tanıtarak ve bir mutabakat mekanizmasının blok zinciri özellikli bir IoT sisteminde neden vazgeçilmez bir rol oynadığını göstererek başlamaktadır. Ardından, iki ünlü mutabakat mekanizması olan PoW ve PoS'un ana fikirlerini tartışıyor ve IoT'deki sınırlamalarını listeliyoruz. Daha sonra, iki ana akım DAG tabanlı mutabakat mekanizması olan Tangle ve Hashgraph, DAG mutabakatının IoT sistemi için neden PoW ve PoS'tan daha uygun olduğunu göstermek için gözden geçirilmektedir. DAG tabanlı mutabakat mekanizmalarının gelecekte ele alınması gereken potansiyel sorunları ve zorlukları son bölümde tartışılmaktadır (Cao vd., 2019).

Blok zinciri, insanların çevrimiçi iletişim kurma şeklini tamamen değiştirme potansiyeline sahiptir. Finans sektöründen çok sayıda diğer ekonomik sektöre kadar geniş bir uygulama alanına sahiptir. Blok zinciri teknolojisi nedir, temelinde yatan ilkeler nelerdir, şu anda teknolojik olarak nasıl uygulanmaktadır ve şu anda nasıl düzenlenmektedir? Bu makalede bu soruları ele alacak ve bazı temel yanıtlar sunacağız, ancak bunların yanıtları, çok sayıda ilgili alanda çok çeşitli uzmanlar tarafından yazılmış çok sayıda makalenin okunmasını gerektirmektedir. Yasal, akademik, teknolojik, endüstriyel veya başka bir perspektiften bu alana dahil olan bireyler için blok zinciri ve dijital para birimi alanı hakkında kapsamlı bir anlayışa sahip olmak çok önemlidir.

Dağıtık defter teknolojisi, blok zincirleri ve dijital para birimlerine genel bir bakışla birlikte, ilgili temel fikirler ve terminolojinin yanı sıra bu fikirlerin nasıl etkileşime girdiği de tartışılmaktadır. Blok zinciri teknolojisi ve altyapısının uygulanmasıyla ilişkili ödünleşimler, avantajlar, kısıtlamalar ve performans ölçütlerini gözden geçirmektedir. Ayrıca izinli blok zinciri kavramı hakkında da konuşuyoruz. Ayrıca, blok zinciri teknolojisinin finans sektörü dışındaki çeşitli gerçek dünya kullanımlarını keşfetmektedir (Kakavand vd., 2017).

Çevrimiçi mikro ödemelerin neden başarısız olduğuna dair mantıklı gerekçeler sunuyoruz. Müşterilerin bu tür işlemlerle ilişkilendirdiği "güçlük faktörü" tanımlanmaktadır. Daha sonra, zihinsel işlem maliyetleri ve fiyat ayrıntı düzeyi çerçevesi tanıtılmakta ve mikro ödemelere ilişkin argümanlar bu bağlamda yeniden çerçevelendirilmektedir. Online alışverişle ilişkili psikolojik işlem maliyetlerini düşürmek için bazı önerilerle sonuçlandırılmaktadır (Szabo, 1990).

Menkul kıymet ihraç eden, ticaretini yapan ve elinde tutan müşterilere farklı oyuncular tarafından sağlanan çok çeşitli hizmetler, Menkul Kıymet Hizmetleri Değer Ağı veya SSVN olarak da bilinen menkul kıymet hizmetleri ekosistemini oluşturmaktadır. Deloitte'e göre, yaklaşık 130 uluslararası menkul kıymet borsası hisse senetleri, opsiyonlar, borsa yatırım fonları (EFT'ler), vadeli işlemler, takaslar ve emtia, enerji ve nakit türevlerini işlemektedir. Bununla birlikte, ticari bankalar, brokerler, yatırım bankaları gibi diğer sağlayıcılar da çeşitli müşteri grupları için özel hizmetler sunmaktadır. Bu hizmetleri sağlama konusunda uzmanlaşmış kurumlar bazen saklama kuruluşları olarak adlandırılır. Varlık hizmeti, bir saklama bankası tarafından sunulan temel işlemdir.

Bunlar arasında, bilgi için bir aracı olarak hizmet vermek ve menkul kıymet sahipleri ile ihraççılar arasındaki iletişimi kolaylaştırmak ve yatırımcıların bu görevi kendilerinin üstlenmesinden daha uygun fiyatlı hizmetler sunmak yer almaktadır (Droll vd., 2016).

Menkul kıymet hizmetleri sektörü büyük ölçüde teknolojiye dayanmaktadır ve yıllar içinde yaşadığı hızlı gelişmeler, menkul kıymet işlemlerinin kaydedilmesi ve mutabakatında iyileştirmeler getirmiştir. Örneğin, kağıt tabanlı bir ortamda, menkul kıymet işlemleri 20. yüzyılda manuel olarak çözülmekteydi. Bu işlemler, yeni teknoloji geliştikçe elektronik platformlara taşınmıştır. Küresel menkul kıymetler sektöründe değişiklikler kademeli olarak ve değişen oranlarda gerçekleşmiştir. Günümüzde neredeyse tüm işlemler elektronik

ortamda çözülmektedir; para bankalar arası elektronik ödeme sistemi aracılığıyla transfer edilmektedir ve hisse senetleri kaydıleştirilerek merkezi saklama kuruluđu tarafından saklanmaktadır.

Her geen gn daha fazla iřlem gerekleřmektedir. Bu gvenlik iřlemlerini blok zinciri platformuna ve teknolojisine tařımak uygun mudur? Blok zincirinin byk hacimli iřlemleri gvenilir bir řekilde ve zamanında gerekleřtirme kabiliyeti sorgulanmaktadır.

rneğın, iř ispatı doęrulama yntemi kullanılarak Bitcoin blok zincirinde yeni bir blok oluřturulması artık ortalama on dakika srmektedir (Satista, 2024). ok sayıda arařtırma kuruluđu kapasite sorununu ele alırken, bazı projeler bařı ekmektedir. rneğın, Japon Mitsubishi UFJ Financial Group, saniyede bir milyondan fazla iřlem gerekleřtirme hedefiyle blok zinciri teknolojisine dayalı bir finansal iřlem zmn arařtırmaktadır (Barbaschow, 2018). Gney Afrika Merkez Bankası bir bařka rnektir; blok zinciri teknolojisini kullanarak lkenin normal 70.000 gnlk deme iřlemini iki saatten kısa bir srede gerekleřtirmiřtir (Zhao, 2018).

Bu sektrde blok zincir teknolojisi iki nedenden dolayı nemlidir. ncelikle, bu teknoloji sektr ve deęer zincirlerinde yer alan herkesi tamamen deęiřtirme gcne sahiptir. İkincisi, henz emekleme ařamasındadır; sektrdeki oyuncular bunun ne kadar ok farkında olursa, potansiyelden o kadar iyi faydalanabilecek ve riskleri azaltabileceklerdir. Bununla birlikte, arařtırmamızın yapıldıęı tarih itibariyle, tm menkul kıymet iřleme yařam dngs henz uygulanabilir bir utan ua zm tarafından kapsanmamaktadır. Blok zinciri teknolojisi beklentiler, olasılıklar ve potansiyel sunmaktadır, ancak SSVN'deki kabul oranı olduka yavařtır. Carson ve arkadaşları (2018), finans sektrnn henz blok zinciri teknolojisinin sunduęu tm avantajlardan yararlanmaya hazır olmadıęını belirtmektedir (Carson vd, 2018). Sektr, geliřmiř gvenlik saęlayabilecek nemli zelliklere ve niteliklere sahip olmasına raęmen, blok zinciri teknolojisini daha byk lekte dahil etme konusunda hala tereddtldr. oęu firma rekabette ne gemek iin daha evik olmanın yollarını ararken, oęu hızla ilerleyen teknolojik geliřmelerin getirdięi hızlı deęiřikliklere uyum saęlamak iin kurum apında bir stratejiden yoksundur. Bu inanılmaz teknolojik ilerleme, diren anlayıřının arařtırılmasını gerektirmektedir.

Tablo 2.1 Literatür Tablosu

Yıl ve Isim	Konu	Sonuç
2019;Monrat, Shélén, & Andersson,	Blok Zinciri Teknolojisinin Potansiyel Uygulamaları	Blok zinciri teknolojisinin risk yönetimi, sağlık tesisleri, finansal ve sosyal hizmetler gibi çeşitli uygulama alanlarını çalışma yapılmıştır.
2021,Gang, Lau, & Hong	Bankacılık ve finans sektöründeki blok zinciri araştırmalarının bibliyometrik analizi	Bankacılık ve finans sektöründe 2016-2020 yılları arasındaki literatürü inceleyerek blok zinciri teknolojisinin önemli araştırma konularını, iş avantajlarını ve sektörde karşılaşılan zorlukları belirlemiştir.
2022 ;Banerjee	Finans sektöründe blok zinciri teknolojisinin benimsenme engellerinin hiyerarşik yapıda sınıflandırılması ve çözüm önerilerinin sunulması.	Finans sektöründe blok zinciri teknolojisinin benimsenmesinin önündeki engelleri dört sınıfa (özerk, bağımlı, bağlantılı, bağımsız) ayırarak sistemli bir şekilde ele almıştır.
2017; Yeoh	AB ve ABD'nin blok zinciri teknolojileri ile ilgili düzenleyici sorunlarının analizi	AB ve ABD'nin blok zinciri teknolojileri için benimsediği düzenleyici yaklaşımları karşılaştırmaktadır.
2016;Vukolic	PoW ve BFT tabanlı blok zincirlerinin performans ve ölçeklenebilirlik özelliklerinin karşılaştırılması.	PoW tabanlı blok zincirlerinin ölçeklenebilirlik kısıtlamalarını vurgulayarak, BFT durum makinesi replikasyonuna dayalı olanların avantajlarını ve dezavantajlarını ele almaktadır.
2021;Kumar, Aggarwal, & Raj	Blok zinciri teknolojisinin iş operasyonları ve teklifler üzerindeki etkisi	Blok zinciri teknolojisinin işletmeler için çeşitli ticari faydalar sağlayabileceğini ve özellikle kripto para birimleri ve tedarik zinciri yönetimi gibi alanlarda nasıl kullanılabileceğini incelemektedir.
2022;Rao& Saritha	Bitcoin'in ortaya çıkışı ve blok zinciri teknolojisinin gelişimi	Bitcoin'in yaratılmasıyla birlikte blok zinciri teknolojisinin temelini oluşturduğunu ve bu teknolojinin dağıtık defter sistemi olarak güvenli işlemleri mümkün kıldığını vurgulamaktadır.
2017;Slepak & Petrova	Blok zinciri tasarımında ödünleşmeler ve DCS Üçgeni'nin kullanımı.	blok zinciri tasarımında ölçek, merkezi olmama ve mutabakat özelliklerinin bir arada olamayacağını göstermek için DCS Üçgeni'ni kullanmaktadır.
2016;Smith & Khovratovich	Kimlik sisteminin temel niteliklerini belirlemek.	Açık bir platformun yüksek düzeyde egemenlik, güvenlik ve gizlilik sunan bir kimlik sistemi oluşturmanın etkili yolunu ortaya koyuldu.
2018;Henry, Herzberg, & Kate	Bitcoin ve diğer blok zincirlerinde gizlilik zorlukları ve çözüm önerileri	Anonim kullanıcılar için güçlü gizlilik garantilerinin sağlanması gerekliliği vurgulandı.
2015;Biryukov	Bitcoin madenciliği ile	Tor yerine Bitcoin kullanmanın kullanıcıları

& Pustogarov	ilişkili enerji kullanımının incelenmesi.	güvenlik açısından nasıl savunmasız bıraktığını gösterdi.
2020;Seldmeir, Buhl, Fridgen, & Keller	Blok zinciri teknolojisinin genel enerji tüketimine odaklanan bir inceleme	Blok zinciri teknolojisinin enerji tüketimi hakkında yapılan genelleme ve endişeleri değerlendirdi.
2016;Nayak, Kumar, Miller, & Shi	Madencilik stratejilerinin genişletilmesi ve inatçı saldırıların incelenmesi	Kendine hizmet eden madencilik saldırısının her zaman en iyisi olmadığını ve madencilik dışı saldırılarla kombinasyonunun geliri artırabileceğini gösterildi.
2019;Varma	Blok zinciri teknolojisinin finansal sistemde merkezi olmayan alternatif olarak rolü	Blok zinciri gibi merkezi olmayan sistemlerin, geleneksel finans merkezlerine duyulan güvenin sorgulanması ile cazip hale geldiğini tartışır.
2019;Cao; Li; Zhang; Zhang; Moumtaz; Zhou & Peng	Blok zinciri teknolojisinin IoT için kullanımı ve mutabakat mekanizmalarının karşılaştırılması.	PoW ve PoS'un IoT için sınırlamalarını ve DAG tabanlı mutabakat mekanizmalarının avantajlarını tartışır.
2017;Kakavand, De Sevres, Chilton	Blok zinciri teknolojisinin genel bir bakışı ve temel ilkeleri	Blok zinciri teknolojisinin finans sektörü dışında da çeşitli gerçek dünya kullanımlarının olduğunu ve uygulamaların avantajlarını ve kısıtlamalarını tartışır.
Szabo, 1990	Çevrimiçi mikro ödemelerin başarısızlığı: güçlük faktörü ve çözümler	Müşterilerin çevrimiçi mikro ödemelerle ilişkilendirdiği güçlük faktörü tanımlanmaktadır
Droll, Podlich, & Wedow, 2016	Menkul Kıymet Hizmetleri Değer Ağı veya SSVN	Menkul kıymet ihraç eden, ticaretini yapan ve elinde tutan müşterilere farklı oyuncular tarafından sağlanan çok çeşitli hizmetlerin oluşturduğu menkul kıymet hizmetleri ekosistemi tanımlanmıştır.
2024;Satista	Bitcoin blok zinciri iş ispatı doğrulama yöntemi	Bitcoin blok zincirinde iş ispatı doğrulama yöntemi kullanılarak yeni bir blok oluşturmanın ortalama on dakika sürdüğü belirtilmiştir
2018; Zhao	Güney Afrika Merkez Bankası'nın blok zinciri teknolojisi ile ödeme işlemleri hızlandırma çalışması	Güney Afrika Merkez Bankası'nın blok zinciri teknolojisi kullanarak normalde 70.000 günlük ödeme işlemini iki saatten kısa sürede gerçekleştirdiği vurgulanmıştır.

3. BLOK ZİNCİRİ: ORTAYA ÇIKIŞI VE TEKNOLOJİLERİ

Blok Zinciri'nin vaatleri çok büyük ve finans sektöründen başlayarak birçok ekonomik sektörde oyunun kurallarını kesin olarak değiştirebilir. Ancak bu yıkıcı teknolojinin finans dünyasına sunduğu fırsatlar konusunda daha fazla ilerlemeden önce, blok zincirinin nasıl çalıştığını ve özelliklerini eğitici bir şekilde deşifre etmek bana çok önemli görünür. Bu, bankacılık sektörüne ve genel olarak finansa getirebileceği değişimi anlamamanın kaçınılmaz bir parçasıdır. Önemi ve etkisini daha iyi kavrayabilmek için nasıl ortaya çıktığını da inceleyeceğiz. Kurumlarda yaygın bir güven krizinin yaşandığı bir ortamda, birçok uzmanın bu teknolojinin toplumlarımızdaki katılımcılar arasında daha fazla karşılıklı güvene yol açması gerektiğini düşündüğünü görecektir. Netice olarak, bu teknolojiyle ilişkili başlıca ekonomik, sosyal ve kurumsal riskleri analiz edeceğiz. Çeşitli ekonomik alanlardaki bazı potansiyel uygulamaların yanı sıra devrim yaratmayı amaçladığı kurumsal işlevleri de incelenecektir.

3.1. Blok Zincirinin Ortaya Çıkışı

Bir olguyu daha iyi anlamak için, sadece orijinal amacını değil, aynı zamanda ortaya çıktığı ortamı da anlamak için onu kökeniyle karşılaştırmak yararlıdır. Teknolojinin teknik özelliklerine ve karşılaştığı zorluklara geçmeden önce bu alt bölümde bunu analiz edilecektir.

3.1.1 Bitcoin'in Kökeni

Blok zincir dediğimizde birçok kişinin aklına Bitcoin gelmektedir. 1988 yılında D. Chaum, kullanıcıların hükümet tarafından takip edilmeden İnternet üzerinden para transfer edebilmelerini sağlayacak yeni ve anonim bir ödeme sistemi önermiştir (Chaum vd., 1988). Bunu sağlamak için daha önceki çalışmalarında geliştirdiği kör imzaları kullanmaktadır (Chaum, 1983, pp. 199-203). Ertesi yıl, uygulama DigiCash adı altında piyasaya sürüldü. Ancak, kısmen e-ticaretin henüz emekleme aşamasında olması nedeniyle proje başarısız oldu ve yeterli kaynak olmadığı için projeden vazgeçildi.

1991 yılında S. Haber ve W.S. Stornetta, bir belgede tahrifat yapılmadığını belgelemenin yeni bir yolu üzerine bir makale yazmıştır (Haber ve Stornetta, 1990) . Bunu başarmak için,

hash fonksiyonunun çarpışmaya dirençli olduğunu varsayarak, belgenin parmak izini doğrusal bir zincirde saklamayı önermektedirler. Bilgi depolamayı kolaylaştırmak için D. Bayer, S. Haber ve W.S. Stornetta, 1992 yılında birden fazla belgeden Merkle ağaçlarını tek bir blok zincirine dahil ederek fikri genişletmiştir (Bayer vd., 1993).

1993 yılında elektronik para birimlerini tanıtan iki yeni makale yayınlanmıştır: N. Ferguson tarafından Tek Terimli Off-Line Paralar (Ferguson, 1993) ve S. Brands Gözlemcileri ile Cüzdanlarda İzi Sürülemez Kayıt Dışı Nakit (Brands, 1993).

1996 yılında NSA, "Nasıl para kazanılır: anonim elektronik paranın kriptografisi" başlıklı bir rapor yayınlamakla şu konulardaki endişelerini dile getirdi elektronik para birimleri (Law vd., 1996).

1997 yılında A. Back, hashcash olarak bilinen bir iş ispatı yöntemi önermiştir (Back, 2002). Prensipte, bir hizmete erişmek için CPU kaynakları gerektiren belirli miktarda iş yapmaktır. Yasal bir durumda kullanıcı için bu iş ihmal edilebilir düzeydeyken, hizmete tekrar tekrar erişmek isteyen kötü niyetli bir kişi söz konusu olduğunda bu iş miktarı önemli hale gelmektedir. Bu teknik, örneğin spam veya hizmet reddi ile mücadele etmek için kullanılmaktadır. Ancak hashcash aynı zamanda mutabakat sorununun da üstesinden gelmektedir.

1998 yılında W. Dai, bu çalışma kanıtını, her bir katılımcının sahip olduğu değerin kaydedildiği bmoney adlı bir ağ üzerindeki bir veri tabanını senkronize etmek için kullanmıştır (URL-29, 1998). Aynı yıl, N. Szabo benzer bir prensibe dayanan BitGold'u önermiştir (URL-28, 2024).

Bu teknolojik dalgaın kökeninde bir protokol ve aynı zamanda bir hesap birimi olan Bitcoin'ler bulunmaktadır. Bu yaratımın kökeninde: Satoshi Nakamoto (takma ad), mevcut çeşitli bilgisayar ve kriptografik gelişmeleri (P2P eşler arası değişim, hash fonksiyonu, blok şifre mekanizmaları, çalışma kanıtı...) birleştirerek zarif bir çözüm sunma dehasına sahiptir. Yaratıcının amacı "finansal kurumların aracılığı olmadan çalışabilen bir elektronik ödeme sistemine sahip olmaktır" (Collomb ve Sok, 2017). Bu yeni aracısız ödeme yönteminin ortaya çıkışının, finansal kurumların ve hükümetlerin müdahaleleri nedeniyle eleştirildiği 2008 ekonomik krizinin ardından geldiğini belirtmek gerekmektedir.

Satoshi Nakamoto 2007'den beri geliřtirdiđi Bitcoin'i nihayet 31 Ekim 2008'de piyasaya srd. Bizans generalleri sorunu olarak da adlandırılan ve bu makalenin ilerleyen blmlerinde tartıřacađımız ifte deme sorununa bir zm nermiřtir. Kimilerine gre bu, etkinlik ve karřılıklı gven ile karakterize edilen bir dnemin bařlangıcı oldu. Bazıları iinse yepyeni bir verimlilik ve karřılıklı gven ađının bařlangıcını iřaret etmektedir. Diđerleri ise bunu, "suun Truva Atı" ve 2000'li yılların dotcom balonunu anımsatan speklatif bir cazibe unsuru olarak lekelenmiř itibarından duyulan endiřenin damgasını vurduđu yeni bir dnemin bařlangıcı olarak grmektedir (Toledano ve Janin, 2018). Grdđnz gibi, Bitcoin gvenilir bir nc tarafın deđerini kanıtlamıřtır, bu yzden zaman zaman abartılı ve son derece ideolojik olmasına rađmen bugn hala bu kadar yaygın olarak kullanılmaktadır.

Blok zinciri, amacı tamamen merkezi olmayan bir paylařılan gven sistemine dayalı bir para biriminin fizibilitesini gstermek olan Bitcoin'in altında yatan teknolojidir. Gvenilir bir nc tarafta merkezileřtirilmek yerine birka ađ dđmne dađıtılmıř bir iřlem kayıt sistemine sahip řifreli bir para birimi olarak Bitcoin, alıřveriřleri merkezsizleřtirmeyi ve aracılar olmadan deđer akıřını mmkn kılmayı sađlayan İnternet evriminin ilk taslađıdır (Caseau ve Soudoplatoff, 2016, p. 14).

2013 yılında V. Buterin blok zinciri konseptini ele almaya karar verdi ve merkezi olmayan uygulamaları alıřtırma yeteneđini ekledi. Ethereum adı verilen bu yeni blok zincirinin amacı, bir tr merkezi olmayan dev bilgisayar inřa etmektir (Buterin, 2013). Bu, daha sonra daha ayrıntılı olarak inceleyeceđimiz akıllı szleřmeler kavramı ve bir dizi reticinin ve geliřtiricinin harekete gemesini sađlayan bir dizi bařka hizmet sayesinde alanı her trl iřleme amıřtır (Laurent, 2018).

3.1.2 Gven Krizi

Bilim ve teknolojide muazzam ilerlemelerin yařandığı, internetin Rnesans'ın matbaasını ađrıřtırdığı byk bir deđerim ađındayız. Aralarımız giderek daha gl, bilgimiz giderek daha ok ve bu sre son on yılda daha da hızlanarak kolektif zekanın ođalmasına yol amaktadır. Tm bunlar kurumlarımıza karřı temel bir gven sorunu yaratmakta ve bu da ilerlemenin nnde byk bir fren oluřurmaktadır.

Bugünlerde kime güveniyoruz? GAFAM (Google, Apple, Facebook, Amazon, Microsoft) 'a mı, hükümetlere mi, küresel kurumlara mı? Devlete güvenin nispeten yüksek olduğu ülkelerde bile güven azalmaktadır. Günümüzde güven iki ortamda teyit edilmektedir: aile ve toplum. Ancak güven, enerji ve bilgi gerektiren kırılgan bir dengedir. Sosyal modellerimiz hala büyük ölçüde enerjinin ebeveynler, öğretmenler, yöneticiler, hakimler vb. tarafından sağlandığı dışsallaştırılmış güven modellerine dayanmaktadır. Ancak son zamanlarda topluluk güveninin ortaya çıktığını görüyoruz. Airbnb, Blablacar gibi tüm topluluk sitelerinde bulunan bir kavram olan eBay'in alıcılar ve satıcılar arasında çağrışım kavramını icat etmesi, topluluk güveninin ortaya çıkışına bir örnektir. Öte yandan, etkileşim sayısının patladığı bir dünyada, dış kaynaklı güven modelinin tek başına yetersiz kalması kaçınılmazdır. Bazıları, etkileşimlerdeki bu artışla başa çıkmak için kaynakları artırmamız gerektiğini savunacaktır, ancak bu yöntem azalan getiri yasasıyla karşılaşma riskini taşımaktadır (Caseau ve Soudoplatoff, 2016, p. 12). Hem iş hem de yönetim açısından bakıldığında, kuruluşlar organizasyon modellerine (silo modelleri, dikey yapılar, hantal hiyerarşiler, güvensizliğe dayalı yönetim vb.) Bu modeller, bilginin düzgün dolaşımını engelledikleri ve dolayısıyla bilgi üretimini azalttıkları için artık sınırlarını göstermektedir.

Topluluk güven modeli ölçeklenebilirdir ve çok sayıda etkileşimi çözebilir, bu da onu bu kadar güçlü kılan şeydir. Topluluk güven modeli için blok zincirinin gücü, işlemlerin güvenilir, denetlenmiş ve dağıtılmış olmasını sağlama yeteneğinde yatmaktadır (Caseau ve Soudoplatoff, 2016). İnternet bir yıkım mantığının ürünüdür ve Blok zinciri bu mantığı daha da ileri götürür.

Kanonik haliyle blok zincir, genel çıkar adına güvenilir kurumlara bir alternatif olarak görülebilir (Manas ve Bosc-Haddad, 2017).

İnternet tarafından desteklenen protokollerin ve kriptografik ilkelerin ustaca bir kombinasyonu olan blok zinciri, güven sorununa ideal bir modern çözüm gibi görünmektedir. Geçmişte geliştirilen sosyal çözümler (tapu sicili, emanetçiler, merkez bankaları, vb.) hem verimlilik hem de kurumlara olan güven kaybı adına eleştiriye iki kat açık görünmektedir.

Mevcut kurumların genellikle muhafazakâr olduğu ve teknolojik yeniliklerden faydalanmakta yavaş kaldığı söylenmelidir. Benzer şekilde, güven kaybı da çok gerçek bir

olgudur. Dahası, 2008 krizi ve 2013'teki Snowden olayı vatandaşlar-tüketiciler ve kurumlar arasındaki ilişkiyi daha da zayıflatmıştır. Aynı zamanda bilgisayarlara ve algoritmik teknolojiye olan güvenimiz de artmaktadır.

Bununla birlikte, bu kaldırma işleminin bankalar ve uluslararası finans kuruluşları gibi toplumumuzdaki araçlar, popülizmden arınmamış bir ideolojik duruşa dayanmaktadır. Bu teknolojik çözümcülük, sosyal ya da yasal kökleri olmayan "soğuk" algoritmalar aracılığıyla güven tesis etmek istemektedir. Arnaud Maras gibi pek çok ekonomist ve alan uzmanı bu radikal değişimin hayali olduğuna inanmaktadır. İtibari para birimi toplumlarımızda güvenin birincil dayanağı olduğundan, Bitcoin'in yerini almaya çalıştığı şey de budur (Manas ve Bosc-Haddad, 2017). Elbette para biriminin teknolojik özellikleri var, ancak her şeyden önce herkesin sorumluluğuna ışık tutan yasal bir temele dayanıyor. Bitcoin ile hiç kimse gerçekten sorumlu değildir ve yanlış uygulamalarla mücadele etmekten sorumlu kimse yoktur. Son olarak, teknolojinin marjinal faydası ne olursa olsun, küresel çözümcülük tuzağından kaçınmak çok önemlidir. Gördüğümüz gibi, aşırı uygulama stratejileri tüm sektörler için çok risklidir. Bununla birlikte, bu teknolojinin güvenilir saklama kurumları tarafından uygulanması parlak bir gelecek vaat etmektedir (Manas ve Bosc-Haddad, 2017).

3.2 Blok Zincirinin Teknik Özellikleri

"Paylaşılan, taklit edilemeyen ve tasarımı gereği yok edilemeyen büyük bir bilgisayar defteri fikri, yeni bir devrimin, blok zincirinin kalbinde yer almaktadır." (Dalahaye, 2015).

Blok zincir bazen internetten bu yana en büyük icat ya da yaşam şeklimizi değiştirecek gerçek bir devrim olarak tanımlanmaktadır (URL-22, 2018). Nitekim ünlü İngiliz gazetesi The Guardian provokatif bir başlık atmaktan çekinmedi: " blok zinciri: yaşamın, evrenin ve her şeyin cevabı mı?" (URL-29, 2016).

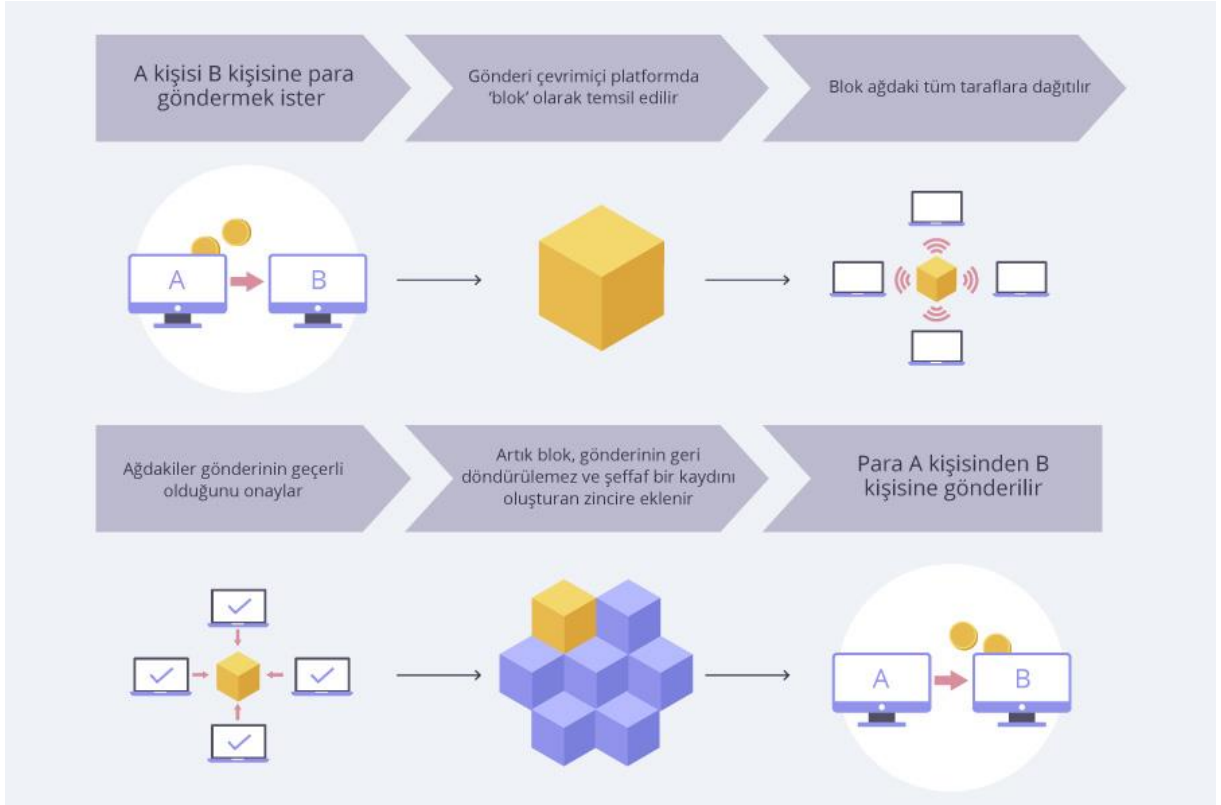
3.2.1 Blok Zinciri: İnternet Üzerinde Değer İşlemlerinin Yeniden Tanımlanması

Blok zinciri, bilginin internet üzerinden saklanmasını ve iletilmesini sağlayan bir teknolojidir. Günümüzde ağırlıklı olarak İnternet üzerindeki değer işlemleri için kullanılmaktadır. Tüm İnternet işlemleri, bir noktada işlemi onaylamak için güvenilir bir üçüncü taraf (finans kurumu, noter veya kamu kurumu) gerektirir.

Blok zincir genel olarak "bilgi saklama ve iletme ve bilgi aktarma teknolojisi" olarak tanımlanmaktadır. Blok zincir, varlık işlemlerini ve bunların ayrıntılarını aynı anda birden fazla konumda kaydeden dijital sistemleri ifade eden Dağıtılmış Defter Teknolojisidir (DLT). Blok zincir en bilinen DLT teknolojisidir (Pignel, 2019). Bir blok zinciri, oluşturulduğu günden bu yana kullanıcıları arasındaki tüm alışverişlerin geçmişini içeren bir veri tabanıdır. Bir defter görüntüsü genellikle bir blok zincirini görselleştirmek için kullanılır: bir blok zinciri, kuruluşundan bu yana kullanıcıları tarafından yapılan tüm alışverişleri içeren geniş bir kamu defterine benzetilebilir. Ana özelliklerinden biri değiştirilemez olmasıdır (Pignel, 2019). Bloklar, geriye dönük olarak değiştirilmelerini imkânsız kılan bir dizi yenilikçi kriptografik işlemle korunmaktadır (Dalahaye, 2015). Bu teknolojiye şeffaf karakterini veren de budur: sadece işlem ekleyebilirsiniz, ancak bunları değiştiremez veya silemezsiniz ve sahteciliğe karşı dayanıklıdır.

Bu teknoloji merkezi olmayan eşler arası (P2P) bir sisteme dayanmaktadır: veriler tek bir sunucu tarafından barındırılmamakta, araçlar olmadan kullanıcılar arasında dağıtılmaktadır. Kullanıcılardan bazıları, dünyanın herhangi bir yerinde bulunabilen blok zincirinin kopyalarına sahiptir (Pignel, 2019). Bu yüzlerce kopya sürekli olarak aynı anda güncellenmektedir (Dalahaye, 2015). Merkezi operatörler tarafından yönetilen geleneksel veri tabanlarının aksine, blok zinciri ağdaki tüm düğümler tarafından kolektif olarak yönetilir. Bu düğümlerin hepsi, takip edilecek prosedürlerin yanı sıra veri tabanının güncellenmesi için gerekli koşulları tanımlayan aynı bilgisayar protokolüne uyar (Pignel, 2019).

Pratik anlamda, blok zinciri teknolojisi, birbirine bağlı bloklar halinde gruplandırılmış verileri, genellikle işlemleri kaydeden bir defter şeklini almaktadır. Bir blok basitçe bir araya getirilmiş bir bilgi koleksiyonudur ve bloklar geri döndürülemez bir şekilde (zincirlerle) birbirine bağlıdır. Her blok, "madenciler" olarak bilinen kullanıcı doğrulayıcılar olan ağ düğümleri tarafından doğrulanır. Doğrulandıktan sonra bloklar zaman damgalı hale getirilir ve tüm kullanıcıların erişebileceği şekilde blok zincirine entegre edilir. İşlem daha sonra alıcı ve tüm ağ tarafından görülebilir. Madenciler tokenlar aracılığıyla ücretlendirilir (Pignel, 2019). Son seviye ise blok zinciri kullanıcısının ihtiyaç duyduğu bilgi ve hizmetleri (değişim platformu, para cüzdanı vb.) sağlamak üzere geliştirilen uygulamalar veya akıllı sözleşmelerdir. Blok zincirini değiştirmenin tek yolu bir blok eklemektir: mevcut bir bloğu değiştirmek veya zincirleri değiştirmek mümkün değildir (Pignel, 2019).



Şekil 3.1: Blok zinciri nedir?

Kaynak: <https://www.ceyrekmuhendis.com/blok-zinciriblockchain-nedir/>

İnternet, insanları anında birbirine bağlamayı ve doğrudan yayın yapmayı mümkün kılmıştır. Blok zincir teknolojisi ise doğrudan işlem ve sertifikasyon vaat etmektedir (Tolanado ve Janin, 2018). Blok zinciri ile ilişkilendirilen çeşitli özellikler vardır: aracılıktan çıkarma, izlenebilirlik, şeffaflık, dağıtık mutabakat, etkisizlik, dağıtık yapı, esneklik, güvenlik ve güven (URL-22, 2018). Tüm bu özellikler blok zincirinin yenilikçi potansiyelini oluşturmaktadır (Pignel, 2019). Şimdi blok zincirini yıkıcı bir teknoloji haline getiren üç ana teknik özelliği açıklayacağız.

3.2.2 Mutabakat Algoritması: İşlem Doğrulama Süreci

Blok zinciri, dağıtık bilgi işlemde eski bir sorunu çözmemizi sağlar ve teknolojiye aşına olmak için bunu anlamakta fayda vardır. Blok zinciri, emirleri içeren ve güvenin harici bir aktör olmadan yönetilmesini sağlayan şifrelenmiş, dağıtılmış bir defterdir. Geleneksel veri tabanlarının aksine, dağıtık defterlerin merkezi bir veri deposu ya da yönetim işlevi yoktur. Dağıtılmış bir defterde, her düğüm her bir ögeyi işler ve doğrular, her ögenin bir kaydını

oluşturur ve doğruluğu konusunda bir fikir birliği oluşturur (URL-21, 2020). Dağıtılmış bir defter, defter gibi statik verileri ve finansal işlemler gibi dinamik verileri kaydetmek için kullanılabilir (URL-21, 2020). Blok zincirinden bahsederken genellikle bir ağ oluşturan bloklar dizisi ve merkezi olmayan, güvenli ve güvenilir bir süreç kastedilir. Bir blok zincirinin güvenli ve güvenilir olması için bir mutabakat algoritmasına sahip olması gereklidir.

Somut bir ifadeyle, mutabakat algoritması, blok zinciri ağındaki her bir aktörün her bir bloğun oluşturulması ve sıralanması konusunda anlaşmaya varmasının bir yoludur.

Bir blok zinciri genellikle tek bir şirket veya bireyden bağımsızdır, çünkü birden fazla oyuncunun ittifakıyla çalışır. Her aktör, her işlem ve etkileşimin mümkün olduğunu ve başka hiçbir aktör ya da katılımcının diğerlerinin zararına hile yapmaya çalışmadığını kontrol ederek ağın güvenliğine katkıda bulunur. Bu sıkıcı doğrulama süreci, blok zincirinin işlem geçmişinin doğru ve kurcalamaya karşı korumalı olmasını sağlamaktadır. Tüm oyuncular blok zinciri kaydındaki bir girişi doğrulamayı kabul etmelidir, bu bir konsensüs algoritması olarak bilinmektedir (URL-23, 2021).

Blok zinciri mutabakat algoritması, bir blok zincirine kimin yeni bloklar ekleyebileceğini ve düğümlerin zincire eklenecek bir sonraki işlem üzerinde nasıl anlaşmaya varacağını belirleyen mantıktır. Blok zinciri algoritmalarının birkaç ana kategorisi vardır: Proof of Work, Proof of Stake, Delegated Proof of Stake ve Proof of Authority (URL-23, 2021).

Proof-of-Work (PoW), kripto para birimlerindeki en ünlü mutabakat algoritmasıdır, ancak yüksek enerji ve donanım maliyetleri nedeniyle çok daha az yaygın olarak kullanılmaktadır. Bitcoin'in oluşturulması için Satoshi Nakamoto tarafından kullanılan ilk mutabakat algoritmasıdır. Bu nedenle Proof of Work mutabakat mekanizmasının çalışması için büyük miktarda enerji ve donanım gerekir ve birçok kişi tarafından bir ağ için en güvenli çözüm olarak kabul edilir ve ayrıca sansüre direnir (Tolanado ve Janin, 2018). Daha yaygın olarak madencilik olarak bilinen bu eylem, bir "hash" fonksiyonu denkleminin çözülmesini içerir; bu denklemin özelliği, sonuçlarının muazzam sayıda olası kombinasyonla öngörülemez olmasıdır. Bu denklemin çözme olasılığı madencinin hesaplama kapasitesiyle orantılıdır ve giderek daha büyük ve enerji yoğun bilgisayar kurulumları gerektirir. Günümüzde fikir, madencinin rastgele çekildiği ve çekilme şansının aynı seviyede olduğu "proof of stake"

temelli dağıtılmış bir mutabakat kullanmaktır. Bu "forging"(sahtecilik) olarak bilinir (Vamparys, 2018).

3.2.3 Kriptografi: İşlemleri Güvence Altına Alma Süreci

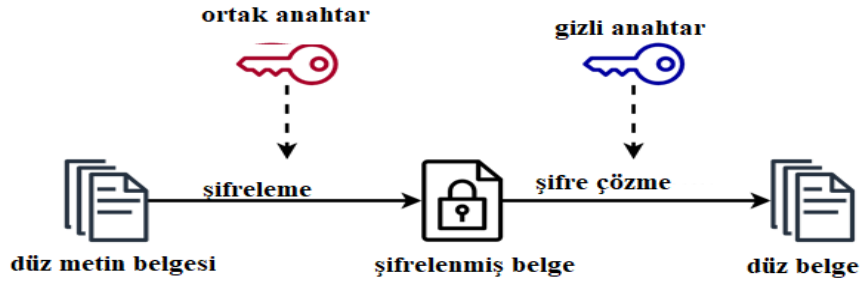
Kriptografi, gelişmiş şifreleme ve kimlik doğrulama teknolojileri aracılığıyla dijital güvenlikte devrim yaratmaktadır. Kripto ile yakından bağlantılı olan kriptografi, kripto para birimi işlemlerinin güvenliğini sağlamada, değiş tokuş edilen verilerin gizliliğini ve bütünlüğünü garanti etmede çok önemli bir rol oynar Kriptografi, verileri yetkisiz erişime karşı güvence altına alma yöntemidir. Blok zincirinde kriptografi, bir blok zinciri ağındaki iki düğüm arasında gerçekleşen işlemleri güvence altına almak için kullanılır. Ayrıca çevrimiçi iletişimleri ve hassas kurumsal verileri güvence altına almak için de kullanılmaktadır (URL-25, 2023).

Kriptografi tekniği uzun yıllardır hükümetler ve ordu tarafından gizli mesajları kendi aralarında iletmek için kullanılmaktadır. Ancak internetin ve eşler arası veri alışverişinin patlamasıyla birlikte kriptografi, kişisel ve ticari verilerin korunmasında her zamankinden daha önemli hale gelmiştir. Günümüzde güvenlik uzmanları çevrimiçi iletişimin, bankacılık işlemlerinin ve şirketler arasındaki hassas veri alışverişinin güvenliğini sağlamak için kriptografiyi kullanmaktadır. Kriptografi, veri şifreleme ve kimlik doğrulamayı kapsar.

Şifreleme teknikleri hassas ve gizli verilerin korunması için vazgeçilmez araçlardır. Kriptografi türleri arasında tek bir anahtar kullanan simetrik şifreleme ve bir çift anahtar kullanan asimetrik şifreleme yer alır. 1970'lerde oluşturulan asimetrik kriptografi, blok zinciri tarafından güvenlik için kullanılan ana araçtır. Asimetrik kriptografi, bir açık anahtar ve bir özel anahtar olmak üzere iki anahtar kullanarak şifrelemeye dayanmaktadır. Kriptografik bir değiş tokuşu göstermek için bir örnek alalım.

Paul ve Ruth ne konuştuklarını kimsenin görmemesi için birbirlerine özel olarak mesaj atmak isterler. Sonuç olarak asimetrik bir şifreleme algoritması kullanmayı seçerler. Ruth genel ve özel anahtarları oluşturur. Bir arkadaşınızın e-posta adresine erişmek için kendi şifrenizi kullanamamanızın tek nedeni bu iki anahtardır. Ruth mesajını açık anahtarıyla şifreler ve Paul'a mesajında gönderir. Paul'a gönderdiği mesajları şifrelemek için bu anahtarı kullanır. Paul daha sonra kendi özel anahtarını kullanarak mesajın şifresini çözerek içeriğini

okuyabilir (URL-26, 2023).



Şekil 3.2: Kriptografik güvenliğin açıklaması.

Kaynak: <https://www.cnil.fr/fr/cybersecurite/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement>

Bu buluş, bir kuruma ihtiyaç duymadan bir anahtarın iletilmesi sorununu çözmektedir. Kripto para işlemleri de aynı prensibi kullanır. Bu durumda, her bir tarafın bir çift açık ve özel anahtarı vardır. Açık anahtar serbestçe paylaşılabılırken, özel anahtar gizli tutulur. Bir taraf diğerine para gönderdiğinde, işlemi şifrelemek için diğer tarafın açık anahtarını kullanır. Yalnızca ilgili özel anahtar işlemin şifresini çözebilir ve fonlara erişebilir (URL-26, 2023).

3.2.4 Dağıtık Defterlerde Bilgi Paylaşım Süreci

Kullanıcıların, merkezi bir doğrulama sistemi olmadan ve kendi standartlarına ve prosedürlerine göre çalışabilen genel defteri paylaşılan bir veri tabanında varlıklar ve holdingler hakkındaki verileri veya kayıtları saklama ve alma yeteneği, dağıtılmış defter teknolojisi olarak bilinir. DLT'lerin yönetilme şekli, tek bir merkezi kuruluşun aksine dağıtılmış bir katılımcı ağı ("düğümler" olarak adlandırılır) tarafından kontrol edilmeleri nedeniyle geleneksel muhasebe defterlerinden farklıdır (Kakavand & De Sevres, 2017).

DLT'ler, finansal hizmetler sektöründe ortak bir veri tabanına erişimi olan kullanıcılar arasında menkul kıymetlerin ve nakit transferlerinin doğrudan takas ve mutabakatını kolaylaştırarak aracılara olan ihtiyacı ortadan kaldıracaktır.

Blok zincirindeki paylaşım fikri, oluşturduğu kaydın birbirinden ayrı birkaç bilgisayarın belleğinde, sistemin tutarlılığını ve sürekliliğini kolektif olarak kapsayan ve garanti eden ağ düğümlerinde çoğaltılmasına olanak tanır (Vamparys, 2018).

Aynı sektördeki kuruluşlar, güvenilir bir üçüncü tarafın yardımı olmadan bir bilgi kaydını paylaştıklarında risklerle karşı karşıyadır. Şirket, bir değişim altyapısını paylaşmaya istekli olduğunda maliyetlerin karşılıklı hale getirilmesinden fayda sağlarken, gizli bilgileri rakiplerine ifşa etme riskiyle karşılaşmaktadır (Collomb ve Sok, 2017). Kullanıcı verilerinin gizliliğini garanti eden özel blok zincirleri bugünlerde ortaya çıkmaya başlıyor. Merkezi olmayan mimarinin merkezi mimariden daha az tehlikeli olduğu her zaman doğru değildir. Pierre Joubert, dağıtık kayıtların ağı saldırılara karşı daha savunmasız hale getirdiğini savunmaktadır (Andriy, 2019). Ancak bu saldırılar, güçlü bir kriptografik sistemle birlikte bir eylemi zaman damgası ile damgalama yeteneği ile engellendiğinden, sistemin güvenilirliği, blok zincirinin uygulanması için çok önemli olan güvenlik kavramına dayanmaktadır.

3.2.5 Halka Açık Blok Zincirleri ve Özel Blok Zincirleri

Farklı tipolojilere sahip çok sayıda blok zinciri ortaya çıkacaktır, bunları iki kategoride sınıflandırabiliriz: halka açık blok zincirleri ve özel blok zincirleri.

Ethereum ya da Bitcoin gibi halka açık blok zincirleri herkese açıktır. Diğerlerinin ise "özel" ya da "izinli" olduğu, erişimin kullanıcı tarafından belirli bir amaç için kısıtlandığı söylenir. Tüm erişim ve izin kuralları önceden zincire kaydedilir. Özel zincirin avantajı, üyelerin kendi içeriklerinden sorumlu olmaları ve bu sorumluluğun bir veya daha fazla üyeye devredilebilmesi, böylece mülkiyetin yanı sıra maliyetlerin de paylaşılmasıdır. Yüksek düzeyde düzenlemeye tabi olan finans dünyasının, zincirden kimin sorumlu olduğunu ve zincirin niteliğini belirleme konusunda bir çıkarı olması muhtemeldir. Birkaç düğüm tarafından kontrol edilen birkaç özel zincire atıfta bulunan özel zincir veya konsorsiyum seçiminin sadece finans kuruluşlarında değil, diğer sektörlerde de norm haline gelmesi muhtemeldir. Bununla birlikte, bazı uzmanlar blok zincirinin yıkıcı tarafının gerçekten de kamu zincirlerinde yattığını savunmaktadır. Gerçekten de güvenilir bir üçüncü tarafın ya da zinciri kontrol eden ve özel veya konsorsiyum blok zincirlerinde gözetim hakkına karar

veren en az bir ya da daha fazla kuruluşun yeniden entegrasyonunun ilk varoluş nedenini kaybetmesi anlaşılabilir bir durumdur. Bununla birlikte, özel blok zincirleri finans, lojistik ve diğer sektörler için önemli bir kaldıracı temsil etmektedir, zira bu teknoloji taklit edilemez olmasının yanı sıra özgünlük ve izlenebilirlik avantajlarını da korumaktadır (Vamparys, 2018, s. 35).

Sadece sistemin yönetişimini değil, aynı zamanda bilgi sağlanmasını da dikkate almak önemlidir. Joelle Toledano'ya göre, bu üç parametre, diğerlerinin yanı sıra, çok sayıda varyasyona yol açmaktadır (Toledano ve Janin, 2018, p. 25):

- **Kimlik**, zinciri kullanmak isteyen herkes tarafından takma adla ve otonom olarak oluşturulabilir. Gerçek bir kimlik, örneğin KYC yükümlülüklerini yerine getirmek için üçüncü taraf bir onaylayıcı tarafından doğrulanacaktır.
- **Tesvik**, sicili korumak ve işlemleri doğrulamak ödüllendirilmelidir. Blok zinciri dünyası çeşitli olanaklar sunmaktadır; bunlardan en iyi bilineni, tipik olarak halka açık blok zincirleri söz konusu olduğunda, kripto para tahsisidir. IOTA geliştirmeleri gibi diğerleri, bir işlemin gerçekleştirilmesi olasılığını başka bir işlemin doğrulanmasına bağlı hale getirmektedir. Alternatif olarak, paydaşlar arasında sözleşmeye dayalı bir anlaşma yoluyla işlemleri onaylamak için harici bir yönetim mekanizması kullanılabilir. Örnek olarak SETL Grup, başta bankalar olmak üzere müşterilerinin blok zinciri teknolojisini kullanarak varlık takaslarının maliyetini önemli ölçüde azaltmalarını sağlamaktadır.
- **Kayıt bilgileri**: değişken parametrelerle. İşlem bilgileri (tutar, alıcı, zaman damgası, vb.) tam olarak kamuya açıklanabilir veya bir işlemin ayak iziyle sınırlı şifrelenmiş bilgiler olabilir veya veriler tam olarak şifrelenebilir ve erişim belirli üyelerle sınırlandırılabilir.

Operasyonları kontrol etmek ve gizli bilgileri korumakla ilgilenir bilgi, bankalar gibi kurumsal oyuncular ağa erişimi kontrol etmeyi tercih etmektedir. Açık ağlardaki halka açık blok zincirleri finansal kuruluşların güvenlik ve gizlilik ihtiyaçlarını karşılamamaktadır. Özel ve kamusal blok zincirleri arasındaki ikilik sadece farklı mutabakat modellerine değil, aynı zamanda oldukça farklı iş modellerine de işaret etmektedir. Son yıllarda, her iki blok zinciri türünün savunucuları çatıştı. Sonuç olarak, kuruluşlarda düzenlenmiş ve kontrollü erişime sahip bir kulüp mantığı hâkim olmuştur. Örneğin finans sektöründe, birbirini tanıyan kurumlar işlemlerin geçerliliği konusunda anlaşabilir ve sapkın davranışlara yaptırım uygulayabilir. 10 bankadan oluşan bir konsorsiyum örneğin, birbirini tanımayan milyonlarca kullanıcının oluşturduğu bir konsensüsten çok daha az zorluk yaşayacaktır (Collomb ve Sok,

2017).

3.2.6 Akıllı Sözleşmeler

Akıllı sözleşmeler kavramı, blok zinciri teknolojilerine dayanan bir ağ tarafından özerk olarak yürütülen bir bilgisayar programıdır. Akıllı sözleşmeler, altta yatan dağıtılmış deftere yazılan ve ağ düğümleri tarafından otomatik olarak yürütülen programlardır. Bir bilgisayar tarafından yürütülebilen herhangi bir talimat teorik olarak bir akıllı sözleşme tarafından yürütülebilir. Akıllı sözleşmelerin yazılması, üst düzey dil olarak bilinen son derece teknik bir bilgisayar dili gerektirir (Dinçel, 2020). Bilgisayar kodu daha sonra çevrilir ve bir blok zinciri ağında kullanılmak üzere bir makine diline dahil edilir. Bu bilgisayar protokolü 1990'larda başlatıldı, ancak blok zincirinin tamamlayıcısı olan akıllı sözleşmelerin önünü açan Bitcoin oldu. Aslında akıllı sözleşmeler ilk olarak Ethereum blok zincirinin kurucu ortağı Vitalik Buterin tarafından resmileştirilmiştir. Ethereum blok zinciri. Bunlar, herhangi bir ölü zaman, kesinti, sahtekarlık veya müdahale olmaksızın programlandıkları gibi çalışan uygulamalardır (Collomb ve Sok, 2017). Dağıtık deftere kaydedilen işlemler veya veriler akıllı sözleşmeyi tetikler ve alınan işlemler de deftere kaydedilir (Natarajan vd., 2017). Halka açık bir blok zinciri ağında konuşlandırılan bu sözleşmeler, doğal olarak bir kripto para birimi ya da token aracılığıyla fonları yönetebilir.

Kriptograf Nick Szabo, 1994 yılında verileri ve dijital sözleşmeleri kod halinde kaydetmenin bir yolu olarak akıllı sözleşmeleri yaratmıştır (URL-24, 2022). Literatürde ilk olarak 1994 yılında ortaya çıkmasına rağmen, akıllı sözleşmeler blok zincir teknolojisinin ortaya çıkışına kadar gerekli değildi. Bunun nedeni, Nick- Szabo tarafından geliştirilen modelde taraflar arasında sözleşme kurallarının uygulanıp uygulanmadığını denetleyecek bağımsız bir üçüncü tarafa ya da kuruluşa ihtiyaç duyulmasıydı. Bu fikir ortaya çıktığında, akıllı sözleşmelerin üçüncü bir tarafın müdahalesi olmadan güvenilir bir şekilde kendi kendini yürütmesi mümkün değildi. Bunu yapmak için gereken teknoloji o dönemde henüz mevcut değildir.

Bitcoin'in ortaya çıkmasıyla birlikte, blok zinciri teknolojisinin merkezi olmayan doğası, merkezi otoriteler ve akıllı sözleşmelerin blok zincirinde kodlanarak gerçekleştirilmesi için artık gerekli değildir. Blok zincirindeki akıllı sözleşmelerin yürütülmesini denetleme sorumluluğu, blok zinciri ağına dahil olan bilgisayarlara dağıtılmış olarak artık mümkün.

Blok zincirinde kodlanmış bir sözleşme, özellikleri sayesinde blok zincirinin değiştiremeyeceği bir sözleşmedir. Akıllı sözleşmelerin ekonomi üzerinde büyük bir etkisi olması muhtemeldir. Sözleşmeler dünyadaki borsaların çoğunu yönetir ve ilgili işlemlere bağlı olarak son derece karmaşık olabilir, çok sayıda çelişkiye yol açabilir ve yürütölmelerini zorlaştırabilir (Andriy, 2019). Akıllı sözleşmenin avantajı, sözleşme ilişkilerindeki tüm insan müdahalesini otomatikleştirmesi ve ortadan kaldırmasıdır. Bununla birlikte, kod oluşturulduğu sırada, sözleşmenin yürütölmesi ve denetlenmesi konusunda güven konusunda endişeler vardı. Bugün blok zinciri sayesinde sadece içeriği değil algoritmaları da saklayabiliyoruz. Blok zinciri sayesinde bu algoritmalar denetlenebiliyor ve böylece güven yeniden tesis edilmektedir. Artık sözleşmelerin dijital olarak kodlandığı ve paylaşılan, şeffaf ve güvenli veri tabanlarında saklandığı bir dünyayı dört gözle bekleyebiliriz (Iansiti ve Lakhani, 2017). Bu dünyada tüm süreçler, görevler, ödemeler ve anlaşmalar kayıt altına alınabilir ve dijital olarak imzalanarak saklanabilir, doğrulanabilir, dağıtılabılır ve kimlik doğrulaması yapılabilir. Yazarlara göre: "Akıllı sözleşmeler belki de blok zincirinin en dönüştürücü uygulamasıdır. Sözleşmeler, işlemler gibi, ekonomik, siyasi ve yasal sistemlerimizin tanımlayıcı çerçeveleridir. Kurumsal sınırları belirler ve varlıkları korurlar. Bugünlerde, bir sözleşme ilgili tüm taraflarca anlaşılmalıdır. Kimse anlamadığı bir sözleşmeyi imzalamak istemez. Bu nedenle, akıllı sözleşmeleri daha güvenli ve günlük yaşamdaki herkes tarafından okunabilir hale getirmek için çaba sarf edilmektedir, böylece insanlar tarafından okunabilir ve aynı zamanda makineler tarafından anlaşılabilir. Sistem, işlemlerin dürüstlüğünü garanti eder. Örneğin bir sigorta sözleşmesi söz konusu olduğunda, geri ödeme koşulları yerine getirilirse, sözleşme yerine getirilmiş olur ve poliçe sahibi tazminat alır. Bu algoritmik sözleşmeler tüm sözleşme bilgilerini (şartlar, taraflar hakkında bilgiler, tarihler, maddeler...) kaydeder ve doğrular, ancak zincirin dışında fiziksel bir doğrulama yapmak söz konusu olduğunda, Ethereum jargonunda Kâhin olarak da bilinen güvenilir bir üçüncü tarafa başvurmak gerekir. Blok zinciri kahinleri harici bilgileri alır ve akıllı sözleşmelerde önceden belirlenmiş kuralları işletmek için bunları blok zincirine entegre eder (Garrick ve Roux, 2017). Akıllı sözleşmeler alanındaki zorluk, Fiat bir sözleşme (yasal ortam) ile şifrelenmiş bir sözleşmenin nasıl ilişkilendirileceğini bilmekte yatmaktadır (Leloup, 2017).

Merkezi Olmayan Özerk Kuruluşlar" (DAO'lar) akıllı sözleşmeler temelinde faaliyet gösteren özerk yapılardır ve topluluğa güvenlik, yönetim ve değış tokuşların değışmezliğı ve önceden tanımlanmış tüm şeffaflık kurallarını sağlar. Ethereum kurucu ortağı Vitalik

Buterin bu noktayı şöyle açıklıyor: "Bir fiyat endeksi yerine hava durumu veri akışını kullanarak kolayca bir finansal türev sözleşmesi yapabilirsiniz. Iowa'daki bir çiftçi, ödemeleri Iowa'daki yağışla ters orantılı olan bir türev satın alırsa ve bir kuraklık meydana gelirse, çiftçi otomatik olarak para alacaktır. Eğer yeterince yağmur yağarsa, çiftçi memnun olacaktır çünkü mahsulleri iyi ürün verecektir. Bu genel olarak doğal afet sigortasına genişletilebilir (Buterin, 2013).

3.3 Blok zinciri Teknolojisinin Geleceği: Yeni İnternet Çağı ve İş Dünyasında Değişen Dinamikler

Bazı araştırmacılar yeni bir rönesansa tanıklık etmek üzere olduğumuza, risklerin ve fırsatların çok büyük olduğuna inanmaktadır. Özel blok zincirlerini savunanlar ile Bitcoin ve diğer kripto para projelerine liderlik edenler arasında bir çatışma olduğu söylenebilir. Bu teknoloji çok sayıda sektörde çok sayıda kullanım alanına sahip güven artırıcı bir araca dönüşmüştür. Makine öğrenimi, yapay zekâ ve blok zinciri teknolojisindeki temeli nedeniyle Bitcoin, her türlü değer dijital değişiminin mümkün olduğu yeni İnternet 3.0 veya web 3.0 çağına giriş noktası olarak hizmet etmiştir. Liana Doulliet Guzman'a göre, internet ağına bağlı özel blok zincirleri teknolojinin birincil odak noktası olacaktır (URL-27, 2018).

Günümüzde blok zinciri teknolojisi, insanların değer sahibi olmalarını ve değer alışverişinde bulunmalarını sağlamaktadır. Pierre Joubert'e göre, "blok zinciri ister bir karar ister bir değişiklik olsun, belirli bir anda bir değişikliği doğrulama yeteneği gerektiren hizmetleri esasen etkileyecektir" (Andriy, 2019).

Blok zinciri, Coase'un görüşüne göre, kurumların amacının daha da ötesine geçmektedir. Ekonomist Ronald Coase'un 1937'de ortaya koyduğu gibi, işletme ilkesi lojistik ve bilgiyi merkezileştirerek aktörler arasındaki işlem maliyetlerini düşürmek için geliştirilmiştir. Kuşkusuz hem bireyler hem de maddi ve maddi olmayan varlıklar bir kurumu oluşturur. Çeşitli sanayi devrimlerinin başlamasıyla birlikte, makineler çeşitli görev yapma kapasitelerinde yavaş yavaş insanların yerini almıştır. Kuruluşlarımız prosedürler ve yönergelerle ne ölçüde düzenlenirse, otomasyonları da o ölçüde belirginleşecektir. Blok zinciri eşler arası (P2P) modeli, bilgi aktarımının sürekliliğini garanti ederken aktör güvenliğini de korur. Yapay zekâ ile birlikte bu kayıt modeli, yönetim uygulamalarımızı ve iş modellerimizi kademeli olarak altüst edecek; zekâ artık anlamsız, tekrarlayan görevler için

değil, bilgi yaratmak için kullanılacaktır (Caseau ve Soudoplatoff, 2016).

Bir blok zinciri ağı, oyuncu güvenini ve işlem verimliliğini koruduğu sürece, finansal olsun ya da olmasın her türlü işlemi barındırabilir. Blok zinciri teknolojisi, ekonomik istikrarsızlığa ve temel işlem prosedürlerine neden olmanın yanı sıra, ekonomideki katılımcıları nasıl iş birliği yaptıklarını yeniden gözden geçirmeye zorlayan riskler de oluşturmaktadır.

3.3.1 Blok Zincirlerin Desteklediği Ekonomik İlkeler

Blok zincirinin yıkıcı doğası, bankacılık, sertifikasyon ve para transferleri de dahil olmak üzere bir dizi alanda önemlidir. Bu durum özellikle işlemlerin otomatik olarak ve önemli ölçüde azaltılmış maliyetlerle nasıl gerçekleştirilebileceği göz önünde bulundurulduğunda geçerlidir. İnternet, dağıtık defter teknolojisi ve onun ilk yaratıcısı olan Bitcoin sayesinde aracılık maliyetlerinde ya da bir ağ kurmanın bedelinde önemli bir düşüşten faydalanmıştır (Catalini ve Gans, 2020).

Değer, tarihte ilk kez iki uzak ve güvenilmeyen varlık arasında bir aracıya ihtiyaç duyulmadan güvenli bir şekilde transfer edilebilmiştir.

- **Blok zinciri ve aracılık:** Blok zinciri teknolojisi ile araçların yerini blok zinciri ağına ve onu yönetmek için oluşturulan mutabakat kurallarına duyulan güven alır. Araçların kullanımı hala çoğunlukla gereklidir, ancak sayıları keskin bir şekilde azalmıştır. Aracılık maliyetlerindeki kazançlar, işlem yakında kaydileştirilecek bir malla ilgili olduğunda önemlidir. Maddi bir varlık söz konusu olduğunda (bina, ofisler, metaller vb.), fiziksel gerçeklikle bağlantı kurmak, varlık ile blok zincirindeki kaydı arasında bağlantı kurmak için bir aracının müdahalesini gerektirir.

Son olarak, araçların sayısının azaltılması, örneğin korsanlık durumunda bilginin yayılması ve kullanılması risklerini sınırlandıracaktır.

- **Blok zinciri ve ağ edinimi:** blok zinciri teknolojisi, platform ve hizmet geliştiricilerinin geleneksel araçlara güvenmeden daha düşük maliyetle bir topluluk oluşturmalarını sağlar. ICO'lar (Initial Coin Offerings) aracılığıyla proje finansmanı: Proje başlatılmadan önce projenin değerine ikna olan yatırımcılar tarafından abone olunur. Projenin hızla gelişen bir ağ tarafından kademeli olarak

benimsenmesi, kullanıcıların hizmetlerine erişimini kısıtlayacak, hatta yasaklayacak veya engelleyecek konumda olmayan oyuncuların baskın bir pozisyonunun olmamasıyla kolaylaştırılır.

3.3.2 Blok Zincirlerin Desteklediği Ana İşlevler

Blok zincirinin ekonomiye katkıları:

- **Bilgi veya değerin aracısız iletimi:** Blok zinciri teknolojisinin temel bir özelliği, eşler arası (P2P) işlemlerin aracılar olmadan gerçekleştirilmesini sağlamasıdır. Bazı işlemler, özellikle de iletilen değer somut bir varlıkla ilgili olduğunda, bir aracının müdahalesini gerektirecektir. İşlemlerin güvenilirliği artık güvenilir bir üçüncü taraf tarafından onaylanmamakta, protokol ve ağda yer almaktadır (Lawrens, 1999). Blok zincirleri, şirket kuruluşlarında ticaret mahkemesi kâtibi veya gayrimenkul işlemlerinde noter gibi aracılardan vazgeçilmez olduğu belirli prosedürleri kolaylaştırabilir.
- **Bilgi depolama ve paylaşımı:** Blok zinciri teknolojisinin bir diğer güçlü özelliği de bilgilerin (belgeler, arşivler, sözleşmeler, vb.) merkezi olmayan, paylaşılan bir şekilde depolanmasıdır. Bu bilgiler aynı zamanda değişmez olma avantajına sahiptir ve bunlara erişim ücretsiz olabilir veya yalnızca belirli katılımcılara yetki verilebilir (değiştirme, okuma vb.). Bu işlev, bir operasyonu yönetme maliyetini önemli ölçüde azaltır.
- **Veri ve değerlerin güvenliğini sağlama:** Ağ üyeleri arasındaki alışverişlerin güvenliği bir ağın asimetrik kriptografik teknolojisinden faydalanır ve böylece bir mesajın bozulma riskini sınırlandırır. Madenciler için mesajların gerçekliğini ve geçerliliğini garanti altına almak için bilgisayar problemlerini çözme teşviki operasyonların geçerliliği de belirleyici bir faktördür. Bu, daha önce merkezi olmayan mutabakat bağlamında bahsedilen soruna veya Bizans generalleri sorununa yanıt verir. Tek bir altyapıya değil, bir altyapılar ağına dayanan bir ağ altyapısına sahip olmak da başarısızlık riskini sınırlar. Nitekim, bir veya daha fazla ağ düğümünün kaldırılması tüm ağın kaldırılmasıyla sonuçlanmayacaktır. Bugüne kadar, blok zincirlerine yönelik bilinen saldırılar, blok zinciri protokollerine veya altyapılarına değil, yalnızca kripto para birimi değişim platformlarına odaklanmıştır. Dolayısıyla güvenlik açıkları blok zincirinin kendisinde değil, ortamda yatmaktadır.

- **Bir mal veya hakkın sahipliğinin doğrulanması:** Blok zinciri teknolojisi sayesinde, "akıllı mülkiyet" olarak bilinen bir malın veya hakkın sahipliğini doğrulamak artık mümkün. Teknolojinin "sanal sürekliliği" sayesinde kaydi borsalardaki çifte harcama sorunu çözülmüş oluyor. Daha açık bir ifadeyle, A, B'ye bir dosya gönderdiğinde, B aslında dosyayı değil, dosyanın bir kopyasını alır. Bu sorun blok zinciri teknolojisi ile çözülmüştür: A dosyasını B'ye gönderdiğinde, B artık dosyanın sahibi değildir. Bununla birlikte, güvenilir bir üçüncü tarafın müdahalesi olmadan mülkiyet transferlerini hayal etmek hala zordur. Blok zinciri teknolojisi sertifikasyonla sınırlıdır, ancak eylemin geçerliliğinin ve etkinliğinin doğrulanması anlamına gelen kimlik doğrulama ile sınırlı değildir.

Blok zinciri kullanarak bir varlığın sahipliğinin doğrulanması, varlık maddi değilse ve bu nedenle sayısallaştırılabilirse maksimum, maddi ise zayıftır. Bu gereklidir Unvanın veya dijital imzanın gerçekten söz konusu varlığa ait olduğunu doğrulayabilir.

- **Akıllı sözleşmeler ile belirli görevlerin otomatikleştirilmesi:** Blok zincirleri, unsurları otomatik olarak (koşullar yerine getirilirse) yürütülen bilgisayar programları içermeye kapasitesine sahiptir.

3.3.3 Blok Zincirinin Faydaları ve Sınırlamaları

Pek çok insan blok zincirini duymuştur, ancak ne olduğunu gerçekten bilmemektedir. Bu nedenle, bu teknolojiyi daha anlaşılır kılmak ve herhangi bir yanlış anlamayı önlemek için gizemini kaldırmak çok önemlidir. Bu gizemden arındırma gelecek projeksiyonlarına dayanmamaktadır, ancak teknolojinin mevcut gelişimi için bir çerçeve oluşturmalıdır, bu nedenle bazı mitlerin gerçeğe dönüşmek için evrim geçirmesi gerekecektir. Brant Carson ve Matt Higginson konuya biraz ışık tutuyor (London vd., 2018). İşte ortaya atılan beş efsane.

- Birincisi, blok zinciri doğal olarak Bitcoin ile ilişkilendirmemizdir. Gerçek şu ki, Bitcoin sadece başka bir kripto para birimi uygulamasıdır. Blok zinciri teknolojisi başka birçok uygulama için yapılandırılabilir.
- İkincisi, bu teknolojinin geleneksel veri tabanlarımızdan daha iyi olduğudur. Gerçek şu ki, blok zincirini avantajı, genellikle geleneksel veri tabanını daha

yeterli hale getiren birçok ödün verme (örneğin enerji tüketimi) yükümlülüğüyle birlikte gelir. Teknoloji özellikle oyuncular arasında güvenin az olduğu ve katılımcıların doğrudan alışveriş yapabildiği veya bir aracılığı atlayabildiği belirli ortamlarda kullanışlıdır.

- Üçüncü efsane ise teknolojinin değiştirilemez ya da taklit edilemez olduğudur. Bununla birlikte ağın bilgi işlem gücünün %50'sinden fazlasını kontrol ederek "%51 saldırı" zincirindeki bilgiler.
- Dördüncü fikir ise bu teknolojinin %100 güvenli olduğudur. Kuşkusuz, hacklenmesi zor olan asimetrik kriptografi kullanmaktadır. Blok zinciri, saldırıya uğrayabilecek temel uygulamaları kullanır. En son saldırı, %51'lik bir saldırıda bir platformdan bir milyon avronun çalındığı klasik Ethereum'a yapılmıştır.
- Son olarak, beşinci ve son mit teknolojinin bize mutlak güven verdiğine inanmamıza yol açmaktadır. Teknoloji, tüm defterdeki işlemleri ve bilgileri denetlememizi sağlar. Ancak, fiziksel ve dijital dünyalar arasındaki sınır nedeniyle, teknoloji zincire girilen bilgilerin doğru veya güvenilir olup olmadığını değerlendiremez.

4. BLOK ZİNCİRİ TEKNOLOJİSİNİN FİNANSAL SİSTEMDEKİ POTANSİYELİ

Blok zinciri teknolojisi, elektronik para transferleri, mülkiyet hakları kaydı, finansal menkul kıymet ticareti, finansal sözleşme yürütme planlaması ve kripto para birimi bağış toplama dahil olmak üzere finans alanında uygulamalara sahiptir (Google). Satoshi Nakamoto yıllar önce Bitcoin ödeme sistemini yarattığında, "dağıtık defter" şeklinde kullanıcılar arasında yaygın olarak paylaşılan bir blok zinciri veri tabanı kavramını finans dünyasına getirmiştir. Bu, blok zincirinin finans sektöründeki ilk kullanımıdır. Mükerrer ödemeler sorununu ele almak ve bilgi doğrulama güvenliğini artırmak amacıyla merkezi olmayan bir elektronik ödeme sistemi oluşturmak için çaba sarf etmiştir (Swan, 2015). Bununla birlikte, kripto para birimlerinin popüleritesi arttıkça, blok zinciri teknolojisinin veri güvenliğini artırma ve finansal sistemdeki ahlaki tehlike sorunlarını ele alma yeteneğine sahip olduğu giderek daha açık hale gelmektedir (URL-17, 2019). Bu nedenle, blok zinciri teknolojisi finans sektöründe oldukça hızlı bir şekilde ilgi görmektedir.

Son yıllarda düzinelerce üst düzey borsa, sigorta sağlayıcısı, ödeme işlemcisi, banka ve diğer kuruluşlarda keşif amaçlı blok zinciri uygulamaları başlamıştır.

4.1 Finansal Piyasalarda Blok Zinciri Uygulamaları

Geleneksel finans sisteminde blok zinciri teknolojisi ile bugüne kadar birçok ilerleme kaydedilmiştir. İşlemlerin bir defteri veya günlüğü, blok zinciri adı verilen bir veri havuzunda saklanır. Bu, finansal piyasaları oluşturan mülkiyet ve değer transfer kayıtlarının birleşimidir. Herhangi bir anda piyasanın durumunu anlamak için bir defter gereklidir (Yermack, 2019).

Halka açık veya özel bir ağ üzerinden dağıtılan bir blok zinciri, başarılı bir fonlama piyasası için gereken yüksek kullanılabilirlik ve esnekliği sağlar ve dağıtılmış bir veri tabanı, piyasa çalışma süresini en üst düzeye çıkarmaya ve ağ katılımcıları arasındaki dalgalanmayı azaltmaya yardımcı olabilir (Wu ve Duan, 2019). Geçerli taraflar ve işlemler kriptografik ve hash teknikleri kullanılarak tanımlanabilir. Blok zincirinin kriptografik temelleri, varlık sahipliğinin güvenliğini ve meşruiyetini garanti etmeye yardımcı olabilir. Blok zinciri,

neredeyse deđiřmez ve dođrulanabilir bir denetim izidir. Finans piyasasında gerekleřtirilen her iřlemin eksiksiz, deđiřmez bir kaydı, denetim yeteneklerini geliřtirecek ve takas sũrelerini hızlandıracaktır (Morgan, 2018). Teorik olarak, blok zincirleri veri gũvenliđinin sũz konusu olduđu her sektũre fayda sađlayabilir. Finans sektũrũ dıřında veri gũvenliđini artırmaya yũnelik blok zinciri uygulamaları arasında akademik transkriptler, hayati devlet istatistikleri, gıda gũvenliđi, sađlık hizmetleri ve ok sayıda bařka alan bulunmaktadır. Bununla birlikte, ũncelikle bankacılık ve yatırım piyasalarına odaklanacađız ve gayrimenkul ve ticaret finansmanı gibi yakından ilgili alanlara az miktarda dikkat edilecektir (Yermack, 2019).

4.1.1 Blok Zinciri Tabanlı Bankalar Arası Mutabakatlar

Geleneksel bankalar arası ũdeme sistemleri her zaman aracılara, merkezi otoritelere ve modası gemiř teknolojilere dayanmıř, maliyetleri artırmıř, hata riskini yũkseltmiř ve gecikmelere neden olmuřtur. Finans kurumları artık blok zinciri teknolojisinin geliřimi sayesinde, bankalar arasında aracılar olmadan gerek zamanlı, eřler arası iřlemlere olanak tanıyan uygulanabilir bir ikameye sahiptir (URL-30, 2023). Bankalar arası blok zincirleri, katılımcı bankalar arasında gũvenli ve aık iletiřim sađlayan ũzel veya konsorsiyum tabanlı dađıtılmıř defterlerdir. Bu blok zincirleri, mutabakat algoritmaları ve akıllı sũzleřmeler kullanarak iřlemleri sorunsuz bir řekilde kaydeder, dođrular ve yũrũtũr. Bu sistemler, gũvenlik, denetlenebilirlik ve izlenebilirliđi geliřtirirken ũdeme sũrelerini ve maliyetlerini azalttıkları iin popũler hale gelmiřtir (URL-30, 2023). Kapsamlı, deđiřtirilemez denetim izleri sayesinde bankalar arası blok zincirleri řeffaflık sorununa devrim niteliđinde bir ũzũm sunmaktadır. Blok zinciri, her iřlemi sıralı ve kriptografik olarak kaydederek finansal faaliyetin geri dũndũrũlemez bir kaydını oluřturur. Bu řeffaf iz, her iřlemin hesaba katılmasını ve izlenebilir olmasını sađlar ve finansal kurumlar, dũzenleyiciler ve denetiler tarafından kolayca eriřilebilir (Guo ve Liang, 2016).

Dijital tokenlar bor ũdeme iřlemlerinde ođunlukla kullanılmaktadır. Yeterli miktarda token elde ederek ve bunları ađ ũzerinden karřı tarafın adresine gũndererek, taraflardan biri tokenları gelecekteki takas iřlemlerinde kullanmak ũzere alıkoyarak veya basite ev sahibi banka tarafından tutulan fiat para birimi bakiyelerine dũnũřtũrerek diđerine geri ũdeme yapabilir (URL-18, 2020).

En iddialı projelerden biri, IBM'in Hyperledger blok zinciri platformunu kullanarak 79 üye finans kurumu arasındaki mutabakatları hesaplayan CLS Grup'un CLSNet hizmetidir. Günlük ortalama hacmi 5 trilyon doların üzerinde olan CLS, dünyadaki döviz işlemlerinin yarısından fazlasını gerçekleştiriyor. Kuruluş, CLSNet 'in lansmanında "blok zinciri birincil fırsatı, piyasa oyuncuları arasındaki arka ofis operasyonlarına odaklanıyor; verimliliği ve hızı engelleyen sürtünme ve fazlalıkları ortadan kaldırma fırsatı" demiştir (Yermack, 2019).

JPM Coin, ABD dolarını taklit etmek için 2019'un başlarında piyasaya sürülen, ancak sonunda JP Morgan tarafından çeşitli fiat para birimlerine genişletilecek olan blok zinciri tabanlı bir dijital "stabilcoin", benzer bir projedir. Kurumsal hesap sahipleri JPM Coin'leri bir blok zinciri üzerinden satın alabilir, transfer edebilir ve takas edebilirler; amaç, bunları banka içinde anında değer transferi yapmak için kullanmaktır. JPM Coin 'in hedefleri daha hızlı ödeme süreleri ve hata ve anlaşmazlıklarda azalmadır (JP Morgan yurtdışında yapılan ödemeleri hızlandırmak için bir program başlatmıştır. 75 banka, ABD bankası tarafından ikna edildikten sonra Bankalararası Bilgi Ağı'nı (IIN) katılmayı kabul etti. Bunlar arasında Santander, Kredi Tarım, Tek kredi veya Genel Toplum yer almaktadır. Belirli işlemler artık bankalar arasında her iki yönde de işlenebildiğinden, IIN işlem sürelerini sadece birkaç saate indirmeyi ummaktadır (Andriy, 2019).

Mevcut ödeme sistemindeki karmaşıklıklar ve gecikmeler, teknoloji ilerledikçe ve daha yaygın bir şekilde kullanıldıkça ortadan kalkabilir. Blok zinciri tarafından yönlendirilen ödeme çözümleri, güvenli, etkili ve anlık işlemleri kolaylaştırarak finansal kurumların ve müşterilerin günlük operasyonlarında devrim niteliğinde bir değişim yaratma potansiyeline sahiptir (Oerle ve Lemmens, 2016).

4.1.1.1 Sınır Ötesi Ödemelerde Blok Zinciri Teknolojisinin Uygulanması

Sınır ötesi ödemeler iki veya daha fazla ülke veya bölge arasında finansal transfer yapılmasını sağlar. Sınır ötesi ödeme yapmak için, yabancı bir üreticiden ürün satın alan yerli bir müşterinin bir ödeme aracına ve bir ödeme sistemine güvenmesi gerekir. Sınır ötesi bankalar arası ödeme sistemleri en yaygın kullanılan ödeme yöntemleridir ve yabancı para birimleri en sık kullanılan ödeme araçlarıdır. Yurtdışına para göndermek için en yaygın yöntemler kredi kartı ödemeleri, para transfer şirketleri tarafından yapılan transferler, banka havaleleri ve üçüncü taraf ödemeleridir dünya bankalararası finansal telekomünikasyon

derneği ödeme ağı banka havalelerinin temelini oluşturmaktadır (Collomb ve Sok, Blockchain / Distributed Ledger Technology (DLT): What Impact on the Financial Sector?, 2016). Bu ödeme türü yüksek ücretler ve uzun bir bekleme süresi içerir. Buna ek olarak, ödeme işlemini yurtdışındaki onaylı kuruluşlarla doğrulayan bir para transferi şirketi de sınır ötesi ödemeyi gerçekleştirebilir. İşlem inanılmaz kısa bir süre aldı. Üçüncü olarak, bankanın ödeme ve takas sistemi kredi kartı işlemlerinin temelini oluşturur. Mağazalar, yüz yüze veya çevrimiçi alışverişlerde kredi kartı ödemeleri çoğunlukla yapılmasına rağmen, donanım ve yazılım için çok fazla para harcamak zorunda kalıyor. Son yıllarda ortaya çıkan dördüncü ödeme yöntemi ise üçüncü taraf ödemeleridir. Alipay ve WeChat Pay gibi üçüncü taraf ödeme araçları ile müşteriler, hükümetin bu kurumlara hem yurt içinde hem de yurt dışında tüccarlara ödeme hizmetlerini sunma yetkisi vermesi halinde ödeme yapabilmektedir. Yukarıda bahsedilen geleneksel sınır ötesi ödeme yöntemlerinin operasyonel verimliliği daha düşüktür ve çok sayıda ticari taraf ve aracı içerir (Wu ve Duan, 2019).

Günümüzün ileri teknolojisine rağmen, ödeme altyapısı hala karmaşıklıklar ve gecikmelerle doludur. Sınır ötesi işlemler için birden fazla aracı gereklidir ve her birinin farklı kuralları ve işlem süreleri olduğundan, ödeme süreleri daha uzun ve maliyetler daha yüksektir. Buna ek olarak, geleneksel veri tabanları gerçek zamanlı güncellemeler sağlamak için merkezi ve şeffaf bir mekanizmadan yoksun olduğundan, ödemelerin durumunu bunlar aracılığıyla takip etmek zor olabilir (URL-30, 2023).

Merkezi olmayan ödemeleri kolaylaştırmak için uygun fiyatlı ve güvenilir bir yöntem arayışının bu noktada başladığını söylemek yanlış olmaz. Satoshi Nakamoto'nun beyaz kitabı ve Bitcoin protokolünün ilk uygulaması, Bitcoin ödemelerinin çalışır hale gelmesiyle birlikte ilginin artmasına yol açmıştır. Geleneksel banka ücretlerinden daha düşük işlem ücretleri ve çok daha hızlı ödeme uluslararası bir banka havalesi için birkaç güne kıyasla ilk onay için yaklaşık on dakika ile uluslararası transferler yapmak ve havaleler için ödeme yapmak için etkili bir yol olarak kabul edilmiştir (Collomb ve Sok, Blockchain / Distributed Ledger Technology (DLT): What Impact on the Financial Sector?, 2016).

Blok zinciri teknolojisi, geleneksel sınır ötesi ödeme yöntemlerinin dezavantajlarının üstesinden gelmek ve işlem risklerini azaltmak için sınır ötesi ödeme faaliyetlerinde kullanılabilir (Guo ve Liang, 2016). Dağıtılmış defter teknolojisi, ödeme işleme yöntemlerini iyileştirmeyi ve böylece müşteri gereksinimlerini karşılamayı amaçlamaktadır

(Andriy, 2019).

İşlemlerin anında gerçekleştirilmesi blok zincirinin başlıca avantajlarından biridir. Aracı bankalar ve çeşitli doğrulama adımları nedeniyle, geleneksel sınır ötesi ödemeler birkaç gün sürebilir (Wu ve Duan, 2019). Blok zinciri teknolojisi anında mutabakatı mümkün kılarak likiditeyi artırır ve karşı taraf riskini azaltır.

Geleneksel uluslararası ödemeler, aracı olarak hareket eden bankalar tarafından alınan bir dizi ücretin yanı sıra döviz masraflarını da beraberinde getirir. Bankalar arası blok zincirleri, bu aracıları devre dışı bırakarak ve eşler arası işlemleri doğrudan kolaylaştırarak işlem maliyetlerini önemli ölçüde azaltır ve bankaların ve müşterilerinin uluslararası ödemeleri daha erişilebilir hale getirmelerine yardımcı olur (Oh ve Shong, 2017). Blok zinciri teknolojisinin şeffaflığı, tüm işlemlerin değişmez bir deftere kaydedilmesini sağlar. Bu işlevsellik, gerçek zamanlı denetimleri kolaylaştırarak, finansal kurumların ve düzenleyicilerin mevzuata uygunluğu geliştirmelerine ve potansiyel finansal riskleri azaltmalarına yardımcı olur.

Merkezi olmayan mimarileri nedeniyle blok zincirleri tek bir tarafça kontrol edilemez. Tek bir hata noktasını ortadan kaldırarak, bu merkezi otorite eksikliği sistemin esnekliğini güçlendirir. Karmaşık muhabir bankacılık ilişkilerine veya para birimi dönüşümlerine gerek kalmadan, bankalar arası blok zincirleri sorunsuz sınır ötesi işlemlere olanak sağlayabilir. Dünyanın dört bir yanındaki şirketler ve bireyler, uluslararası ticareti ve ticareti kolaylaştırabilecek bu işlevsellikten faydalanabilir (Wu ve Duan, 2019).

Blok zincirler işlem maliyetlerini düşürür ve sınır ötesi ödemeleri bankalar ve müşterileri için daha uygun hale getirir. Ayrıca, para birimi dönüşümlerine veya kapsamlı muhabir bankacılık ilişkilerine ihtiyaç duymadan sorunsuz sınır ötesi işlemleri kolaylaştırma potansiyeline sahiptirler. Bu işlevsellik küresel ticareti kolaylaştırarak dünya çapındaki işletmelere ve bireylere fayda sağlayabilir (URL-30, 2023).

Teknik açıdan bakıldığında, şu anda faaliyette olan iki protokol vardır: Ripple ve Stellar. Her ikisi de genel Bizans mutabakatının varyantlarını kullanmaktadır. Ripple, zincir üyeleri arasında paylaşılan güncel bir kayıt sağlayan bir mekanizma olan Bizans hata toleransı kullanır. BHT, minimum sayıda düğümün (katılımcı) çözümü kabul etmesi ve doğru

olduğunu onaylaması halinde mutabakatın geçerliliğini garanti eder. Bu mekanizma, herhangi bir katılımcının ağdan ayrılmasına veya ağa yeniden katılmasına izin veren Proof of Work'ün yerini alır. BHT'de ağ üyeleri yeni bir katılımcının gelişini onaylar ya da reddeder. Bugün dünya çapında her gün 1.000 milyar dolar alışveriş yapılıyor ve ödemelerin hızlanması, tüketicilerin artan anıdalık talebine yanıt veriyor ve bunun için blok zinciri teknolojisi birkaç ilginç çözüm sunuyor. Ripple veya Stellar'ın uluslararası transferlerin takası için bir protokol ve kripto para birimi olarak kullanılması, bankaların müşteri hizmetlerini iyileştirmesi ve operasyonel maliyetleri azaltması için fırsatlar yaratacaktır. Şu anda Ripple' in Accenture, Andreessen Horowitz, CME Ventures, Core Innovation Capital, Google Ventures vb. gibi çok sayıda finansal ortağı bulunmaktadır (Wu ve Duan, 2019).

4.1.1.2 Menkul Kıymetleştirme

Menkul kıymetleştirme, ticari alacakların yatırımcılara aktarılmak üzere alınıp satılabilir menkul kıymetlere dönüştürülmesini içerir. Ekonomi büyük ölçüde ticari alacaklarla finanse edilmektedir. Günümüzde ticari alacaklar standartlaştırılmadığı için likit olmayan varlıklardır. Bir şirketin hızlı likidite elde etmek için bu varlığı faktöring veya menkul kıymetleştirme yoluyla satması mümkündür. Bununla birlikte, finansman bankasının alıcı ve satıcıyı tanıma ihtiyacı, ilgili taraflar arasındaki tahsilat ve dava prosedürlerini bilme ihtiyacı ve yapının satın alma fiyatını hesaplama yöntemi nedeniyle satışın maliyeti yüksek kalmaktadır. Blok zinciri teknolojisi ve özellikle tokenizasyon ilkesi sayesinde, bir talebi mümkün olduğunca likit hale getirmek, tüm paydaşlar tarafından basitleştirilmiş izleme sağlamak ve aracı sayısını azaltarak yapısal maliyetleri sınırlamak için standartlaştırmak mümkündür. DLT'ler, günümüzün geleneksel menkul kıymetleştirme işlemleri aylık transferleri içerdiğinden, ödeme sıklıklarını optimize etmek için de kullanılabilir (Andriy, 2019). DLT ile transferler günlük olarak yapılabilir (Rossignol ve Laurent, 2017). Hem bankalar hem de şirketler için maliyetleri azaltmanın ötesinde şirketler için blok zincirinin dağıtık mimarisi, 2008'deki subprime krizine atıfta bulunarak, genellikle opak kabul edilen finansal ürünlere olan güveni artırmaktadır. Geleneksel varlıkların menkul kıymet belirteçleri aracılığıyla menkul kıymetleştirilmesi önümüzdeki yıllarda muhtemelen yeni yatırım araçları haline gelecektir (Andriy, 2019).

4.1.1.3 Blok Zinciri Aracılığıyla Müşteri Tanıma (KYC)

KYC genellikle bir bankanın veya şirketin müşteri doğrulama sürecine verilen addır. Bu faaliyetleri düzenleyen bankacılık yönetmeliklerini ifade eder (Google).

Şirketler için KYC (Müşterini Tanı) sürecinin zor olmasının çeşitli nedenleri vardır. Özellikle büyük müşteri tabanına sahip şirketler için zahmetli ve yoğun kaynak gerektiren bir süreç olabilir. Müşterilerin kimliğini teyit etmek ve durum tespiti kontrolleri yapmak, özellikle yurt dışında bulunan veya karmaşık mülkiyet yapılarına sahip müşterilerle çalışırken çok zaman ve çaba gerektirebilir (Oerle ve Lemmens, 2016). Buna ek olarak, müşterini tanı gerekliliklerinin farklı yetki alanlarında yeknesak ve standart olmaması, uluslararası faaliyet gösteren şirketler için kafa karışıklığına ve ek uyum yüklerine yol açabilir. Ayrıca, müşterini tanı düzenlemelerinin çeşitli düzenleyici kurumlar tarafından yorumlanmasında ve uygulanmasında farklılıklara neden olabilir. Dolandırıcılık ve kimlik hırsızlığı olasılığı KYC sürecinin önünde büyük bir engel olabilir. Hırsızların veya diğer suçluların sahte kimlikler oluşturmak için çalıntı veya tahrif edilmiş belgeler kullanması halinde şirketler dolandırıcılık faaliyetlerini tespit etmekte ve durdurmakta zorlanabilir. Şirketler ayrıca mali kayıplara ve itibar kaybına uğrayabilir (URL-20, 2019).

Veri gizliliği endişeleri de şirketlerin KYC prosedürünü uygulamasını zorlaştırabilir. Müşteri gizliliğini korumak için şirketler, kişisel verilerin toplanması ve saklanmasına ilişkin katı yönergeler içerebilecek tüm geçerli yasa ve yönetmeliklere uyduklarından emin olmalıdır. Listelerdeki bir ögenin varlığının doğrulanması ve işlemlerin ve davranışların gözden geçirilmesi, bilgi toplama ve analiz sürecinin bir parçasıdır (Wikipedia). Her banka için bilginin gerekli olduğu çok bankalı bir operasyonda, taleplerin tekrarlanabilirliği hem finansal kuruluşlar hem de müşteriler için bir zorluk teşkil etmektedir. Bankaların müşteri tanımlama için her yıl en az 500 milyon dolar harcadığı tahmin edilmektedir (Myano ve Ross, 2017). Dağıtık defter teknolojisinin bankalar tarafından benimsenmesi yasal düzenleme maliyetlerini azaltabilir, müşteri memnuniyetini artırabilir ve şeffaflığı geliştirebilir. Derinlemesine müşteri bilgisi için yasal gereklilikler bunu göz korkutucu bir görev haline getirebilir ve bazen ilişkilerin geliştirilmesini engelleyebilir. Bu, kuruluşun büyüklüğüne ve çalışma şekline bağlıdır. Mevcut KYC prosedürünün birçok sorunu ve verimsizliği potansiyel olarak blok zinciri teknolojisi ile çözülebilir (Oerle ve Lemmens, 2016). Arşivlemeyi güvenli, açık ve değişmez hale getiren teknolojiye büyük değer

verilmektedir. Şirketler, blok zinciri teknolojisini kullanarak tüketici verilerini güvenli bir şekilde depolayan ve değişmez bir şekilde değiştiren merkezi olmayan bir kimlik doğrulama sistemi kurabilir.

KYC prosedürleri için blok zinciri teknolojisini kullanmanın en önemli faydalarından biri de verimliliğin artırılmasıdır. Müşteri verileri blok zinciri kullanılarak dijital bir kimlikte güvenli bir şekilde saklanabilir, böylece manuel veri girişi ve kâğıt belgelendirme ihtiyacı ortadan kalkar. Bu, işe alım prosedürünü hızlandırabilir ve daha geleneksel KYC prosedürlerine kıyasla para ve zamandan tasarruf sağlayabilir (Yadav ve Chandak, 2019). Blok zinciri ayrıca KYC prosedürlerinin güvenliğini de artırabilir. Geleneksel KYC prosedürleri tipik olarak müşteri verilerinin merkezi veri tabanlarında depolanmasını içerir ve bu da onları veri ihlallerine ve siber saldırılara karşı savunmasız hale getirir. Buna karşılık blok zinciri, sofistike kriptografik teknikler kullanarak müşteri verilerinin gizliliğini ve güvenliğini korur. Merkezi olmayan bir sistem kullanıldığında bilgisayar korsanlarının verilere erişmesi ve bunları değiştirmesi çok daha zordur (Kapsoulis vd., 2020). Blok zinciri teknolojisi, müşteri verilerine tek ve değişmez bir doğruluk kaynağı sağlayarak veri doğruluğunu artırabilir ve hataları azaltabilir. Bunu yaparken, müşteri verilerindeki eşitsizlikleri ve tutarsızlıkları ortadan kaldırarak dolandırıcılık faaliyeti olasılığını ve mevzuata uygunluk sorunlarını azaltabilir.

Blok zinciri, sahip olduğu özellikler sayesinde, bankaların müşterinin diğer bankacılık kurumları tarafından zaten bilinip bilinmediğini kontrol edebilecekleri kronolojik, merkezi olmayan bir bankalar arası kayıt oluşturulmasını sağlar, böylece mükerrer aramalardan kaçınılır ve uyum maliyetlerinden tasarruf edilir. Bunun avantajı, KYC çalışmasının artık her müşteri için banka tarafından değil, tüm bankalar için müşteri tarafından yürütülecek olmasıdır. José Parra Moyano ve Omri Ross çalışma raporlarında dağıtık defter teknolojisinin kullanımının projeye dahil olan banka sayısına göre tasarrufları en üst düzeye çıkardığını tahmin etmektedir (Myano ve Ross, 2017). Süreci yalnızca bir kez tamamlamaları gerektiğinden müşteri deneyimi de iyileştirilmektedir. Araştırmacılar ayrıca dağıtık defter teknolojisinin (DLT) denetim ve kontrol açısından sunduğu önemli iyileştirmelerin de altını çiziyor. Aslında bu teknolojinin kullanımı, kaydedilen bilgilerin net bir şekilde yedeklenmesini sağlıyor. Her oyuncu, müşterinin paylaşılan veri tabanına kaydedilmesindeki iş birliği için ödüllendirilir. Bankalar arasında rekabet veya güven nedeniyle katılımı anonimleştirmek de mümkündür (Andriy, 2019).

Blok zinciri tabanlı kimlik çözümleri, hassas müşteri verilerinin yönetilmesini ve güncellenmesini kolaylaştırırken, gelişmiş gizlilik ve güvenlik sunabilir. KYC süreci, örneğin, kullanıcılara kişisel kimlik verileri üzerinde kontrol sağlayan kendi kendine egemen bir kimlik sistemi kullanılarak geliştirilebilir (URL-31, 2019).

KYC süreci blok zinciri teknolojisi ile daha verimli hale getirilebilir, ancak kullanılan tüm çözümlerin GDPR ve AML/KYC düzenlemeleri de dahil olmak üzere yürürlükteki tüm yasa ve düzenlemelere uygun olmasını sağlamak çok önemlidir (Eduardo Demarco, 2020).

Blok zinciri tabanlı KYC çözümlerinin standartlaştırılması ve daha geniş çapta benimsenmesinin teşvik edilmesi, diğer sektör oyuncularıyla iş birliği yapılarak gerçekleştirilebilir. Diğer kuruluşlarla iş birliği, insan hatasını en aza indirmek ve önceden belirlenmiş düzenlemelere uyumu sağlamak için kaynakların ve uzmanlığın paylaşılmasını da kolaylaştırabilir. Akıllı sözleşmeler, KYC sürecindeki belirli adımları otomatikleştirme yeteneğine sahiptir. KYC sürecinin verimliliğini artırın (Kapsoulis vd., 2020).

Blok zinciri tabanlı KYC çözümlerinin uygulanması, tıpkı diğer tüm teknolojilerde olduğu gibi veri güvenliği gerektirir. Hassas müşteri verileri şifreleme ve ek güvenlik önlemleri kullanılarak korunabilir (Eduardo Demarco, 2020).

Güvenlik ve verimlilikte iyileştirmeler öncelikli olsa bile, KYC sürecinin kullanıcı dostu olmasını ve müşterilere aşırı bir yük getirmemesini sağlamak hayati önem taşır. Kullanıcı dostu bir arayüz sağlamak müşteri memnuniyetini ve benimsenmesini artırabilir (URL-20, 2019).

4.1.2 Sermaye Piyasalarında Blok Zincirleri

Sermayenin kapsamlı sınır ötesi akışı, sermaye piyasalarının geliştirdiği birbirine bağlı bankalar ve araçlardan oluşan sofistike küresel ağ sayesinde mümkün olmaktadır.

Birden fazla aracı her işlem için kendi veri silolarını tutmakta, bu da gereksiz veri girişine, gereksiz mutabakat hatalarına, verimsiz sermaye kullanımına ve mutabakat gecikmelerine neden olmaktadır (URL-12, 2016).

Menkul kıymetlerin takası, mutabakatı ve alım satımının yanı sıra hissedar oylaması ve sözleşmelerin akıllı sözleşmeye dayalı olarak uygulanması gibi daha geleneksel süreçlerle ilgili çok sayıda konu blok zinciri teknolojisiyle ilişkilendirilmiştir. Blok zinciri teknolojisi sermaye piyasalarında çeşitli pilot programlar aracılığıyla kullanılmaktadır. Daimler Benz, Dünya Bankası ve Toplum Genel blok zinciri platformlarında tahvil ihraç etti ve Estonya Menkul Kıymetler Borsası'nda listelenen şirketlerde hissedar oylaması bir blok zinciri üzerinde organize edilmektedir (Yermack, 2019).

Yatırım sektörü genelinde yürütülen bu tür pek çok proje arasında, dağıtık defterler ve blok zincirleri kullanılarak hisse senedi piyasalarının çağdaştırılması olasılığı muhtemelen kamuoyunun en büyük ilgisini çekmiştir. Mevcut sistemler çok karmaşık olduğundan, blok zincirleri hisse senedi piyasalarında takas ve mutabakat için caziptir. Düzenlenmiş bir piyasada işlem yapmak, oyuncular arasında genellikle karmaşık ve zaman alıcı olan çok taraflı bir müzakere sistemi gerektirir (Andriy, 2019). Örneğin, bir hisse senedi işlemi söz konusu olduğunda, Fransız Para ve Finans Kanunu uyarınca, kayda giriş hisse alım emrinin iletilmesinden iki gün sonra gerçekleşir (Vamparys, 2018). Bu karmaşıklık, şirketler, aracılar ve takas kurumları tarafından tutulan ve hiçbirisi bir şirketin tedavüldeki hisselerinin gerçek sahipliğine ilişkin tam ve güncel bir görünüme sahip olmayan, üst üste binen ve eşzamanlı olmayan hisse sahipliği kayıtları sisteminin bir eseri gibi görünmektedir (Yermack, 2019). Blok zinciri teknolojisi, bu karmaşık ve yavaş mekanizmayı bozma ve değiştirme potansiyeline sahipken, aynı zamanda bu oyuncuların tüm gezegenin ekonomisinin kendi içlerindeki merkezileşmesi nedeniyle temsil ettikleri sistemik riski de düzeltmektedir. Teknolojinin bu finans kurumlarının yerini alıp almayacağını söylemek için henüz çok erken. Büyük olasılıkla, finans kuruluşları bu teknolojiyi mevcut operasyonlarına dahil edecek ve piyasada faaliyet gösteren çeşitli oyuncuların bu hizmet için ücret alacak ve maliyetlerini önemli ölçüde azaltacaktır. Blok zincirindeki menkul kıymet alım/satım döngüsünün dolaysızlığı, mevcut bankacılık mekanizmasının müdahalesini gereksiz hale getirebilir. Bu süreçte likidite ve fiyat oynaklığı riskini azaltabilirse, toplum bir bütün olarak minnettar olacaktır. Finans piyasasının bu merkezi organlarının taşıdığı riski azaltmanın ötesinde, blok zinciri teknolojisi borsaların şeffaflığı ve güvenliği konusunda gerçek bir ilerleme sağlamaktadır. Merkezi olmayan, güvenli ve kolayca denetlenebilir bir kayıt defteri olarak blok zinciri, herhangi bir anda kimin hangi sözleşmeye sahip olduğunu bilmeyi mümkün kılan "ticaret deposu"dur: düzenleyicilerin sahip olmayı hayal ettiği bir nesne

(Andriy, 2019).

Moody'ye göre: "Blok zinciri teknolojisi, hisse senedi ticaretinin birçok yönünü dönüştürebilir ve potansiyel olarak finans kurumlarının maliyetleri düşürmesini ve menkul kıymet işlemlerinin gerçekleştirilme hızını artırmasını sağlayabilir (URL-13, 2017)."

Blok zincirinin sunduğu özellikler, menkul kıymet/nakit takasının anlık olması karşı taraf ve piyasa risklerini ortadan kaldırdığından, takas kurumları gibi oyuncuların artık bir varoluş nedenine sahip olmadığını göstermektedir (Andriy, 2019).

Katya Malinova ve Andreas Park, "blok zinciri teknolojisi ile Ticaret için Piyasa Tasarımı" adlı çalışmalarında, finans piyasası için dağıtılmış defter modeline teorik bir yaklaşım sunmaktadır (Malinova ve Park, 2017). Vardıkları sonuçlar şu şekildedir: teknoloji, değişim ve paylaşım için yeni bir mimari sağlayarak finansal piyasa katılımcıları arasındaki etkileşimleri geliştirebilir. Her şeyden önce, akıllı sözleşmeler yoluyla alım satım kurallarının otomasyonu, borsaları daha akıcı hale getirir. Bunlar mevcut broker sistemlerine dahil edilebilir. Bu arada eşler arası etkileşim, sürtünmeyi ve ilgili maliyetleri azaltır ve piyasayı daha fazla oyuncuya açar. Bir zincirdeki tüm oyuncular tarafından görülebilen açık anahtar, güvenilir bir üçüncü tarafa veya paralel sisteme ihtiyaç duymadan alıcı ve satıcı arasındaki iletişimi kolaylaştırır. Likidite arayışı, örneğin bir menkul kıymetin açık anahtarlarını (alıcılar/satıcılar) tarayarak karşı tarafı bulabilen ve işlemi anında gerçekleştirebilen blok zinciri tarafından kolaylaştırılır. Bu kesinlikle broker düzeyinde mevcuttur, ancak bir sürtünmeyi temsil eder. Blok Zinciri'nin borsa sistemini basitleştirmesi, sahipliğin içsel olarak doğrulanmasını sağlayarak aracı kurumda bir hesaba sahip olma ihtiyacını ortadan kaldırır. Dahası, sahiplik bilgileri, düzenleyiciler gibi hesap sahibi veya sahibi dışındaki oyuncular tarafından kullanılabilir (Malinova ve Park, 2017).

Blok zincirlerinin neredeyse anlık işlem gerçekleştirmeye olanak tanınmasıyla birlikte, birçok start-up yeni hisse senedi ve türev piyasaları kurma girişiminde bulunmaktadır. Piyasaya yeni giren bu şirketlerin hiçbiri şu anda büyük borsaları tehdit etmese de birçoğu hala ilgi çekmeye çalışmaktadır (Yermack, 2019).

Hisse alım satımı açısından dünyanın en büyük 8. piyasası olan Avustralya Menkul Kıymetler Borsası (ASX), kısa bir süre sonra hisse alım satımının yanı sıra takas odasını da

yönetmek için ilk kez blok zinciri teknolojisini benimseyecek. CHES olarak bilinen mevcut sistem kısa bir süre sonra yerini, sistemi hem hissedarlar hem de düzenleyiciler için daha verimli ve şeffaf hale getirecek olan dağıtık defter teknolojisine (DLT) bırakacak. Avustralya Menkul Kıymetler Borsası, 2021 yılına kadar tüm takas ve mutabakat işlemlerini bir blok Zinciri'ne geçirmeyi planlıyor (Andriy, 2019). ABD'de, birçok hisse senedi ve türev piyasasının takas merkezi olan Depository Trust Clearing Corp, blok zinciri platformları için benzer bir doğrulama programı başlattı. Blok zinciri platformları geliştirmek, ABD'deki hissedar seçimlerinin çoğunda vekalet oylarını sayan Broadridge'in operasyonlarını daha güvenli ve verimli hale getirmeye çalışmasının bir başka yöntemidir. ABD'nin en büyük varlık yönetim şirketlerinden biri olan Vanguard Grup tarafından sunulan endeksli hisse senedi fonlarının ünlü portföyü, temel endeks üyelerinin kesin ve güvenli bir şekilde temsil edilmesine bağlıdır. Vanguard Grup, borsa endekslerinin bileşimini bir blok zinciri platformunda takip etmek için Symbiont ile ortaklık kurmuştur. ABD'nin ünlü teknoloji borsası ve ABD'deki hisse senedi işlem hacmi bakımından en büyük 2. Nasdaq, blok zinciri teknolojisinin işindeki potansiyel kaldırıcına güçlü bir şekilde inanıyor ve teknolojinin menkul kıymetlerin yerleşimi ve transferiyle ilgili olduğunu düşünüyor ve bu süreçte teminat transferini kolaylaştırıyor. New York borsası da teknolojiyi oylama süreçlerinde kullanmak istiyor. Bu amaçla, şirketlerin, yatırımcıların ve piyasa altyapısındaki tüm oyuncuların oylama süreçlerinin maliyetini ve daha genel anlamda karmaşıklığını ve karar almanın operasyonel yönünü azaltmalarını sağlayan blok zinciri tabanlı bir teknoloji olan eVoting'i yarattı. Web tabanlı bir platform ve blok zinciri altyapısı aracılığıyla eVoting, şu anda çok yaygın olan bir dizi veri, erişim ve güvenlik sorununu çözmektedir (Andriy, 2019).

Bu sermaye piyasası girişimlerinin neredeyse tamamı son kullanıcılar için şeffaf değildir, çünkü işletmeden müşteriye bir strateji yerine işletmeden işletmeye bir strateji uygulamaktadırlar. Kullanıcıların platformla etkileşim biçimine müdahale etmeden müşteri deneyimini hız, güvenilirlik ve güvenlik açısından geliştirerek, sermaye piyasalarının "tesisatını" iyileştirmeyi amaçlamaktadırlar.

4.1.2.1 Sermaye Piyasalarında Uygulanan Blok Zincirleri

Pek çok kişi, işletmelerinin dayanıklılığını artırırken aracılık yapmama, hızı artırma ve maliyetleri düşürme konusunda blok zincirinin potansiyelini araştırmaktadır (URL-12, 2016). İşte blok zincirinin ticari uygulamalarından sadece birkaç örnek:

Yerleşimler; Aracıları ortadan kaldırarak ve yetkili verilerin paylaşılan, güvenilir bir görünümünü sağlayarak, blok zinciri işlem maliyetlerini azaltır, blok zinciri maliyetleri azaltabilir (örneğin daha az mutabakat hatası), Uzlaşmayı hızlandırabilir (örneğin daha hızlı doğrulama), Esnekliği artırabilir (örneğin tek bir arıza noktası yoktur), Şeffaflığı artırabilir (örneğin izlenmesi daha kolaydır).

Teminat Yönetimi; Blok zinciri, daha hızlı mutabakat ve varlık bilgilerinin paylaşılan, güvenilir bir görünümünü sağlayarak yeni teminat gereksinimlerini çözebilir, kullanılmayan varlıklardan yararlanmamızı sağlayabilir, operasyonel karmaşıklığı ve maliyetleri azaltabilir, esnekliği artırabilir (URL-13, 2016).

Onaylar; Onaylanmış yaşam döngüsü sözleşmeleri, blok zincirinde akıllı bir sözleşme oluşturularak otomatikleştirilebilir. Güven ve şeffaflığı artırmak (örneğin ortak bir altın veri kaynağı ile), Maliyetleri azaltmak (örneğin mükerrer veri girişi ve mutabakat hatalarını azaltarak), Operasyonel riski azaltmak, Koşullu riski daha iyi ölçmektedir.

4.1.2.2 Piyasanın Beklediği Yapısal Değişim “Blok Zinciri”

Blok zinciri vizyonu, sermaye piyasalarının yapısında büyük bir değişimi açıkça temsil etmektedir. İlgili düzeyini anlamak için blok zincirinin alım satım öncesi, alım satım, alım satım sonrası ve menkul kıymet hizmetleri alanlarındaki faydalarını düşünmek faydalı olacaktır (Wyman, 2016).

Ön Müzakere; Varlıkların şeffaflığını ve doğrulanmasını sağlar, kredi riskini azaltır, statik verileri bir havuzda topluyor ve varlıklara erişim yoluyla KYC/KYCC1'i basitleştirir.

Müzakere; İşlemlerin güvenli, gerçek zamanlı eşleştirilmesini ve anında geri alınamaz mutabakat, bir defter üzerinde otomatik DVP, otomatik raporlama ve piyasa yetkilileri için daha şeffaf denetim, daha katı AML2 standartları sağlar.

İşlem sonrası: Anlık nakit işlemleri için merkezi takasın olmaması, marj ve teminat ihtiyaçlarının azalması, daha hızlı ikmal ve daha etkili bir işlem sonrası iş akışı, blok zinciri varlıklarının otomatik olarak gerçekleştirilen değiştirilebilir akıllı sözleşmeler olan teminat olarak kullanılmasıdır.

Menkul kıymet saklama ve hizmeti; Menkul kıymetlerin saklanması ve servisi, Doğrudan bir blok zinciri üzerinde birincil ihracı mümkün kılar, Servis süreçlerini otomatikleştirir ve tekilleştirir, Düz muhasebe hiyerarşileri ile merkezi veri setlerini daha zengin hale getirir, Ortak referans verilerini mümkün kılar, blok zincirinde otomatik olarak işlenen abonelikleri / itfaları yönetir, Fon servisini, tahsis muhasebesini ve yönetimini basitleştirir.

4.1.2.3 Piyasa Yapısı Üzerindeki Etkileri

Piyasa katılımcılarının rolleri, iş modelleri üzerinde önemli bir etkiye sahip olacak bu sistemik değişimin bir sonucu olarak değişecektir (Wyman, 2016).

Müşteriler

Birçok müşteri (özellikle alıcı taraftaki), sermaye piyasası ticareti ve menkul kıymet hizmet maliyetlerinin azalmasından en büyük faydayı elde etmeyi bekleyecektir. Perakende ve toptan yatırımcılar, açık piyasalarda garantili uygulama ile birbirleriyle işlem yapabileceklerdir.

Komisyoncular

Aracılar, varlıklar için daha iyi likidite bularak piyasada değerli bir rol oynamaya devam edecek ya da HFT'ler yeni bir işlem yapmadan önce her takas döngüsünde (yalnızca birkaç saniye de olsa) beklemek zorunda kalacaktır. Bu da faaliyet hızlarında önemli bir yavaşlamaya neden olacaktır ki bu da blok zincirinin erişiminin yalnızca HFT'nin önemsiz olduğu piyasalardaki işlem sonrası süreçlerle ya da HFT'lerin blok zinciri mutabakat döngüsü aracılığıyla düzenli olarak temizlenen kredi limitleri üzerinden işlem yapmasına olanak tanıyan hibrit modellerle çalışabilecek piyasalarla sınırlı kalacağı anlamına gelebilir.

Bağımsız ticaret firmaları

Özel ticaret şirketleri, özellikle piyasa yapıcılar ve yüksek frekanslı tüccarlar (HFT'ler), neredeyse gerçek zamanlı bir mutabakat prosedüründen büyük ölçüde etkilenecektir. Alım satımın varlık satışından önce sahipliğin doğrulanmasına geçmesi, muhasebenin sağlanan diğer hizmetlerden ayrılması ve müşterilere olan cazibelerinin ve diğer hizmetleri (teminat

yönetimi gibi) satma yeteneklerinin aşınması.

Yürütme mekanları

İcra yerleri bugün olduğu gibi kalabilir, fiyat keşfini kolaylaştırabilir ve işlem yapmak isteyen tarafları bir araya getirebilir. İşlem sırasında kriptografik imza tarafından üretilen veriler aynı zamanda mutabakat için gerekli veriler olarak hizmet ettiğinden, icra merkezlerinin oynadığı rolün değeri artmaktadır. Ancak, HFT gibi alım satım stratejilerinin işlem hacimlerinin (ve dolayısıyla komisyon gelirlerinin) önemli bir kısmını oluşturduğu göz önüne alındığında, piyasa yapısındaki köklü değişikliklerin borsalar ve diğer alım satım platformları üzerinde zincirleme bir etkisi olabilir.

Merkezi Saklama Kuruluşları (CSD)

Varlık konularının gözetiminin koordine edilmesi ve piyasanın düzgün işleyişinin sağlanması ihtiyacı devam etmektedir. Depozitlere gelince, büyük defter ana emisyon varlıklarının varış noktası haline gelebilir, CSD geleneklerinin operasyonel yönetim rolünü oynamasını bekleyebiliriz, büyük defter protokollerinin evriminin koordinasyonundan sorumlu, büyük defterdeki jetonların tanıtımı veya iptalinin yönetimi, düzenleyici ile arayüz vb.

Merkezi karşı taraflar

Neredeyse gerçek zamanlı nakit uzlaşmalı bir varlık işlemi söz konusu olduğunda, artık işlemin merkezi olarak takas edilmesine gerek yoktur (çünkü her iki taraf da işlemten önce karşı tarafın işlemin şartlarını yerine getirebileceğini bilir ve takas neredeyse anında gerçekleşir). Ancak, daha uzun bir yaşam döngüsüne sahip işlemler (türevler gibi), takastan faydalanmak ve gelecekteki karşı taraf kredi riskini (değiştirme riski) azaltmak için CCP yeniliğinin faydaların ihtiyaç duymaya devam etmektedir.

Yetkililer

Saklama kuruluşlarının ve alt saklama kuruluşlarının bugün oynadığı rol, düz muhasebe yapılarına sahip dağıtılmış varlık defterleri tarafından kısmen ortadan kaldırılabilir. Saklama

kuruluşları, varlık bilgilerini muhafaza etmenin ve otomatik menkul kıymet yönetimi prosedürlerinin doğru şekilde yürütülmesini sağlamanın yanı sıra, nihayetinde "kilit bekçisi" rolünü de üstlenebilirler. Likidite düşük olduğunda, bu durum anapara riskine yol açabilir. Piyasa erişimi sunmanın aksine, birincil değerleri fiyat belirleme, işlem tavsiyesi ve uygulama yönetimi olacaktır.

4.1.3 Gayrimenkulde Blok Zincirleri

Gayrimenkul insanların temel bir varlığıdır. Bir ev barınma ihtiyacını karşıladığı gibi birçokları için de emeklilik için temel yatırım aracıdır (Malviya, 2017).

Gayrimenkul, büyük bir zenginlik kaynağıdır ve mülk tapularının siyasi otoriteler tarafından tutulduğu kayıt sistemlerine dayanmaktadır. Bu kurumlar dünyanın birçok bölgesinde mevcut olmayabilir, tutarsız olabilir, siyasi etkilere maruz kalabilir veya eksik olabilir. Bankalar, avukatlar, sigortacılar, tapu şirketleri, düzenleyiciler, vergi daireleri ve müfettişlerin dahil olduğu karmaşık bir işlem olan bir ofis binası satın alımını düşünün. Her adımı kontrol etme ve kaydetme maliyeti, hepsi ayrı kayıtlar tutan bu oyuncular tarafından karşılanmaktadır. Bir işlemin tamamlanması ortalama 50 ila 60 gün sürüyor. Blok zinciri teknolojisi, işlemin tüm unsurlarını gösteren, tüm katılımcılar tarafından görülebilen güvenilir, güvenilir, değişmez bir dijital defter olarak bir çözüm sunar (Malviya, 2017). Tapuların blok zincirlerine kaydedilmesi mülkiyet haklarını netleştirebilir ve güvence altına alabilir, bu da ticari yatırımları ve ekonomik büyümeyi finanse etmek için gayrimenkulün teminat olarak kullanılmasını teşvik edebilir (Yermack, 2019). Blok zinciri, gayrimenkullere aşağıdaki gibi birçok fayda sunar: Güven ve şeffaflık; blok zinciri, veri paylaşmanın sorgulanamaz ve sansüre dayanıklı bir yolunu sunar. Paylaşılabilen ve aynı zamanda kurcalamaya karşı dayanıklı veri tabanları sağlar. Verimli işlemler; İşlemler hiçbir zaman ve ekstra maliyet olmadan gerçekleştirilebilir. Aracıların kullanımı; blok zinciri, üçüncü tarafların veya aracılardan kullanımını veya katılımını sınırlandırabilir. Bu şekilde, ek maliyetler ve dolandırıcılık faaliyetleri sınırlandırılabilir veya ortadan kaldırılabilir (Joy ve Sebastian, 2020).

De Soto'ya (2000) göre, güney yarımkürenin büyük bir bölümündeki az gelişmişliğin başlıca nedenlerinden biri, güvenli mülkiyet sistemlerinin yokluğudur. ABD gibi gelişmiş ülkelerde bile, mülkiyet kayıtlarındaki eksiklikler önemli işlem maliyetlerine ve sürüşmelere yol

açmaktadır (De Soto, 2000). Blok zinciri tabanlı ulusal mülkiyet kayıtları önerilmiştir ve bazı durumlarda şu anda Honduras, Gana ve Gürcistan da dahil olmak üzere bir dizi geliştirmekte olan ülke tarafından inşa edilmektedir.

Gayrimenkul ve arazi işlemleri blok zinciri kullanılarak gerçekleştirilebilir. Blok zinciri kullanarak emlak işlemlerimizi daha güvenli ve daha hızlı hale getirebilir.

Kayıtlı bir kullanıcı yalnızca blok zinciri kullanarak bir mülk satın alabilir veya satabilir. Blok Zinciri'nin akıllı sözleşmeleri mülk işlem sürecini kolaylaştıracaktır. Alıcı ve satıcı şartlar ve koşullar (arazi ile ilgili detaylar) üzerinde anlaştıktan ve alıcı işleme devam etmek istedikten sonra, akıllı bir sözleşme yardımıyla arazi üzerinde işlem yapılabilir (Joy ve Sebastian, 2020).

Dolayısıyla, alıcı ve yararlanıcı arasında bir işlem gerçekleştiğinde, akıllı sözleşme tarafından aralarında bir sözleşme oluşturulur. Oluşturulan bu akıllı sözleşme, işlem kanıtı olarak kullanılabilir. Satıcıya aktarılması gereken para da blok zinciri üzerinden aktarılabilir. Banka veya komisyoncu gibi üçüncü bir tarafın yardımı olmadan doğrudan satıcıya teslim edilebilir.

Bu teknolojiyi sadece mülk satın almak veya satmak için değil, aynı zamanda sahip olduğumuz mülkü kiralamak için de kullanabiliriz. Kiracı ve ev sahibi, şartlar ve koşullar konusunda dijital olarak akıllı bir sözleşme imzalayabilir. Şartlar ve koşullar arasında kira ücretleri, kira süresinin uzunluğu ve ödeme sıklığının yanı sıra her bir tarafın ayrıntıları da yer alabilir (Kejriwal ve Mahjan, 2017) . Üzerinde anlaşmaya varılan hüküm ve koşullara bağlı olarak, akıllı sözleşmeler ev sahibi ve kiracı arasında otomatik olarak bir sözleşme oluşturur. Akıllı sözleşmeler ayrıca kiracının ev sahibine kira ödemesini ve sözleşme feshedildiğinde depozitonun kiracıya ödenmesini otomatik olarak tetikleyebilir (Joy ve Sebastian, 2020).

Bugüne kadar, blok zinciri tabanlı bir tapu sistemine yönelik en kapsamlı girişimler, ulusal tapu sicili Lantmäteriet'in mülk transferleri için bir blok zinciri platformu oluşturduğu ve başarıyla test ettiği İsveç'te gerçekleşmiştir. İsveç sisteminden sorumlu şirket ChromaWay, 2018 sonunda Avustralya'nın Yeni Güney Galler eyaletinde benzer bir pilot program kurmak üzere sözleşme imzalamıştır (Yermack, 2019).

4.1.3.1 Blok Zincirinin Gayrimenkul Piyasasına Etkileri

Blok Zinciri'nin gayrimenkul piyasasını etkileyeceği 3 yol şunlardır (Malviya, 2017):

a) Süreci hızlandırmak

Geleneksel emlak piyasası kolay ve hızlı bir piyasa değildir. Aracıların kullanımı gayrimenkul işlemlerini her zaman zaman alıcı, maliyetli ve karmaşık hale getirmiştir. Bu araçlar, sizin sahip olmadığınız bilgi veya lisanslara sahip oldukları için ya da mevcut gayrimenkul işlem ekosisteminde işlev görmeleri gerektiği için gereklidir. Her iki tarafın da işlemi tamamlamasını garanti altına almak ve dolandırıcılık olasılığını azaltmak için bir güvenlik önlemi olarak, günümüzde alıcı ve satıcıların çoğu üçüncü taraf doğrulaması için emanet ve tapu şirketlerini kullanmaktadır.

Çok önemli olmasına rağmen, bu üçüncü taraf doğrulaması pahalıdır ve tamamlanması daha uzun sürer. Bu durumda aracı olan emanet şirketi blok zinciri teknolojisi ile başarılı bir şekilde ortadan kaldırılabilir. Sahipler, bağımsız üçüncü taraf doğrulaması için ödeme yapmak zorunda kalmadan, gerçekliği doğrulamak için blok zinciri tarafından sağlanan bir veri tabanını kullanarak mülkiyeti anında ve yasal olarak aktarabilirler.

Tüm mülkler blok zincirinde karşılık gelen bir dijital adrese sahip olabilecek ve bu adres önceki tüm işlemleri sürekli olarak iletecek ve saklayacaktır. Bu adres bina performansı, doluluk, finans, yasal hususlar ve fiziksel nitelikler hakkında bilgiler içerecektir. Verilerin tüm mülkler arasında ilişkilendirilmesi ve anında çevrimiçi olarak erişilmesi de mümkün olacaktır. İşlemlerin hızı günler, haftalar ve aylardan dakikalar veya saniyelere indirilecektir.

b) Dolandırıcılığın önüne geçilmesi

Bir tarafın emlak dolandırıcılığının kurbanı olma olasılığını azaltmak, alıcı

ve satıcıların tarihsel olarak emanet ve üçüncü taraf doğrulama tekniklerini kullanmalarının başlıca nedenlerinden biridir. Emlak dolandırıcılığı, farkında olmayan alıcılara her yıl milyonlarca dolara mal olmaktadır ve bir işlemi hızlı bir şekilde tamamlamak isteyen ve bu nedenle güvenlik önlemlerinden vazgeçmeye hazır olan alıcılar veya satıcılar tarafından daha da kötüleşmektedir. Yüz milyonlarca dolar değerinde işlemler gerçekleştiren dünyanın en büyük bankaları ve ipotek kreditorlerine kadar 500 dolarlık alt kiralardaki küçük çaplı hırsızlar tarafından gerçekleştirilmektedir.

Blok zinciri, fonların göndericisinin ve alıcısının kayıtlı olduğu ve gayrimenkul için "dijital mülkiyet sertifikalarının" güncel tutulduğu tamamen bozulamaz bir kaynak sunarak sahte mülkiyet belgelerini ve listelemelerini esasen ortadan kaldıracaktır (Malviya, 2017). Sistemdeki bir mülke doğrudan bağlı olan ve sahip olmadığınız bir mülkü listelemeyi veya satmayı neredeyse zorlaştıran türünün tek örneği "dijital mülkiyet sertifikalarını" kopyalamak neredeyse zor olacaktır."

c) Tam şeffaflık sunmak

Programlanabilme özelliği blok zincirine gücünü veren şeydir. Örneğin, bir filmi oynatmak, bir birey, işletme veya gayrimenkul parçası için dijital bir kimlik oluşturmak veya akıllı bir sözleşme (programlanabilir bir emanete benzer) geliştirmek için programlayabilirsiniz (Ullah ve Al- Turjman, 2021). Mülkün tapu zincirinin, yapılan tüm onarım ve iyileştirmelerin bir listesinin ve beklenen mülkiyet ve bakım maliyetlerinin bir tahmininin eklenmesiyle, gayrimenkule kendi sanal kimliği atanabilir.

Blok zincirini bu kadar güçlü kılan şey programlama kabiliyetidir. Bir filmi oynatmak, bir kişi, şirket veya gayrimenkul için dijital bir kişilik yaratmak veya akıllı bir sözleşme (programlanabilir bir emanete benzer şekilde işlev gören) oluşturmak için programlamak mümkündür. Mülkün tapu zincirini, yapılan tüm onarım ve geliştirmelerin bir envanterini ve beklenen sahip olma ve bakım maliyetlerinin bir tahminini içerdiğinde gayrimenkul kendi

sanal kimliğine sahip olabilir (Ullah ve Al- Turjman, 2021).

Akıllı bir sözleşme kullanarak, bir taraf yerine getiremezken diğer taraf yerine getirmeyi reddeder veya yerine getiremeyecektir. Satıcı taraf A ve alıcı taraf B aynı işlem üzerinde anlaşabilir, ancak akıllı bir sözleşme sayesinde bunu farklı şekilde yapılandırabilirler. Taraf B, Taraf A'nın Taraf B'ye belirli bir miktarda sanal para ödemesi karşılığında mülkün mülkiyetini blok zincirindeki benzersiz bir coin türüne vermeyi kabul eder. A Tarafı sanal para birimini B Tarafına aktardığında B Tarafı otomatik bir tetikleyici olay alır; B Tarafı daha sonra A Tarafına söz konusu kat mülkiyetinin sahipliğini temsil eden benzersiz jetonu otomatik olarak gönderir. Bu şekilde transfer tamamlanır ve blok zincirindeki kamuya açık bir kayıt A Tarafının kat mülkiyeti üzerindeki sahipliğinin teyit edilmesini sağlar (Malviya, 2017).

4.1.3.2 Gayrimenkul Tokenizasyonu

Blok zinciri teknolojisinin kullanılmaya başlanmasıyla birlikte emlak sektöründe tam anlamıyla bir yenilenme yaşanmıştır. Güven ve şeffaflık eksikliği gibi sorunları gizleme kabiliyeti nedeniyle, daha önce dijital gayrimenkul sahipliğinden dışlanan kişilerin bunu yapmasını sağlamıştır.

Büyük sermaye gereksinimleri ve uzun süren işlem prosedürleri nedeniyle, gayrimenkul tarihsel olarak çok likit olmayan bir varlık olmuştur. Ancak tokenleştirme ile bu durum değişmiştir. Ayrıca, blok zinciri teknolojisi daha önce hiç görülmemiş bir şeffaflık düzeyi getirmiştir. Bununla birlikte, tokenize edilmiş gayrimenkul alıcıları artık işlemleri değişmez bir şekilde gerçekleştirebilmektedir (Malviya, 2017).

Gayrimenkulün tokenleştirilmesi, bir varlığın tüm hak ve sorumluluklarıyla birlikte gerçek mülk yerine geçen dijital tokenlara bölünmesini içerir. Bir sözleşmenin ayrıntıları akıllı sözleşmeler kullanılarak tanımlanır. Önceden belirlenmiş bir sözleşme koşulunun karşılanması durumunda, dijital sözleşmenin algoritması kodda belirtilen olayları başlatacaktır (Gupta vd., 2020).

Gayrimenkulün tokenleştirilmesi, bir varlığın blok zincirinde çalışan otomatik bir program

olan akıllı bir sözleşme kullanılarak daha küçük kısımlara bölündüğü kitle fonlamasına benzer. Gayrimenkulün bir kısmı, bir token satın alan veya edinen kişiye aittir. Hem dayanak varlık hem de ilgili kazanç veya kayıplar onlarındır.

Açıklığa kavuşturmak adına, birisinin hızlı nakit paraya ihtiyacı olduğunu ve 100.000 dolarlık bir mülke sahip olduğunu varsayalım. Ancak yatırımcılar onlara yaklaştığında, gerekli fonlara sahip değiller ve mülk sahipleri mülklerini daha azına vermeyecektir.

İşte bu durumda tokenleştirme faydalı olmaktadır. Varlıkları, her bir birim tarafından temsil edilen 1.000 \$ değerinde dijital token ile dağıtılacaktır. Bu şekilde, varlığa zaman içinde yatırım yapmak kolaylıkla yapılabilir. Bu işlem merkezi olmayan bir ağ üzerinden yapıldığı için şeffaflık garanti edilir (URL-19, 2023).

Ticari, konut ve hatıra gayrimenkullerinin tümü tokenize edilebilir. Kısmi dilimler, yatırım maliyetini düşürmek için alışveriş merkezleri ve alışveriş merkezleri gibi pahalı ticari mülkleri parçalamak için kullanılabilir (Latif vd., 2020). Çok katlı konut kulelerindeki dairelerin tokenlaştırılmasıyla hızlı satış ve alımlar mümkün hale gelir. Tokenlaştırma süreci, bir kişinin kupa varlıklarını satarken projeler için para toplamasına olanak tanır.

Ödül varlıkları, yatırımcılar arasında yüksek talep gören çok nadir mülklerdir. Ganimetler, önemli gayrimenkul temellerine sahip ikonik yapıları içerir. Bu her zaman bir bina olmayabilir. Sonuç olarak, dijital bir hissedenden tapunun bir bölümüne, teminatlandırılmış borçtaki bir mülkiyet hissesine veya tüzel kişilikteki bir öz sermaye payına kadar her şeyi tokenlaştırmak mümkündür (Gupta vd., 2020).

Özellikle veri şeffaflığı söz konusu olduğunda, ticari gayrimenkul sektörü teknolojik bozulmaya hazırdır. Aracı kurumlar, kurumsal yatırımcılar ve pahalı piyasa veri sağlayıcıları, piyasa bilgilerine kimin erişebileceği konusunda sıkı bir kontrole sahiptir. Yatırım araçlarının alıcı ve satıcılarla olan ilişkileri ve onlardan bilgi edinme kapasiteleri onları vazgeçilmez kılmaktadır. Öte yandan, ticari gayrimenkul alım satımında yer alan çok sayıda idari ve yasal engel nedeniyle işlemler pahalı ve zaman alıcıdır (Joy ve Sebastian, 2020).

Bitcoin'e benzer şekilde, gayrimenkul varlıkları da blok zinciri sayesinde tokenize edilebilecek ve alınıp satılabilecektir. Gayrimenkullerin unvanları ve sahiplik kayıtları blok

zincirinde saklanacak ve bir mülkün değerini temsil eden bir token, değerini belirtmek için kullanılacaktır. Ticari binalar için dijital bir adres, blok zinciri teknolojisi ile mümkün olacak ve binanın doluluğu, fiziksel özellikleri, yasal durumu, geçmiş performansı ve finansal durumu hakkında ayrıntıları içerecektir. Ticari mülk verileri dünya çapında yayılmaya devam ettikçe komisyoncular artık bilgi asimetrisi avantajına sahip olmayacak. Bilgiler mülk türleri ve alt pazarlar arasında anlaşılabilir ve çevrimiçi olarak erişilebilir olacaktır. Yatırımcılar olası alımlar hakkında daha kolay bilgi edinebildiklerinde, yatırım brokerlerinin yardımcı olmadan binaları fiyatlandırmak daha kolay olacaktır (Latif vd., 2020).

Evrensel bir gayrimenkul blok zincirinin üzerinde çalışan bir uygulama olarak bir değişim platformu geliştirilirse, pazarın altyapısı, iki tarafın gayrimenkul işlemlerini çok daha hızlı ve uygun maliyetli bir şekilde gerçekleştirebileceği şekilde değişebilir. Hisse senetleri gibi ticari gayrimenkul ticareti yapabilirsiniz. İşlem süresi haftalar veya aylar yerine dakikalar olacaktır. Ticari komisyoncuların bilgi avantajı blok zinciri teknolojisi sayesinde azalacak, operasyonel engeller azalacak ve eşler arası ticari gayrimenkul ticaretinin önü açılacaktır. Giderek daha likit ve aktif olarak işlem gören bir varlık sınıfı ticari gayrimenkul olacaktır (Malviya, 2017).

4.1.3.3 Gayrimenkulün Tokenlaştırılmasından Elde Edilen Kazançlar

Gayrimenkul sektörü, bir dizi şaşırtıcı değişikliği beraberinde getiren tokenizasyondan büyük ölçüde faydalanabilir (Gupta vd., 2020). Blok zincirlerinin merkezi olmayan mimarisi işlemleri şeffaf ve değiştirilemez hale getirir, bu da onları birden fazla tarafın dahil olduğu ve karmaşık süreçlere sahip gayrimenkuller için mükemmel kılar. Otomatikleştirilmiş akıllı sözleşmeler aracılığıyla insan müdahalesi işlem sürecinden çıkarıldığında haksız anlaşmalar ortadan kalkar (Ullah ve Al- Turjman, 2021).

Blok zinciri sistemlerinde evrak işi yoktur ve işlemler anında tamamlanır. Bu sayede hızlı aksiyon ve hızlı işlemler gerçekleşir. Gayrimenkulde blok zinciri, geleneksel bankacılık sisteminin aksine, işlemlerin tamamlanması için belirlenmiş ofis saatlerine olan ihtiyacı ortadan kaldırır. Bunun yerine, şeffaf sistem sürekli ve günün her saati çalışır (URL-19, 2023).

Çoğu zaman gayrimenkul elit bir yatırım seçeneği olarak kabul edilir. Öte yandan tokenleştirme, gayrimenkul yatırımını daha küçük yatırımcılar için de erişilebilir hale getirmiştir. Daha küçük bütçeli yatırımcıların, yüksek maliyeti nedeniyle gayrimenkule katılma konusunda cesaretleri çoğunlukla kırılmaktadır.

Bununla birlikte, gayrimenkul yatırımının tokenleştirilmesiyle oyun değişti ve pazar perakende ve küçük ölçekli gayrimenkul alıcılarına açıldı. Büyük varlıklar, tokenleştirme yoluyla yönetilebilir parçalara indirgenerek makul bir fiyatla ilgili tarafların kullanımına sunuluyor (Gupta vd., 2020).

Piyasanın serbest akışı, merkezi finansal sistemler tarafından zarar görmektedir çünkü bu sistemler yüksek düzeyde düzenlenmekte ve çoğunlukla taraflı olmaktadır. Blok zincirine dayalı tokenleştirme, gayrimenkul sektörünü merkezi olmayan, önyargısız bir finansal sistemle tanıştıır. Her paydaşın bir dereceye kadar kontrol gücü vardır ve grup olarak karar verirler. İrrasyonel engeller ortadan kaldırıldığında piyasa daha verimli hale gelir ve ilgili tüm taraflara büyümek için eşit fırsat verir.

Uzun işlem zincirlerinin izini sürmek zordur. Tokenlaştırılmış gayrimenkulden önceki günlerde bu bir sorun teşkil ediyordu çünkü üçüncü taraflar işin içindeydi, bu da durumu bulanıklaştırıyor ve şeffaflıktan uzak hale getiriyordu. Düzenleyici perspektifler, blok zinciri tabanlı işlemlerin temel bir bileşeni olan akıllı sözleşmelerle geliştirilmiştir (Ullah ve Al-Turjman, 2021). İşlem zinciri kısa tutulur ve minimum insan etkileşimi olduğunda zayıf halkalarla ilişkili riskler ortadan kaldırılır. Sonuç olarak, tamamen ortadan kaldırılmasa bile karşı tarafın müdahil olma olasılığında önemli bir azalma söz konusudur (Malviya, 2017).

4.1.4 Ticaret Finansmanında blok Zincirleri

Tedarikçiler ve alıcılar arasında mal ve hizmet ticareti ile ilgili riskleri azaltmak için kullanılan çeşitli finansal araçlar ticaret finansmanı olarak adlandırılır. İthalatçı ve ihracatçıları içeren uluslararası ticari işlemler ticaret finansmanının ana odak noktasıdır. Ticaret finansmanı, esas olarak uluslararası ticarete odaklanmış olmasına rağmen, alıcılar ve satıcılar arasındaki yurt içi işlemler için de kullanılabilir (URL-32, 2023).

Yerel bankaların ve küresel finans ve kredi piyasalarının kredi kaynaklarının kullanımı ile ticaret finansmanı, müşterilerin uluslararası ticaret anlaşmalarını finanse etmesine olanak tanıyan teknikler, araçlar ve sistemler koleksiyonunu ifade eder (Dicaprio ve Jessel, 2018).

Ticaret finansmanı ürünleri çoğunlukla alıcılar veya ithalatçılar tarafından ödeme yapılmaması riskini ve satıcılar veya ihracatçılar tarafından üzerinde anlaşılan şartların dışında teslimat yapılması riskini azaltmak için kullanılır (Kowalski vd., 2021).

Üçüncü bir taraf, tipik olarak bir banka veya bir ticaret finansmanı şirketi, iki taraf bir işleme girdiğinde anlaşma şartlarının yerine getirildiğinden emin olmak için bir aracı olarak hizmet eder.

Kredi mektupları, kredi limitleri ve farklı sigorta ürünleri yaygın ticaret finansmanı ürünlerine örnektir. Ticaret finansmanı alanında, akreditifler birincil tekliftir. Genellikle alıcının bankası tarafından sağlanırlar ve satıcının ürün teslimatı için gereklilikleri yerine getirmesi koşuluyla anlaşma şartlarına uygun olarak ödeme yapılmasını sağlarlar (Nurmukhametov vd., 2018). Sözleşme tarafları, akreditifler ve diğer ticaret finansmanı ürünleri ile sözleşmelerden kaynaklanan dolandırıcılık ve anlaşmazlıklara karşı korunmaktadır. Ayrıca döviz dalgalanmaları, kanunlardaki ani değişiklikler, siyasi huzursuzluk ve piyasa istikrarsızlığı gibi dışsallıklara karşı da korunmaktadır (Kowalski vd., 2021).

Modern ticaret finansmanını kolaylaştırma çabalarına rağmen, bürokratik, yavaş ve karmaşık işlemler hala modern ticaret finansmanını karakterize etmektedir. İşlemlerin maliyeti ve karmaşıklığı, çoğunlukla çok sayıda aracı içermeleri nedeniyle artmaktadır (URL-15, 2022). İhracatçılar ve ithalatçılar, riski azaltan ve krediyi genişleten ticaret finansmanı yardımıyla uluslararası ticaret yapabilirler. Bu, dünya finans sisteminin hayati bir bileşenidir, ancak çoğunlukla güncelliğini yitirmiş yazılı ve manuel belgeler kullanılmaktadır. Pek çok ticaret finansmanı faaliyeti hala kâğıt işi ve zahmetli manuel süreçler içermektedir. Faturalar, akreditifler ve diğer evrak işleri birçok ticaret finansmanı işlemi için gereklidir (Kowalski vd., 2021).

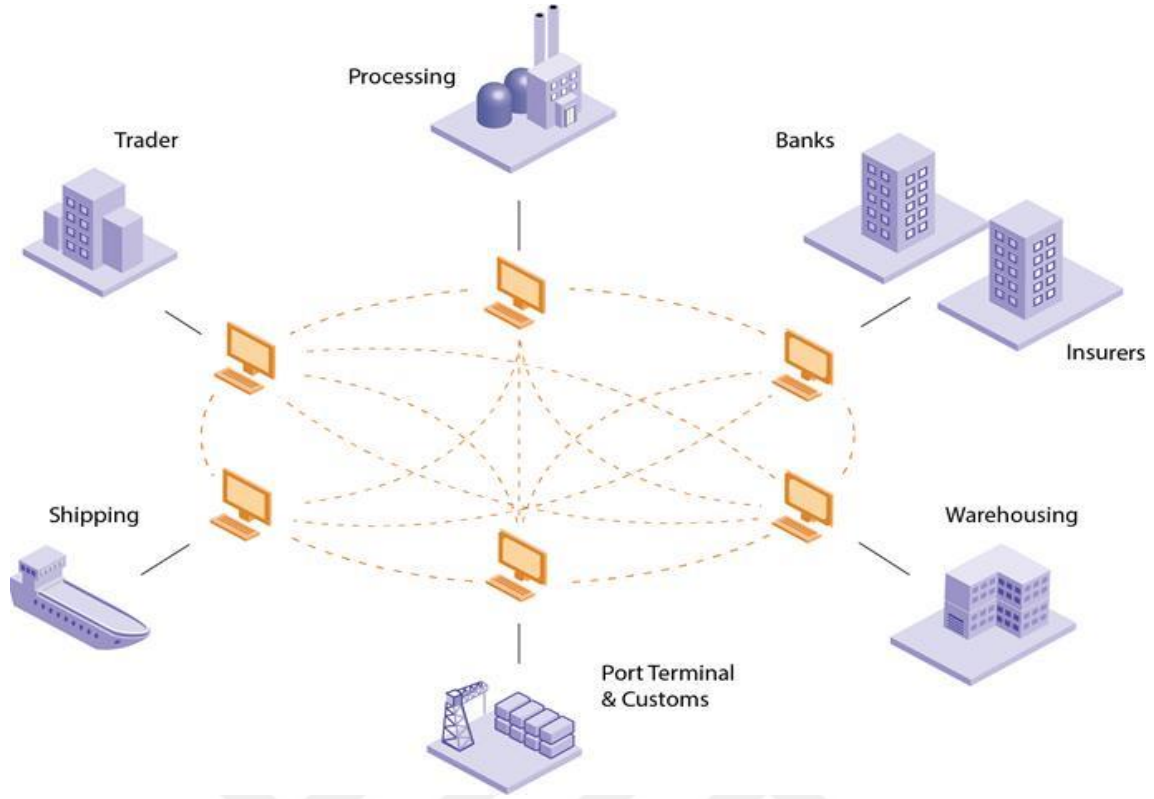
Blok zinciri teknolojisi, karmaşık ticaret finansmanı alanını basitleştirme ve hızlandırma potansiyeli sunarak ithalatçılara, ihracatçılara ve finansörlerine her yıl milyarlarca dolar

tasarruf sağlar. Akıllı sözleşmeler ve kripto para birimleri, ithalatçılar ve ihracatçılar tarafından otomatik ödeme gerektiren kurallar oluşturmak için kullanılabilir.

Ticaret programlarında zaman içinde daha yaygın hale gelmiş olsa da blok zinciri teknolojisi krediler ve konşimentolarda ancak yakın zamanda ana akım bir rol oynamaya başladı. Ticaret finansmanı piyasası, tıpkı diğer pek çok sektörde olduğu gibi, modası geçmiş, maliyetli ve emek yoğun manuel belgelendirme prosedürlerinin getirdiği lojistik aksaklıkları uzun süredir yaşamaktadır. Ödemenin alındığını garanti etmek için, bir tarafın bankasından diğer tarafın bankasına fiziki bir akreditif hala sıklıkla kullanılmaktadır. İşletmelerin menşeyi, ürünleri, işlem ayrıntılarını ve diğer tüm belgeleri güvenli ve dijital olarak doğrulamasını sağlayan blok zinciri teknolojisi sayesinde, transit halindeki gönderiler hakkında daha şeffaf ve ithalatçılar ve ihracatçılar için daha güvenli olacaktır. Bu sayede yüksek derecede güven sağlanır (URL-18, 2020).

Geleneksel ticaret finansmanı sistemlerinde, her üye işlemle ilgili belgelerden oluşan bir veri tabanını muhafaza etmekten sorumludur. Buna ek olarak, bu veri tabanlarının her biri arasında sürekli olarak bir karşılaştırma yapılmalıdır. Bir belgenin farklı veri tabanlarındaki kopyaları, orijinal belgeyle aynı hataları içerebilir. Blok zinciri aynı belgenin farklı versiyonlarının saklanması gerektirmez. Veriler, tüm ağ üyeleri tarafından erişilebilen ve gerçek zamanlı olarak güncellenebilen tek bir dijital kopya halinde birleştirilebilir (Kowalski vd., 2021). Dolandırıcılık riski, özellikle malların ve belgelerin hareketine ilişkin gizlilik ve gözetim eksikliği söz konusu olduğunda, ticari taraflar için en büyük endişelerden biridir. Bu da aynı sevkiyatın birden fazla kez ipotek altına alınmasını mümkün kılmaktadır. Bu, emtia ticaretini finanse eden bankaların bunu gerekli bir masraf olarak yazmasına neden olacak kadar sık gerçekleşen üzücü bir olaydır. Blok zinciri teknolojisi sayesinde ithalatçılar ve ihracatçılar arasında malların teslimi veya teslim alınması üzerine tokenize formda ödemeler yapılabilir. İthalatçılar ve ihracatçılar, otomatik ödemeleri mümkün kılan ve kaçırılan, süresi dolan veya yeniden sigortalanan teslimat şansını ortadan kaldıran akıllı sözleşmelerle kurallar oluşturabilirler (URL-18, 2020).

Ticaret finansmanında blok zinciri teknolojisinin kullanılması sayesinde müşteriler malların menşeyi ve sevkiyat tarihleri hakkında daha fazla bilgiye sahip olmaktadır. Bu veriler geleneksel sistemlerde çoğunlukla eksiktir. Ayrıca güven ve şeffaflığı artıran blok zinciri, müşterileri işlemin her adımında bilgilendirir (Kowalski vd., 2021).



Şekil 4.1: Ticaret finansmanı;

Kaynak: <https://phemex.com/academy/blockchain-in-trade-finance>

Bankacılık kurumları ve diğer ticaret finansmanı ürünleri sağlayıcıları blok zinciri teknolojisinden aşağıdaki şekillerde kazanç elde edebilirler:

Artan ürün teşhiri: Ticaret finansmanı sağlayıcıları, yeni veya özelleştirilmiş ürünleri platforma bağlı çok sayıda potansiyel müşteriye sunmak için blok zincirini kullanabilir. Bu, ürünün benimsenme oranlarının artmasına ve bankaların genellikle ürünlerin iş geliştirmesiyle ilgili olan pazarlama, tanıtım ve reklam giderlerinden tasarruf etmesine neden olabilir (Dicaprio ve Jessel, 2018).

Blok zinciri teknolojisi sayesinde yeni müşteri segmentlerine ulaşılabilir. Küçük ve orta ölçekli işletmeler (KOBİ'ler) geleneksel sistem aracılığıyla ticaret finansmanı elde etmeyi zor bulmaktadır, ancak blok zinciri bunu makul bir maliyetle yapmalarını mümkün kılmaktadır. Bu nedenle bankalar bu yeni pazarın farkına varabilir (Nurmukhametov vd., 2018).

Sektör düzeyinde kapsamlı analitiklere erişim: Blok zinciri üzerine inşa edilen ticaret finansmanı platformları bankalar için harika bir bilgi kaynağı olabilir. Tipik olarak, bir bankanın veya başka bir ticaret finansmanı sağlayıcısının erişebildiği tek ticari işlem, kolaylaştırdığı işlemlerdir. Bu sağlayıcılar, blok zinciri teknolojisi sayesinde daha fazla ticari işleme ve bunlarla birlikte gelen analitiğe erişebilir. Blok zincirinde gerçekleşen farklı ticari işlem türlerini gözlemleyebilmek içgörünü olabilir. Bir analitik sağlayıcı, örneğin ticaret finansmanının genel olarak genişlediği, ancak onlar için müşteri eksikliğinin olduğu yeni bir sektöre yönlendirilebilir (URL-15, 2022).

Belgelendirme ve onay sürecinin kolaylaştırılması: Ticaret finansmanı sağlayıcıları, belgelendirme ve onay prosedürlerini kolaylaştırmak için blok zinciri teknolojisinin kullanımından büyük ölçüde faydalanabilir. Ürünleri onaylamak için gerekli tüm verilerin derlenmesi ve onaylanması, geleneksel ticaret finansmanı sisteminde genellikle zahmetli ve zaman alıcı bir prosedürdür. Blok Zinciri'nin birleştirilmiş, güvenli ve otomatik olarak doğrulanmış verileri sayesinde bu prosedürler kolaylıkla basitleştirilebilir (Kowalski vd., 2021).

Blok zinciri, alıcılar ve satıcılar için ticaret finansmanında aşağıdaki faydaları ve fırsatları sağlamaktadır:

Tek bir platformdan çok sayıda ticaret finansmanı seçeneğine erişme imkânı: Alıcılar ve satıcılar, katılımcı bankalar platformunda yeni ürünler sundukça, sunulan daha geniş bir ürün yelpazesine kolayca göz atabilir ve değerlendirebilir. Tipik olarak, bir ticaret finansmanı şirketi, her bir sağlayıcıdan yeni ürünler hakkında bilgi almak, bu ürünleri değerlendirmek ve karşılaştırmak ve en iyi seçeneği seçmek için önemli miktarda zaman ve kaynak yatırımı yapmalıdır. Bu da uzun ve zorlu bir alışveriş deneyimine dönüşür. Birçok müşteri, daha önce kullandıkları ticari finansman şirketiyle çalışmaya devam ederek bu karmaşıklıklardan kaçınmaktadır. Müşteriler arasında yeni bir sağlayıcıya geçerek tasarruf edebilecekleri yaygın bir bilgidir. Ancak sağlayıcı değiştirmek zaman ve para gerektireceğinden, insanlar genellikle "her zaman kullandıkları" sağlayıcıya bağlı kalmaya zorlanmaktadır. Daha iyi bir teklife geçmek ve yeni ürünler ve sağlayıcılar seçmek blok zinciri ile daha hızlı ve kolay hale getirilmiştir (URL-15, 2022).

KOBİ'ler artık geleneksel ticaret finansmanı ürünlerini daha makul fiyatlı hale getiren blok zinciri teknolojisi sayesinde geleneksel sistemde kendileri için mümkün olmayan yollarla ticaret finansmanına erişebiliyor. Geleneksel ticaret finansmanı ürünleri, mevcut ticaret finansmanı uygulamalarının risklerini ve karmaşıklığını içerecek şekilde fiyatlandırıldığından, küçük işletmeler genellikle bunları karşılayamamaktadır. Sağlayıcılar da dahil olmak üzere her paydaş için blok zinciri, ticaret finansmanı ile ilişkili riskleri, giriş maliyetlerini ve karmaşıklığı azaltır. Bu sayede KOBİ'ler daha makul fiyatlı ürünlerden faydalanabilir (Basumatary ve Joshi, 2022).

Siparişin uygulanmasının her adımının basit takibi: İşletmeler, özellikle alıcılar olmak üzere, blok zincirinin sunduğu birleşik verilere erişimden faydalanabilir. Aracı sürecinin her adımında, siparişlerinin yerine getirilmesini basitçe izleyebilirler.

Keşfedilecek yeni pazarlar bulun: Müşteri işletmeler, araştıracakları yeni pazarlar bulmak için blok zinciri tabanlı ticaret finansmanı platformlarını kullanabilirler. Bu platformların genellikle çok çeşitli pazarlar, müşteriler ve tedarikçiler hakkında veri ve analizler içermesi nedeniyle, alıcılar ve satıcılar yeni pazarlara girmeyi araştırmak için bu bilgileri kullanabilir (Basumatary ve Joshi, 2022).

Bütünleştirilmiş belgelendirme: Müşteri işletmeler, tıpkı bankalar gibi, kendi ticaret finansmanı evrak işlerini basitleştirmek için blok zincirini kullanabilir. Ticaret finansmanı evraklarını saklamak, erişmek ve güncellemek için çoğunlukla kendi dahili sistemlerini kullanmak zorunda olan müşteriler, blok zincirinde birleştirilmiş ve kolayca erişilebilir belgelerden faydalanacaktır (URL-15, 2022).

4.1.5 Blok Zincirle Ticaret Finansman Sistemlerini Geliştirme Örnekleri

Birçok işletme ve banka uzun vadeli bir çözüm arayışında olduğundan, ticaret finansmanında blok zincirinin zamanı gelmiş olabilir. Ticaret finansmanını yönetmek için blok zinciri teknolojisini kullanmayı vaat eden bir konsorsiyumun üyeleri arasında Standard sözleşmesi ve HSBC olmak üzere iki banka bulunuyor. R3 ve CryptoBLK tarafından yönetilen ve kâğıt akreditifleri dijitalleştirmek için bir blok zinciri platformu işleten bu tür bir gruba Voltron adı veriliyor. On dört ülkede pilot projeler gerçekleştirildikten ve elliden fazla şirket ve banka uluslararası denemelere katıldıktan sonra bir Akreditifin (L/C)

işlenmesi için geçen süre beş günden yirmi dört saatten daha kısa bir süreye indirildi. 2020'de adını Contour olarak değiştirdi ve R3 ve bir dizi ek banka tarafından desteklenen dijital bir ticaret finansmanı ağını tanıttı (URL-18, 2020).

DBS ve Standard Chartered, ABN Amro, Deutsche Bank, ICICI Bank ve Lloyds'u içeren blok zinciri tabanlı bir ticaret finansmanı platformu olan ticaret finansmanı sicilliyi geliştirmek için Ekim 2020'de on iki diğer bankayla güçlerini birleştirdi. Platform, tek bir işlemde gerçek zamanlı dolandırıcılık tespiti ve finansmanın ikiye katlanmasına yardımcı olacaktır (URL-16, 2022).

Blok zinciri sonunda projeden çıkarıldı. Ticaret Finansmanı Sicili, DLT tarafından geliştirilen bir testin ardından platformu geliştirmek için MonetaGo'yu seçti. Blok zinciri MonetaGo'nun küresel ölçekteki ihtiyaçları için yeterince etkili olmadığından, şirket dolandırıcılığı durdurmak için blok zincirini kullanmak yerine hassas verileri işlemeye karar verdi. Bu, blok zinciri girişimlerinin çoğunlukla teorik hedeflerinin gerisinde kaldığını gösteren klasik bir vaka çalışmasıdır. Israeli Wave gibi fintech şirketleri tarafından geliştirilen platformlar sayesinde finans grupları artık mektupla kredi verme işlerini bir blok zinciri çözümü olarak sunabiliyor. Wave, Ornu ve Seychelles Trading Company'ye bir blok zinciri çözümü sunmak için 2016 yılında Barclays ile iş birliği yaptı. Bu, belgelerimizi müşterilerimize daha hızlı aktarmamızı, işlem maliyetlerini düşürmemizi ve tedarik zincirimizi kolaylaştırmamızı mümkün kılmaktadır. Ayrıca dokümantasyondaki hataları azaltmamıza da yardımcı oldu. Bu örnekte, yaklaşık 100.000 \$ değerindeki peynir ve tereyağı için işlem süreci, akreditifin düzenlenmesinden onaylanmasına kadar her zamanki yedi ila on gün yerine dört saatten az sürdü. Wave ayrıca bir Akdeniz nakliye şirketi ile birlikte Hapag-Lloyd'un elektronik konşimento çözümünü kullanıyor. Dijital Konteyner Nakliye Derneği (Container Shipping Association) (DCSA), nakliyecilerin yarısının Wave gibi bir elektronik konşimento sistemi kullanması halinde denizcilik sektörünün yılda 4 milyar dolardan fazla tasarruf edebileceğini iddia etmektedir (URL-18, 2020).

Avustralya ve Japonya artık ticaret yapabiliyor; ticari belgelerin teslim edilmesi ve akreditiflerin düzenlenmesi gibi ticaretle ilgili prosedürler blok zinciri ve DLT sayesinde kolaylaştı. IBM, bu örnekte Linux Vakfı tarafından geliştirilen Hyperledger Fabrika ticaret sürecini uyguladı ve korudu. Ticaret finansmanı edinme prosedürlerini kolaylaştırmanın yanı sıra, tüm bu projeler finans kuruluşlarının her müşteriyi ve işlemi derinlemesine

incelemesinin ne kadar önemli olduğunu vurgulamaktadır. Ve blok zinciri bu konuda yararlı bir araç olduğunu göstermiştir (URL-16, 2022).



5. FİNANS ALANINDA BLOK ZİNCİRİ TEKNOLOJİSİ KULLANIMI İLE İLGİLİ BAŞLICA ENGELLER VE KISITLAR

Günümüzde teknoloji ve iş dünyasında en popüler sözcüklerden biri blok zinciridir. Çalışması için merkezi bir otorite ya da aracı gerektirmediğinden, finans sektörünü tamamen dönüştürecek teknoloji olarak görülmektedir. Diğer yeni teknolojiler gibi blok zincirinin de sınırlamaları vardır ve her tür iş modeli için uygun değildir (Monrat vd., 2019).

Finans sektöründe blok zinciri uygulaması, teknolojik, organizasyonel ve kullanıcı ile ilgili konuların yanı sıra toplumsal ve yasal sorular da dahil olmak üzere çeşitli zorluklarla karşı karşıyadır (Gan vd., 2021).

Küresel standartların ve protokollerin eksikliği, boşa harcanan kaynaklar, disk alanı kısıtlamaları vb. yaygın teknik zorluklara örnektir. Blok zinciri çok fazla enerji tükettiğinden ve birçok düğüm diğer düğümler tarafından yapılan hesaplamaları çoğaltarak ağı bir bütün olarak yavaşlattığından ek zorluklar ortaya çıkarmaktadır. Verim, ölçeklenebilirlik, ağ saldırıları ve güvenlik açıkları diğer yaygın zorluklardır (Banerjee ve Chandani, 2022).

Çeşitli nedenlerden dolayı, bazı gruplar ve bireyler blok zincirine karşı çıkabilir. İlk olarak, sistemdeki tüm bankalar blok zinciri ağını paylaşacağından, blok zinciri bankalar arasındaki rekabeti caydıracak ve kendi sistemlerini geliştirme yeteneklerini engelleyecektir. Buna ek olarak, blok zinciri teknolojisinin mevcut sisteme ve iş akışına başarılı bir şekilde entegre edilmesi, iş akışında bir değişiklik gerektirmektedir (Gan vd., 2021).

Buna ek olarak, blok zinciri teknolojisi düzenleyici ve sosyal riskleri de beraberinde getirmektedir. İşgücü piyasası değişmekte, yaygın teknolojik çözümler daha standart hale gelmekte ve yeni teknolojilerin cirosu yasal düzenlemelere tabi olarak sosyal riskler oluşturmaktadır. Blok zinciri teknolojisi bir tür dağıtık defter teknolojisidir. Çeşitli yasal riskler barındırır ve özellikle kara para aklama, dolandırıcılık ve terör finansmanı gibi mali suçlara karşı hassas olabilir. Devletten uzak ve tamamen kullanıcı mutabakatı ile kendi kendini yöneten ağlar için tasarlanmıştır (Yeoh, 2017).

Gelecekteki yasama ve düzenleme sorunları, blok zincirinin gerçek dünya uygulamalarında kullanılmasını zorlaştırabilir. Blok zinciri teknolojisinin karşılaştığı zorluklardan biri de

bankacılık ve finans sektörüne girmektir.

Blok zinciri teknolojisinin zorlukları ve sınırlamaları aşağıdaki gibi açıklanmaktadır:

5.1 Blok Zinciri Yanılsaması

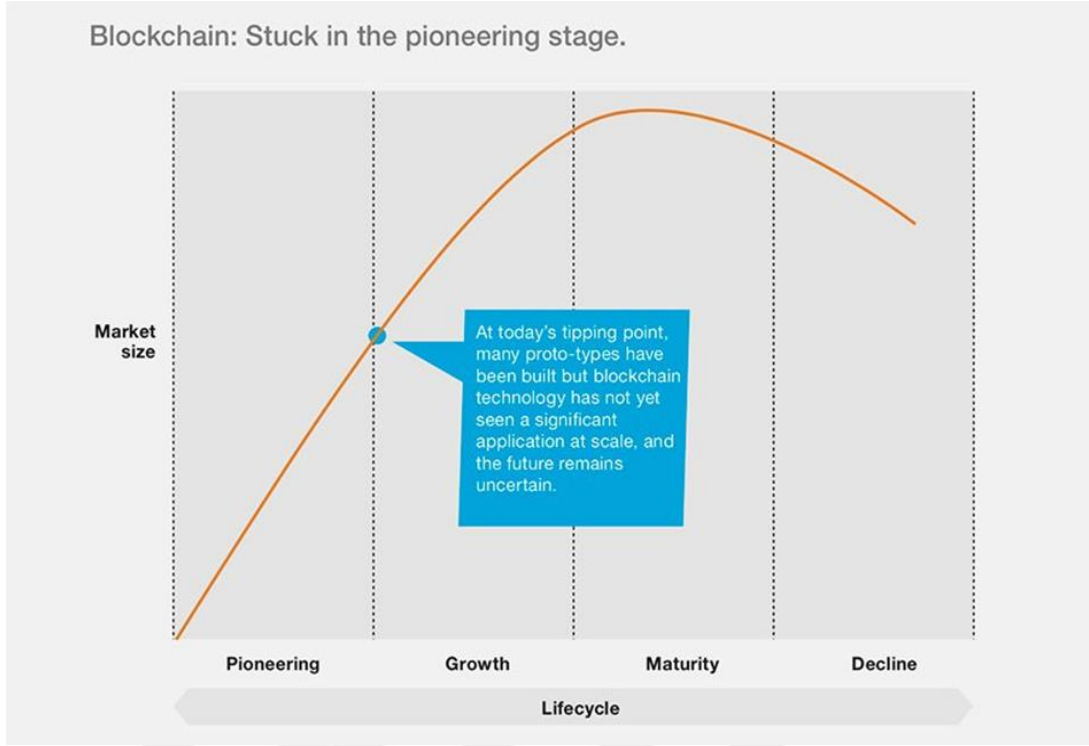
McKinsey'in son birkaç yıldır finansal hizmetler sektöründeki liderlerle yaptığı çalışmalara göre, blok zincirindeki "kömür" oyuncularını ikinci kez düşünmeye başlamaktadır. Aslında, üst düzey yöneticilerin aksi yöndeki güvencelerine rağmen, diğer sektörler hazırlanırken finansal hizmetler endüstrisinin belirli seviyelerinde artan bir temkinlilik olmuştur (URL-2, 2019). Gerçekte, milyarlarca dolar yatırım yapıldı, ancak neredeyse hiçbir kullanım senaryosunun büyük ölçekte uygulanması mümkün değil ya da teknolojik, ticari veya stratejik açıdan mantıklı değildir. Başta finans sektörü olmak üzere birçok sektörde "Kavram Kanıtı" aşamasına ulaşan blok zinciri projeleri, büyük ve istikrarlı yatırımlara rağmen durmaktadır. Blok zinciri teknolojisi birçok finans sektörü profesyoneli tarafından ya gereksiz ya da kurumsal düzeyde kullanılmak için çok genç olarak görüldü. Örneğin, birçok Kavram Kanıtı (POC), cevapladıklarından daha fazla soru ortaya çıkardı ve bulut çözümlerinin ötesinde çok az fayda sağlamıştır. Ticari uygulanabilirlik konusunda da endişeler vardı çünkü önemli bir maliyet tasarrufu veya ekstra gelir göstergesi yoktur (URL-3, 2023).

Birkaç banka blok zinciri taktiklerini yeniden değerlendirmeye başladı. Kalkınma finansmanına yönelik daha hedefli bir yaklaşım benimsediler ve POC'lere yönelik incelemelerini artırırlar. Çok sayıda kuruluş, izledikleri kullanım vakalarının sayısını birkaç düzineden bir veya ikiye indirdi ve ağın benimsenmesini, veri standartlarını, yönetişimi ve uyumluluğu izleme çabalarını artırmaktadır (Andriy, 2019).

Finansal hizmetler, blok zinciri teknolojisini diğer endüstri sektörlerinden daha önce denemeye başlamış ve endüstri yaşam döngüsünde diğer sektörlerin 18 ila 24 ay önünde yer almıştır. Bunun nedeni, kripto para birimlerinin ve özellikle de Bitcoin'in olası geleneksel finansal araçlar olarak ortaya çıkmasıdır. Bu eşitsizlik, bankacılık sektörünün başlangıçtaki endişelerinin şimdi başka yerlere kaymasını ve artan başarısızlık duygusu nedeniyle başlangıçtaki heyecanın azalmasını şaşırtıcı kılmamaktadır (URL-3, 2023).

McKinsey ayrıca, bazı sektörlerin süreçlerinin dijitalleştirilmesinde hala geride kaldığını, bunun da büyük ölçüde manuel müdahale ve tekrarlayan kâğıt tabanlı formalizasyon gerektirdiğini belirtmektedir. Önümüzdeki birkaç yıl içinde 20 milyardan fazla bağlı cihaz olacağı ve bunların hepsinin veri yönetimi, depolama ve geri alma gerektireceği tahmin edilmektedir (URL-2, 2019). Ancak, tipik bir ağdaki her bir düğümün her bir işlemi işlemesi ve tüm durumun bir kopyasını tutması gerektiğinden, blok zincirleri verimsiz veri kaplarıdır. Sonuç olarak işlem sayısı tek bir düğümün sınırını aşamaz. Ve gecikme sorunları nedeniyle yeni düğümler eklendikçe blok zincirleri daha az duyarlı hale gelir.

Son olarak Matt Higginson, bazı kuruluşların ve karar vericilerin başarılı iş operasyonları için risk oluşturduğuna inanmaları halinde bu teknolojinin benimsenmesini yavaşlatabileceklerine dikkat çekmektedir. Dahası, ödemeler sektörü geleneksel yeniliğinin ikilemiyle karşı karşıyadır; bu ikilemde yerleşik operatörler, yıkıma ve müşterilerin daha hızlı, daha basit ve daha ucuz hizmetlere yönelik beklentilerinde beklenen artışa yatırım yapmaları halinde kendi gelirlerinin tükenebileceğinin farkındadır (URL-2, 2019). Örneğin, sınır ötesi ödemelerle ilgili ücretleri göz önünde bulundurduğumuzda, bu ücretler toplam işlem tutarının %10'una kadar ulaşabilmektedir. Gerçek şu ki bu teknoloji pahalı, karmaşık, nispeten istikrarsız ve henüz emekleme aşamasında. Buna ek olarak, düzenlemeden yoksundur ve seçici güvensizliği teşvik etmektedir. Yukarıda gösterilen farklı uygulamalardan, özellikle de finans sektöründekilerden, teknolojinin henüz ürün yaşam döngüsünün sadece ilk aşamasında olduğu anlaşılmaktadır. Kavram kanıtlarının (POC'ler) çoğu hala öncü aşamasında olduğundan, ilerleme eksikliğinin ana nedenlerinden biri budur (URL-3, 2023). Mevcut yüksek aracılı sistemden paylaşılan bir deftere geçmenin mantıklı olduğu alanlardan biri ödemelerdir. Ancak blok zincirlerinin yanı sıra başka seçenekler de mevcut.



Şekil 5.1: Blok zinciri: öncüllük aşaması

Kaynak:<https://www.mckinsey.com/industries/financial-services/our-insights/blok-zinciris-occam-problem>

Değer zinciri bir dizi fintech şirketi tarafından altüst edilmektedir. ABD fintech'lerine yatırılan 12 milyar doların yaklaşık %60'ı, hız ve şeffaflığın yanı sıra ilgi çekici blok zinciri ikameleri sağlayan ödemeler ve kredi alanına odaklanmıştır (Andriy, 2019).

Blok zinciri teknolojisi çok ilgi görüyor, ancak Franck Chemin'in belirttiği gibi, pazar taleplerini gerçekten karşılayıp karşılamadığını veya sadece "kolaylaştırıcı" veya "yavaşlatıcı" bir araç olup olmadığını araştırmalı ve belirlenmelidir (Andriy, 2019).

5.1.1 Blok Zinciri Teknolojisinin Ölçeklenebilirliği ve Performansı

Blok zinciri teknolojisi ve kripto paraların çeşitli iş modellerinde kullanımının popülaritesi giderek artıyor. Özellikle performans ve ölçeklenebilirlik açısından, çeşitli ticari ve kamu sektörlerinden gelen artan talebi karşılama kabiliyetleri konusunda endişeler bulunmaktadır (URL-4, 2023).

Sistemdeki düğüm ve istemci sayısı, blok zinciri ölçeklenebilirliğini gecikme ve verim kadar etkilediğinden, bu iki konuyu tamamen izole etmek imkansızdır. Bununla birlikte, PoW ve BFT teknolojilerinin pratik olduğunu gösterdiği düğüm ve istemci sayısına odaklanılmaktadır (Vukolic, 2016).

Teorik olarak, PoW tabanlı blok zincirleri, Bitcoin ağını oluşturan binlerce madencilik düğümünün de gösterdiği gibi ölçeklenebilir. Bununla birlikte, madencilerin madencilik havuzlarında (madencilik ödüllerini bölmek ve madenciliği daha öngörülebilir bir iş haline getirmek için tasarlanmıştır) gruplandırılmasının bir sonucu olarak Bitcoin'in esasen merkezileştirildiğini belirtmek önemlidir. Madencilik havuzlarının merkezileşmesinin Bitcoin'e özgü bir özellik olmadığını, daha ziyade İş İspatı blok zincirinin benimsenmesinin bir yan ürünü olduğunu, bunun da çok sayıda altcoin'i veya Bitcoin'e benzer şekilde işleyen alternatif kripto para birimlerini ve Ethereum gibi iyi bilinen blok zincirlerini de etkilediğini belirtmektedir (Aggarwal vd., 2021).

Tersine, makine durumu replikasyonu ve BFT replikasyonu genellikle yetersiz ölçeklenebilir platformlar olarak kabul edilir. Ancak, BFT protokollerinin veri tabanları gibi geleneksel uygulamaların replikasyonunda hata toleransı için geliştirildiği göz önüne alındığında, örneğin $n = 10$ veya $n = 20$ düğümün ötesinde ölçeklenebilirlik açısından hiçbir zaman tam olarak test edilmemiştir. Blok zinciri uygulamalarının genellikle düşük performans hedefleri göz önüne alındığında bu özellikle doğrudur. Veri tabanı ve sistem topluluklarının BFT protokollerini, çoğunlukla blok başına $O(n^2)$ 'ye kadar mesaj gerektiren yüksek ağ iletişimi nedeniyle ölçeklenebilir olarak görmediği varsayılmaktadır. Bu durum, birçok büyük ölçekli sistemde kullanılan Paxos, Zab ve Raft gibi replikasyon protokolleri gibi hataya dayanıklı eşdeğerleri için bile geçerlidir, ancak neredeyse hiçbir zaman bir avuç replikadan daha fazlasında kullanılmamaktadır (Vukolic, 2016).

Son olarak, istemci sayısına dayalı ölçeklenebilirlik söz konusu olduğunda, PoW ve BFT protokolleri binlerce istemciyi destekler ve iyi uyum sağlar.

PoW tabanlı blok zincirlerinin performans sorunları, saniyede yalnızca 7 işlem (mevcut blok boyutuyla) ve 6 blokluk onaylama ile bir saatlik gecikme süresini kaldırabilen Bitcoin'in son derece kısıtlı yeteneklerinin ötesine uzanmaktadır. Blok boyutu ve sıklığı, daha önce de belirtildiği gibi bir Proof of Work blok zincirinin iki temel performans ölçütüdür. İnternet

üzerinden daha büyük bloklar için daha uzun yayılma süreleri, blok boyutu artırılarak verim artırıldığında daha yüksek gecikmeyle sonuçlanır (Rao ve Saritha, 2022). Daha uzun gecikmelerin blok zinciri güvenliği üzerinde de zararlı etkileri vardır. Geçici zincir çatallanmaları ve iş kanıtı blok zincirlerinde mutabakat kesinliğinin olmaması, çatallanmalarda artışa ve çift yatırma saldırıları potansiyeline yol açabilir. Çoklu blok onayının gecikme süresini azaltmak amacıyla blok sıklığı artırıldığında da benzer güvenlik sorunları ortaya çıkar. PoW tabanlı blok zincirlerinde blok boyutu ve sıklığı ayarlamaları, genellikle oldukça karmaşık oldukları için dikkatle değerlendirilmesi gereken özel güvenlik sonuçlarına sahiptir. Bu bilgiler ışığında, PoW blok zincirlerinin doğal olarak sınırlı performansa sahip olduğu görülmektedir; bu durum belirli bir uygulamanın yan ürünü değildir (Vukolic, 2016).

Buna karşılık hem çalışan prototipler hem de gerçek dünya sistemleri olarak çağdaş BFT protokollerinin neredeyse ağ hızında gecikmelerle on binlerce işlemi gerçekleştirebildiği doğrulanmıştır (Aggarwal vd., 2021).

Araştırmacılar son zamanlarda ağdaki replika sayısını içeren ölçeklenebilirlik sorunlarına ek olarak gecikme (blok zincirine bir işlem bloğu eklemek için geçen süre) ve verim (saniyedeki işlem sayısı) gibi performans sorunlarına odaklanmıştır. Replika aşırı yüklenmesi, ağ tarafından daha fazla mesaj gönderilmesi ve alınması gerektiğinden ve bu da daha fazla kaynak gerektireceğinden verimi ve gecikmeyi olumsuz etkileyebilir. PoW gibi protokoller ölçeklenebilirliği sağlayabilirken, yüksek gecikme süresi ve düşük verim ile sınırlıdır. Bir bloğun nasıl yayınlanacağını ve kriptografik olarak zincire nasıl ekleneceğini bulmak için kaybedilen kaynaklar bu darboğazın nedenidir. Çok sayıda kopyayı destekleyebilen PoW tabanlı bir protokol örneği Bitcoin'dir. Bununla birlikte, bir bloğu ortalama 10 dakikada oluşturarak düşük bir verimliliğe sahiptir ve saniyede yalnızca 6 ila 10 işlem gerçekleştirebilir (hatta ağın karmaşıklığına bağlı olarak daha da az). Bu mutabakat prosedürünün yüksek elektrik tüketimi, büyük ölçüde insan emeğine dayanması nedeniyle bir başka dezavantajdır (Monrat vd., 2019).

Ethereum, grafik işlem birimi veya merkezi işlem birimine benzeyen bir donanım cihazı tarafından gerçekleştirilen ve yüksek enerji tüketimi ve yüksek maliyet pahasına daha hızlı madenciliğe olanak tanıyan ASIC madenciliğini durdurmak için farklı bir Proof of Work (PoW) yöntemi kullanmaktadır. Ancak bu, Bitcoin'in dezavantajlarını ortadan

kaldıramayacak. Birden fazla bağlantı, PoW protokolü ile ilişkili bir başka risktir ve çift harcama sorununa neden olabilir (Ashik vd., 2020). Bu nedenle müşteriler en uzun zincirde altmış dakika veya altı onay bloğu boyunca işlemin tamamlanmasını beklemek zorundadır. Uzun işlem süresinin bir sonucu olarak, pratik uygulamalarda kullanılması uygun olmayabilir.

Kötü niyetli kopyalar mevcut olduğunda PBFT protokolünün bir anlaşmaya varması yalnızca birkaç mesaj değişim turu sürer. Bloklar PBFT tarafından tek bir birincil kopya kullanılarak önerilir ve ağdaki eşlerin üçte ikisinin kabul etmesi halinde zincire eklenir. Ayrıca, mutabakat süreci sırasında çatallanma PBFT tarafından yasaklanmıştır. Enerji verimliliği açısından bu strateji sürdürülebilirdir, ancak sürdürülebilir değildir. PBFT'nin ikinci dereceden mesaj karmaşıklığı nedeniyle, her n replika için $n \times n$ yayın gereklidir. Kötü niyetli replikaların ya da Bizans arızalarının olması mutabakatı garanti etse de, bu ek yük ölçeklenebilirlik sorunlarına neden olur. Herhangi bir büyük platform tarafından her saniye binlerce işlemin işlenmesi gerekir. Aksi takdirde, hem tüketiciler hem de ekonomideki işletmeler için ciddi gecikmeler yaşanacak ve bu yeni teknoloji için ölçeklenebilirlik ve performansın önemi ortaya çıkacaktır (Vukolic, 2016).

Blokların sınırlı kapasitesi nedeniyle, madenciler daha yüksek işlem ücretlerine sahip işlemleri tercih edebilir ve bu da çok sayıda küçük işlemde gecikmeye neden olabilir. Blok boyutları kısıtlıdır; örneğin bir Bitcoin bloğu 1 MB boyutundadır. Bu yöntemin platform güvenliğini artırması amaçlanmış olsa da, diğer mevcut sistemlerle karşılaştırıldığında işlem sürelerini önemli ölçüde yavaşlatır. Küçük blok boyutu nedeniyle birçok işlem aynı anda gerçekleştirilememektedir. Blok boyutu gibi ölçeklenebilirlikle ilgili endişeler Slepak ve Petrova'nın DCS (merkezi olmayan, tutarlı ve ölçeklenebilir) teoreminin de odak noktasıydı (Şekil5-.2). DCS üçgenini kullanarak, merkezi olmayan bir blok zinciri sisteminin tüm DCS özelliklerine aynı anda sahip olamayacağını göstermişlerdir (Slepak ve Petrova, The DCS Theorem, 2017). DCS çerçevesinin blok zincirinin yerine getirebileceği iki gereksinimi vardır. Ancak düşük hacim ve yavaş işlem hızı ya da düşük verim ve yüksek gecikme süresi sağlar.



Şekil 5.2 : DCS üçgeni

Kaynak: <https://arxiv.org/abs/1801.04335>

5.1.2 Gizlilik

Gizlilik ve gizlilik ihlallerinin çok sayıda biçimi olduğundan, gizlilik net bir tanımı olmayan karmaşık bir fikirdir. Bir kurumla ilişkilendirilebilecek bilgilerin paylaşılması mahremiyetin azalmasına neden olabilir ve tüm bu mahremiyet biçimlerinin ortak noktası da budur. Bu nedenle mahremiyeti korumak için ifşanın kapsamını, zamanlamasını ve alıcısını kontrol etmek gereklidir. Buna göre, bir varlık hakkındaki ilişkilendirilebilir bilginin ne ölçüde ifşa edildiği mahremiyeti tanımlar. Ifşanın kapsamı ya da bir kimlik ile gerçek bir varlık arasındaki doğrulanabilir bağlantı, doğrulanabilir bir bağlantının olmadığı ve kamuya ifşa edilmeyen tam anonimlikten, tam kamuya ifşa ve tam kanıtlanabilir ilişkilendirme ile tam anonimliğe kadar değişebilir (Smith ve Khovratovich vd., 2016).

Gizlilik ihlallerinin olumsuz etkilerinin çoğundan, bilginin işleme doğrudan dahil olan taraflarca kullanılmasından ziyade, ilgili bilgileri kullanan müdahil olmayan üçüncü taraflar sorumludur. Buna ek olarak, üçüncü bir taraf, işlemlerin hiçbirinde açıkça ortaya çıkmayan ek özel bilgileri çıkarmak için farklı ikinci taraflarla yapılan çeşitli alışverişlerde zaman içinde paylaşılan verileri izleyerek, birleştirerek ve analiz ederek meta veri toplayabilir (URL-4, 2023).

Bir işlemde, ilgili taraflar kimliklerini kamuya açıklama seçeneğine sahiptir, ancak bunu gönüllü olarak yapmaları gerekir. Öznitelikleri toplamak için başka bir kuruluşla bir işlem

başlatarak, bu öznitelikleri bir alıcı olarak kaynak kuruluşla ilişkilendirebilir ve kimliklerin refleksif profillerini oluşturmak için kimlik işlemlerini kullanabilirsiniz. Sadece kendi tarafları değil, diğer tarafın kimlik grafiği de bir işleme dahil olan her tarafça tutulabilir. Bu, bir kuruluşun kendisine ifşa edilen bilgilerin yanı sıra kendisinin ifşa ettiği bilgileri de izlemesini sağlar (Henry, Herzberg ve Kate, 2018).

İşlemler üç temel gizlilik seviyesine sahip olabilir: tamamen herkese açık, yarı özel ve tamamen özel. İşlem kimliği, hash, şifreli tanımlayıcılar, zaman damgası ve sınıflandırma bilgileri dahil olmak üzere meta veriler her işlem için her zaman kamuya açıktır. Kriptonimlerle bağlantılı kimlikler takma adlara veya genel tanımlayıcılara sahip olabilir ya da kısmen veya tamamen anonim olabilirler. Bir işlem sırasında değiş tokuş edilen öznitelikler de şifrelenebilir veya şifrelenmeyebilir (Herzberg ve Kate, 2018).

Tamamen herkese açık olan bir işlemde, tanımlayıcılar herkese açıktır ve öznitelikler bölümü şifrelenmez. Yarı özel bir işlemin özellikleri şifrelenmemiş olabilir ancak tanımlayıcılardan en az biri anonimdir veya özellikler şifrelenmiş olabilir ancak tanımlayıcılardan en az biri herkese açıktır. Tamamen özel bir işlemde özellikler şifrelenir ve her tanımlayıcı gizli kalır.

Blok zinciri teknolojisi, kullanıcıların gerçek kimlikleri yerine oluşturulan adresleri kullanarak işlem yapmalarına olanak tanıdığından, hassas kişisel veriler için güvenlik ve gizlilik sunduğu düşünülmektedir (Smith ve Khovratovich, 2016).

Ancak bazı araştırmacılar, bir işlemi başlatmak için gereken açık anahtarın diğer ağ eşleri tarafından görülebilir olması nedeniyle, blok zincirinin 'in işlem gizliliği açısından savunmasız olabileceği varsayımında bulunmuştur.

Sakladıkları verilerin kendi başlarına kullanıcı gizliliğini ihlal etmediğinden emin olmanın ötesinde, blok zinciri gizliliğini tam olarak ele almayı amaçlayan herhangi bir araştırma programı ek olarak (en azından) iki temel işlem türü için gizliliği dikkate almalıdır: blok zincirinden veri okuma ve blok zincirine veri yazma. Bunun nedeni çoğu blok zincirinin temelde kitlesel olarak dağıtılmış ve herkesin erişimine açık veri tabanları olmasıdır (Smith ve Khovratovich, 2016).

Bitcoin gibi dijital para birimleri söz konusu olduğunda blok zinciri, finansal işlemlerin kamuya açık ve bağımsız olarak doğrulanmış bir defteri olarak hizmet vermektedir. Daha açık olmak gerekirse, bir işlem her gerçekleştiğinde, işlemi gerçekleştiren taraf, daha sonra işlemin ayrıntılarını ağa yaymak için bir dedikodu protokolü kullanan az sayıda dikkatle seçilmiş varlığı kamuya açık bir şekilde bilgilendirir. İşlem nihayetinde bir dizi başka (ilgisiz) işlemle birleştirilerek ayrı bir blok oluşturur ve bu blok daha sonra kendisinden önce gelen her bloğu içeren bir zincire geri döndürülemez bir şekilde eklenir. Blok zinciri, güçlü bir bütünlük ve kullanılabilirlik elde etmek için aslında kopyalanabilir ve bir ağdaki çok sayıda düğüm arasında bütünüyle paylaşılabılır. Bu, her düğüme şimdiye kadar gerçekleşen her işlemin kapsamlı ve tek tip bir görünümünü verir. Birkaç günden birkaç aya kadar değişebilen belirli bir süre içinde, yeni işlemler blok zincirinin tüm kopyalarına yansıtılır (Herzberg ve Kate, 2018).

Belirli dijital varlıkların göndericisi ve alıcısı, genellikle cüzdan olarak adlandırılan ve her işlemle bağlantılı olan bir çift takma adla tanımlanır. Kullanıcılar dijital varlıkları istedikleri zaman almak için yeni takma ad cüzdanları oluşturabilirler; her işlem için yeni bir geçici cüzdan oluşturma Bitcoin kullanıcıları için en iyi uygulama olduğu düşünülmektedir. Bu geçici cüzdanların temel amacı, bir bilgisayar korsanının defterde belgelenen işlemlerde ortaya çıkan gönderici ve alıcı takma adlarını inceleyerek belirli bir kullanıcıyla ilişkili farklı işlemleri birbirine bağlama yeteneğini engelleyerek kullanıcıların gizliliğini korumaktır. Ancak Bitcoin ve diğer benzer para birimleri popülerlik kazandıkça, bu yaklaşımın "gizliliğinin" en fazla aldatıcı olabileceğine dair endişeler de artıyor. Elbette, geçici cüzdanların yaygın kullanımına rağmen, daha önce de belirtildiği gibi, blok zinciri gizliliğine yönelik son sekiz yıllık araştırma, bilgisayar korsanlarının Bitcoin işlemlerini ortak bir kullanıcıya bağlamasına olanak tanıyan gerçek bir verimli sezgisel hazine üretmiştir (Smith ve Khovratovich, 2016).

Örneğin birkaç ikinci nesil altcoin Zcash ve Monero, blok zincirinin işlem içeriğinin ilgili tarafların özel bilgilerini ifşa etmesini engellemek için açıkça kriptografik yöntemler kullanmaktadır (Arctic wallet, 2023). Araştırmalardaki bir dizi teklif de canlı Ethereum, Ripple ve Bitcoin blok zincirlerinde karşılaştırılabilir işlem gizliliği sunmayı amaçlamaktadır. Benzer şekilde, canlı Ethereum, Ripple ve Bitcoin blok zincirlerinde karşılaştırılabilir işlem gizliliği sunmayı amaçlayan bir dizi araştırma önerisi bulunmaktadır.

Bu yöntemler blok zinciri kullanıcılarını, blok zinciri dağıtımlarını yaygın olarak etkileyen anonimleştirme sezgisellerinin bir kısmından korumada başarılı olsa da, mevcut yöntemlerin yalnızca özel bilgilerin bir blok zincirinden sızmasını önlemeyi amaçladığını; kullanıcılar blok zinciri verileriyle etkileşime girdiğinde ortaya çıkan ağ düzeyindeki verilerden (IP adresleri gibi) veya erişim modellerinden (bireysel bloklar gibi) yararlanan çıkarımların olasılığını önemli ölçüde azaltmadıklarını not etmektedir (Biryukov ve Pustogarov, 2015).

Bu nedenle, mevcut çözümler blok zinciri gizliliği sorununu tam olarak ele almamaktadır.

5.1.2.1 Kullanılan İşlem Gizliliği Protokolleri

CoinJoin, Bitcoin topluluğu geçici takma adların yetersiz olduğunu fark ettiğinde potansiyel bir çözüm olarak ortaya çıkmıştır. İşlemler deftere girilmeden önce, CoinJoin kullanıcıları işlemlerini karıştırıcı olarak da bilinen merkezi bir harmanlama hizmetinden geçirir. Bu, işlemlerin göndericisi ve alıcısı arasındaki ilişkileri gizler. Tumbler hizmeti aslında her işlemin göndericisi ve alıcısı arasındaki ilişkinin her zaman farkındadır. Daha da endişe verici olan şey, karıştırıcı hizmetinin kullanıcıların yönlendirmeye çalıştığı varlıkları çalmasını engelleyecek hiçbir önlemin bulunmamasıdır. CoinJoin'in eksikliklerinin üstesinden gelmek için, giderek karmaşılaşan bir dizi protokol ortaya konmuştur (Rufing vd., 2017).

Mixcoin, bir kullanıcının varlıklarını alması durumunda karıştırma hizmetini "sorumlu" tutarak hırsızlık riskini azaltma girişimidir (hırsızlık teknik olarak hala mümkün olsa da ve karıştırma hizmeti kimin kiminle işlem yaptığını izlemeye devam etse de). Bu ilk gelişmedir. Bu temel konsept üzerinde bir dizi aşamalı iyileştirme (BlindCoin ve Blindly Signed Contracts gibi) üzerine inşa edilen TumbleBit adlı bir öneri, nihayet Mixcoin 'in hesap verebilirlik ve anonimlik zayıflıklarını Bitcoin ile tamamen uyumlu bir şekilde ele aldı; ancak, ortalama olarak, TumbleBit yaklaşımı işlem başına 20 dakika (veya iki Bitcoin bloğu) gerektirir ve ek işlem ücretleri ekler. Farklı bir strateji kullanan Aniket Kate'in CoinShuffle ve CoinShuffle++'ı, kullanıcıların kendi aralarında benzersiz birçok partili hesaplama yapmasını gerektirerek üçüncü parti bir karıştırma hizmetine olan ihtiyacı ortadan kaldırıyor. Yeni popüler, gizlilik odaklı kripto paralar (Rufing vd., 2017).

Sıfır bilgi özlü etkileşimsiz bilgi argümanı (zk-SNARK), izlenebilir halka imzalar, gizli işlemler ve gizli adresler gibi kriptografik ilkeler, Bitcoin işlemlerine göre gizlilik özelliklerini önemli ölçüde iyileştirmek için Zcash ve Monero gibi yeni ortaya çıkan gizlilik merkezli kripto para birimleri tarafından kullanılmaktadır.

5.1.2.2 Mevcut Tekliflerin Yetersizliği

Yukarıda bahsedilen işlem gizliliği protokollerinin her birinin amacı, blok zincirine eklenen işlemlerde belgelendiği üzere gönderenler ve alıcılar arasında var olan bağlantıyı kırmaktır.

Bununla birlikte, tüm yöntemler, bir işleme dahil olan taraflar arasındaki bağlantıları yeniden yapılandırmak için ağ düzeyindeki verilerden ve/veya erişim modellerinden yararlanan saldırılara karşı savunmasızdır; bu saldırılar, kullanıcılar işlemlerini yayınladıklarında ve hangi işlemlerinin kaydedildiğini keşfetmek için blok zincirini trollediklerinde tespit edilebilir. Örneğin bir saldırgan, kullanıcının bir Zcash veya Monero bağışı almadan hemen önce bir web sitesini ziyaret ettiğini fark ederse, bir kullanıcının bağış yaptığını varsayabilir. Saldırgan ayrıca, daha sonra aynı kullanıcının söz konusu işlemin deftere gönderilip gönderilmediğini doğruladığını görürse bu varsayımı sanal olarak doğrulayabilir (Henry vd., 2018).

Bu büyük sorunu çözmek için, bu gizlilik protokollerinin yaratıcıları genellikle kullanıcıların Tor gibi anonim bir iletişim protokolü aracılığıyla iletişim kuracağını varsayar. Aslında, Zcash, Anoncoin ve Torcoin gibi gizliliğe odaklanan bazı altcoinler Tor için yerel desteğe sahiptir ve tüm kullanıcıların Tor'u yalnızca blok zincirleriyle etkileşimde bulunmak için kullanacağını varsaymaktadır. Örneğin Zcash web sitesinde, "benzersiz bir IP adresinin, ağ gözlemcilerinin Zcash işlemlerini birbirleriyle ve diğer borsalarla ilişkilendirmesine izin verebileceği" açıkça belirtilmektedir. Ayrıca "ileri düzey kullanıcıların düğümlerinin IP adresini maskelemek için Tor üzerinden bağlanmayı seçebilecekleri" de belirtilmektedir (Biryukov ve Pustogarov, 2015).

Anonimlik için Tor'a duyulan bu güvenin nadiren kabul edilen bazı rahatsız edici zayıflıkları vardır. Bu zayıflıklardan biri, Tor'un interaktif web taraması ve gerçek zamanlı anlık mesajlaşma gibi düşük gecikmeli iletişimler düşünülerek inşa edilmiş olmasıdır. Aslında, bu

gibi düşük gecikmeli, düşük bant genişliğine sahip anonim iletişim sistemlerinin, Chaumian karışım ağları gibi yüksek gecikmeli yöntemlerle veya kriptograf diner (DC) ağları gibi yüksek bant genişliğine sahip yöntemlerle karşılaştırıldığında yalnızca nispeten zayıf bir anonimlik düzeyi sunabildiği görülmektedir.

Ayrıca Biryukov ve Pustogarov, Bitcoin işlemi yapmak için Tor kullanan kullanıcıların, Bitcoin'in "kara listeye alma" politikalarının bir sonucu olarak kendilerini aktif anonimleştirme saldırılarına, işlemlerini doğrudan duyurmalarına kıyasla nasıl daha duyarlı bulabileceklerini göstermektedir (Biryukov ve Pustogarov, 2015). Bunlar, saldırganın seçtiği Tor çıkış rölelerini yasaklamak için belirli Bitcoin eşlerini zorlamak için Bitcoin ağında yerleşik olan itibara dayalı hizmet reddi savunma mekanizmasından yararlanan ortadaki adam saldırılarını açıklar. Bu da tüm Bitcoin trafiğini Tor ağından saldırganın kontrolü altındaki sınırlı sayıda aktarıcı üzerinden çıkmaya zorlamaktadır. Bu ayrıcalıklı konuma geldikten sonra saldırgan, trafik korelasyonu yoluyla anonimleştirme, birden fazla cüzdan adresini ortak bir kullanıcıyla ilişkilendirme ve belirli bir cüzdan adresini içeren önceki işlemler hakkında ince istemcilere yalan söyleyerek "çift harcama" saldırıları başlatma gibi çeşitli rahatsız edici gizlilik saldırıları başlatabilir.

Kurumsal BT departmanlarının Tor'u çoğunlukla engellemesi ve hatta otoriter hükümetlerin Tor'u devlet düzeyinde sansürlemesi ek bir sorun olarak ortaya çıkmaktadır. Sansür büyük olasılıkla Tor'un diğer ilgisiz kullanımlarını engellemeye yönelik olsa da, bu durum söz konusu kurumlardan ya da ülkelerden bağlanan kullanıcıların gizliliği üzerinde doğrudan olumsuz etkilere neden olmaktadır. Bu tür sansürleri aşmak için Tor, takılabilir aktarımlar ve Tor köprüleri gibi birkaç sansürden kaçınma stratejisini destekler. Bununla birlikte, bu stratejiler mükemmel değildir ve sansür olayları dünyanın her yerinde hala sık sık meydana gelmektedir. Genellikle sansürden muaf olan faaliyetler için sansür atlatma araçlarının yaygın kullanımını teşvik etmek genellikle aptalca görünmektedir (Henry vd., 2018).

Ayrıca, yoğun blok zinciri trafiği Tor gibi bağlı olmayan bir üçüncü taraf anonim iletişim ağı tarafından desteklenmeyebilir. Tor'un çocuk pornografisi, bot net komuta ve kontrolü ve kötü amaçlı yazılım gibi kötü şeyler için kullanılmış olması iki endişeye yol açmaktadır: birincisi, bazı blok zinciri sistemleri onu kullanmak konusunda isteksiz olabilir.

Blok zincirlerde gizliliğin iyileştirilmesi, anonimlik gerektiren herhangi bir sorunu ele almak için harici anonim iletişim altyapılarının kullanılmasına yönelik herkese uyan tek bir stratejinin yeniden gözden geçirilmesini gerektirir. Ağın her üyesinin her bir açık anahtarın bakiyelerini ve özelliklerini görebilmesi, blok zincirinin veri ihlallerine karşı duyarlılığına önemli ölçüde katkıda bulunur. Bu nedenle, gizlilik ve güvenlik gereksinimleri blok zinciri uygulamalarının en başından itibaren belirlenmelidir (Monrat vd., 2019).

5.1.3 Birlikte Çalışabilirlik

Blok zincirleri arasındaki birlikte çalışabilirlik, farklı blok zinciri platformları arasında veri alışverişi yapma ve güvenli ve sorunsuz bir şekilde çalışma kapasitelerini ifade eder. Blok zinciri teknolojisinin diğer sistem ve teknolojilerle entegrasyonu ve düzgün çalışması buna bağlıdır (URL-5, 2022).

Birlikte çalışabilirlik blok zinciri teknolojisini geliştirir. Kripto ekosistemindeki çeşitli oyuncular için ortak bir dil sağlar. Her şeyden önce, farklı blok zincirleri arasında kesintisiz iletişim sağlamayı amaçlamaktadır. Başka bir deyişle, kripto para birimleri, değiştirilebilir tokenler veya NFT gibi veri ve değerleri de değiş tokuş edebilir ve paylaşabilir.

Birçok işletme ve kuruluşun çeşitli uygulamalar için blok zincirlerini kullandığı bir dünyada uyumlu ve etkili bir ekosistem oluşturmak için bu çeşitli zincirleri birbirine bağlayabilmek çok önemlidir. Ek olarak, blok zinciri teknolojisini daha geniş bir kullanıcı tabanına sunarak birlikte çalışabilirlik, güvenlik, şeffaflık ve değişmezlik avantajlarını en üst düzeye çıkarır.

Maalesef, blok zincirlerinin birlikte çalışabilirliği önemli bir zorluktur. Farklı blok zincirleri çok farklı protokollere ve standartlara sahip olduğu için birbirleriyle etkileşim ve iletişim kurmak zor olabilir. Örneğin Ethereum blok zinciri Bitcoin blok zincirinden farklı bir programlama dili kullandığı için iki blok zinciri arasında birlikte çalışabilirlik zordur. Ayrıca, bazı blok zincirlerinin ölçeklenebilirlik sorunları ve performans kısıtlamaları, bunların büyük ölçekli uygulamalar için kullanılmasını imkânsız hale getirebilir (URL-5, 2022).

Deloitte'i 2018 raporunun da gösterdiği gibi, şu anda çok sayıda sektör blok zinciri teknolojisini uygulamakla ilgilenmektedir. Bununla birlikte, herhangi bir ortak protokol

kullanarak birbirleriyle iş birliği yapamıyor ve entegre olamamaktadır. Blok zinciri endüstrisinin genişlemesi, birlikte çalışabilirlik eksikliği olarak bilinen bu durumdan olumsuz etkilenmektedir (URL-7, 2018).

Birlikte çalışabilirlik, blok zinciri alanında standartların ve yasaların bulunmaması nedeniyle de engellenmektedir. Blok zincirlerinin mimarisi ve işleyişi için belirlenmiş bir kılavuz olmadığından, yeni zincirleri mevcut ekosisteme dahil etmek zor olabilir.

Farklı blok zincirlerini birbirine bağlayan köprüler birincil risk kaynağıdır. Pek çok hack fırsatı, köprülerin birincil blok zincirlerine kıyasla genellikle daha zayıf güvenliğe sahip olmasından kaynaklanmaktadır. Köprüler, Nomad ve Ronin Network hack'leri gibi en büyük hack'lerden bazılarıyla bağlantılıdır ve bu hack'ler birlikte yaklaşık 200 milyon \$ ve 635 milyon \$'lık hırsızlıklara neden olmuştur (URL-25, 2022).

Bazı birlikte çalışabilirlik protokollerinin neden olabileceği zincirleme reaksiyon da bir başka risktir. Bir kripto para protokolünde güvenlik için köprülere veya diğer birlikte çalışabilirlik protokollerine bağlı olan uygulamalar, birlikte çalışabilirlik protokolüne veya kripto paranın kendisine bir saldırı olması durumunda kaosu birbirine bağlı diğer tüm uygulamalara ve blok zincirlerine yayma riski taşır (URL-25, 2022). Bir ekosistemi bir bütün olarak etkileyen talihsiz olaylar dizisi olan siyah kuğu etkisini önlemek için hem köprünün hem de her bir kripto para protokolünün güvenliğinin eşit düzeyde olduğundan emin olmak çok önemlidir.

Bu nedenle kripto para birimleri, farklı iş modelleri için bir dizi faydalı yanıt sağlamak yerine birincil blok zinciri platformu olarak hizmet vermeye devam etmektedir. Birlikte çalışabilirlik eksikliği nedeniyle blok zinciri geliştiricileri çeşitli platformlarda kod yazabilirken, bu ağların hepsi izole edilmiş durumda ve birbirleriyle iletişim kuramamaktadır. Bu nedenle, işletmelerin blok zinciri tabanlı çözümleri paylaşabilmesi ve mevcut sistemlerle entegre edebilmesi için uygulama geliştirme iş birliğinde standardizasyon gerekmektedir (Henry vd., 2018).

5.1.4 Enerji Tüketimi

Son yıllarda kripto para birimlerinin artan popülaritesi, madencilik için karşı konulmaz bir

teşvik yarattı. Sonuç olarak, temel PoW blok zincirleri önemli miktarda enerji tüketmektedir (O'Dwyer ve Malone, 2018).

PoW, Bitcoin'de yaygın olarak kabul gören birkaç kriptografik fikrin birleşiminin sonucudur. Hesaplama açısından yoğun bir kriptografik bulmaca çözüldüğünde, sıraya alınan işlemlerin bir kısmından yeni bir blok oluşturma hakkıdır. "Madencilik" terimi, bir çözüm bulma sürecini ifade eder (Sedlmeir vd., 2020).

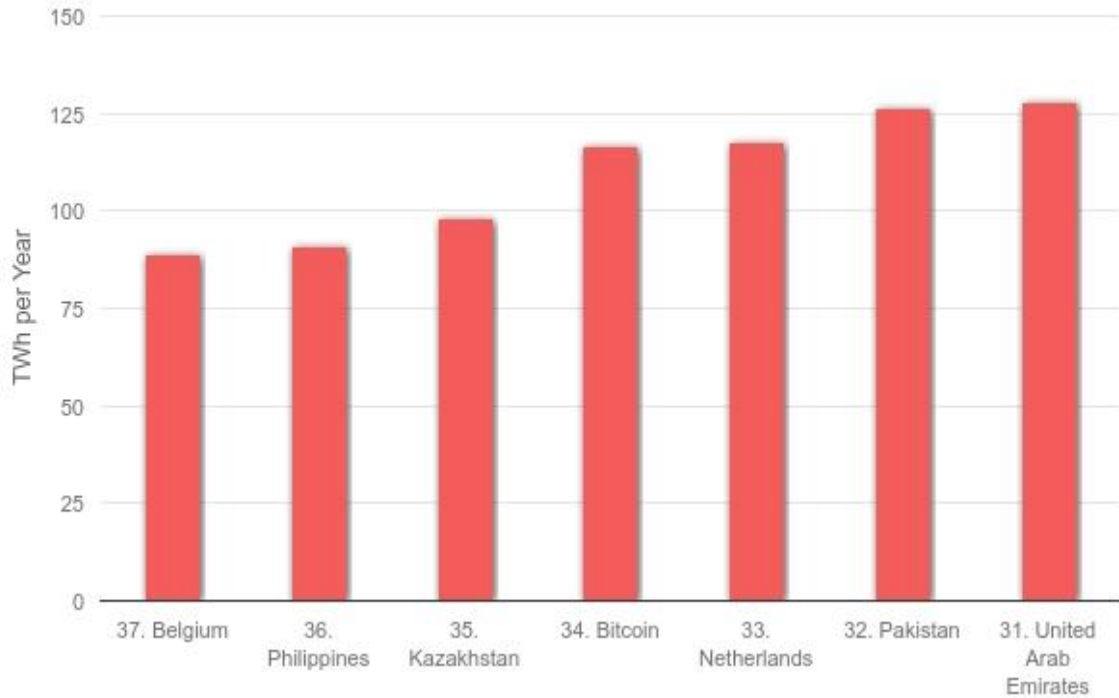
Bununla birlikte, on yılı aşkın bir süredir halka açık olan Bitcoin gibi bazı blok zincirlerinin ve kripto para birimlerinin azmi, bu modellerin henüz bir geleceği olabileceğini göstermektedir. Buna ek olarak, blok zincirlerinin dayandığı halka açık protokoller çevresel sorunlar ortaya çıkarmaktadır. Bir kayda yeni bir bilgi eklenmeden önce, PoW ("proof of work") konsensüsüne uygun olarak kriptografik bir hesaplama yapılmalıdır. Bu hesaplama için gereken enerji çok yüksektir. Yine de bu, kaydın değişmezliğini korumanın tek yoludur. Halka açık blok zinciri ağlarının tam enerji tüketimi henüz bilinmemekle birlikte, Bitcoin'in yıllık tüketiminin genellikle 6 giga watt (GW) olduğu tahmin edilmektedir, bu da dört nükleer enerji santralinin veya tüm İrlanda ülkesinin çıktısına eşdeğerdir. Dahası, ağ genişledikçe işlem gücü ihtiyacı da artmaktadır (Andriy, 2019).

PoW blok zincirlerinin yüksek enerji tüketiminin nedeninin eski donanımlar ya da verimsiz algoritmalar olmadığını unutmamak önemlidir. Bu blok zincirlerinin "tasarım gereği enerjiye aç" özelliği şaşırtıcıdır. PoW blok zincirleri yüksek enerji tüketimleri nedeniyle saldırılara karşı dirençlidir: bir saldırganın, duruma bağlı olarak, katılımcı madenciler tarafından madencilik için kullanılan toplam işlem gücünün en az %25 ila %50'sine ihtiyaç duyarak sistemi başarılı bir şekilde manipüle edebilmesi veya kontrol edebilmesi gerekir. Bu aynı zamanda toplam enerji tüketiminin de aynı yüzdesine karşılık gelir (aynı donanım varsayıldığında) (Eyal ve Sirer, 2018). Sonuç olarak, bir PoW kripto para birimi ne kadar değerli olursa saldırılara karşı o kadar iyi korunur ve PoW 'un iyi düşünülmüş bir tasarım olduğunu kanıtlar.

Araştırmacılar son zamanlarda O'Dwyer ve Malone'un çalışmalarından başlayarak bir dizi bilimsel yayında Bitcoin ile ilişkili enerji tüketimini incelemişlerdir. Bununla birlikte, PoW kripto para birimlerinin ve genel olarak blok zinciri teknolojisinin enerji tüketimi hakkında herhangi bir sonuç bulmak zordur (O'Dwyer ve Malone, 2018). Çok sayıda açık ve dağınık

ağın enerji tüketimini doğru bir şekilde belirlemek zordur, çünkü kaç kişinin dahil olduğunu, ne tür donanım kullandıklarını veya madencilğe ne kadar zaman ve enerji ayırdıklarını bilmek zordur.

Dağıtılmış, merkezi olmayan bir ortamda güven olmadan eşler arası işlemler, Bitcoin'deki iş ispatı (PoW) algoritması ile mümkün olmaktadır. Ancak madenciler tarafından kullanılan bilgisayarlar bu işi yapmak için muazzam miktarda elektrik kullanmaktadır. PoW algoritmasının sürdürülemez doğasına ışık tutmak için Bitcoin Enerji Tüketim Endeksi geliştirildi. Teşvik sistemi, dünya çapında bireyler arasında Bitcoin madencilğini teşvik etmektedir. İnsanlar, madencilik sürecinin yarattığı önemli gelir akışının bir kısmını elde etmek için enerji yoğun cihazları çalıştırmaya teşvik edilmektedir. Sonuç olarak, Bitcoin ağının genel enerji tüketim oranı tüm zamanların en yüksek seviyesine çıktı ve kripto paranın değeri de aynı şekilde arttı. Uluslararası Enerji Ajansı tarafından yayınlanan bir rapora göre, Bitcoin ağının toplam tüketimi birkaç ülkenin tüketiminden daha fazladır (Monrat vd., 2019). Bitcoin bir ülke olsaydı, aşağıdaki şekilde gösterildiği gibi sıralanırdı.



Şekil 5.3 : Ülke grafiğine göre enerji tüketimi

Kaynak: <https://digiconomist.net/bitcoin-energy-consumption>

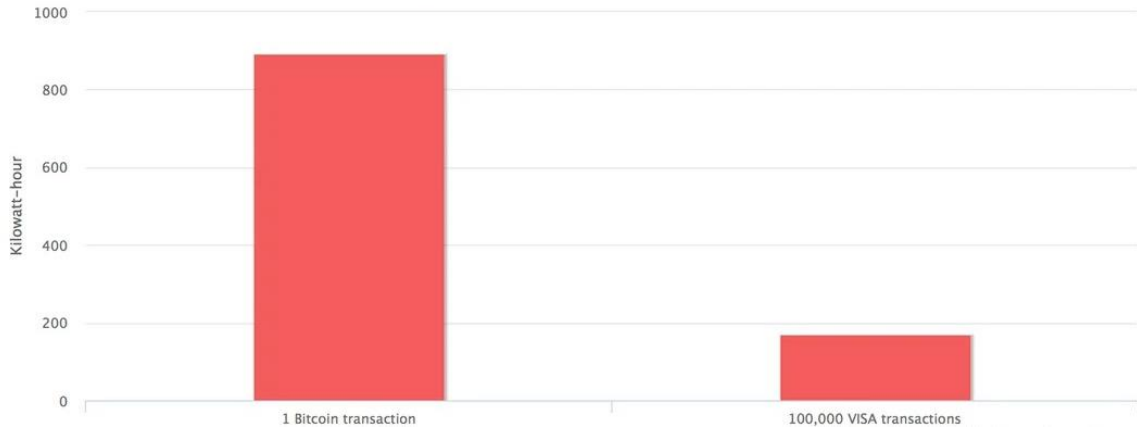
Bitcoin sadece çok büyük bir enerji tüketimine sahip olmakla kalmıyor, aynı zamanda önemli bir karbon ayak izi de bırakır. Çin'de Bitcoin ağı kömürle çalışan elektrik santralleri

tarafından desteklenmektedir. Ekim 2018 gibi erken bir tarihte Nature Climate Change, Bitcoin madenciliğinin tek başına küresel sıcaklık alarmını 30 yıldan kısa bir süre içinde 2 °C'nin üzerine çıkarabileceği gibi cesur bir iddiada bulunmuştur (Monrat vd., 2019).

Bitcoin'in Enerji Tüketim Endeksi'ne göre (Digiconomist, 2022):

- Bitcoin'in tahmini yıllık elektrik tüketimi: 51,92 TWh
- Tahmini yıllık küresel madencilik maliyetleri: \$2,595,834,583
- Küresel elektrik tüketiminin yüzdesi olarak Bitcoin'in elektrik tüketimi: 0.23%.
- İşlem başına karbon ayak izi: 274,29 kg CO₂

Blok zinciri uygulamasının enerji tüketimini VISA gibi diğer ödeme yöntemleriyle karşılaştırmak, ne kadar sürdürülemez olduğunu göstermek için kullanılan bir başka yöntemdir. Şirket 2017 yılında 111,2 milyar işlem gerçekleştirmiş ve 674.922 giga jul enerji kullanmıştır. Yaklaşık 17.000 ABD hanesi bu miktarda enerji kullanabilir. Aşağıdaki şekilde görüldüğü üzere, Bitcoin gibi bir blok zinciri uygulaması işlem başına Visa'dan daha fazla enerji kullanmaktadır. Blok zincirinin araçlara olan ihtiyacı ortadan kaldırdığını söyleyebilirsiniz, ancak bunun çok yüksek bir maliyeti vardır.



Şekil 5.4 : Bitcoin ve Visa ağının ortalama tüketimi

Kaynak: https://www.reddit.com/r/Buttcoin/comments/889wzv/1bitcoin_transaction_uses_over_four_times_as/?rdt=44880

5.2 Blok Zinciri'nin Güvenlik Eksikliği

Dağıtık defter teknolojisindeki güvenlik açıkları, bunun gibi gerçek dünya ortamında henüz

görülmemiş bir güvenlik azmine rağmen keşfedilmiştir. Henüz deneysel aşamasında olan blok zinciri, imajını zedeleyen çok sayıda hack ve başarısızlık yaşamaktadır. Çevrimiçi cüzdanlar, borsa platformları ve akıllı sözleşmeler bu saldırıların ana hedefleridir (Andriy, 2019).

Blok zinciri yeni bir teknoloji olduğu için yeni, daha gelişmiş güvenlik gereksinimleri gerektirmektedir. Bir blok zinciri ağı kurulduktan sonra, hatalı bir kod birden fazla ağ saldırısına yol açabilir ve geri alınamaz. Ağ, birden fazla oyuncu arasında paylaşıldığı ve dağıtıldığı için sistemik bir karaktere sahiptir. Sadece bir kod enjeksiyonu ile, orijinal kodlamadaki bir kusur nedeniyle tüm ağ tehlikeye girebilir (Smith ve Khovratovich, 2016).

Blok zinciri, öncekilerden farklı işleyen yeni bir teknoloji olduğu için (merkezi olmayan ve merkezi), yeni ağ güvenliği yöntemleri gereklidir. Örneğin, blok zinciri ağına bilgi ekleme işleminin hassas aşamalarını güvence altına almak için insan doğrulaması gerektiren kontrol kulelerine ihtiyaç vardır (Walpor, 2016).

Günümüzde açık kaynaklı blok zinciri mimari modelleri ve protokolleri mevcut olsa da, bazı araştırmacılar bunları birbirinden ayıran şeyin güvenlik olduğunu iddia etmektedir. Kendini koruma becerisi, blok zincirinin gerçekten zorlaştığı yerdir (Andriy, 2019).

Çok sayıda güvenilir blok zinciri platformunun saldırılara karşı dayanıklı olduğu ve çok az sayıda önemli hataya sahip olduğu görülmüştür. Bununla birlikte, bunlar üzerinde geliştirilen programlar (akıllı sözleşmeler gibi) ciddi sonuçlara yol açabilecek hatalara karşı savunmasız kalmaktadır. Potansiyel kullanıcılar bu güvenlik kusurları giderilene kadar temkinli olmaya devam edecek ve bu da yaygın olarak benimsenmesini geciktirecektir (Monrat vd., 2019).

Teknolojik olgunlaşmamışlık nedeniyle, kullanıcıları siber suç riski altına sokan güvenlik açıkları mevcuttur. 51 saldırısı, blok zinciri güvenliğiyle ilgili en iyi bilinen sorunlar arasındadır. Bir ya da daha fazla kötü niyetli taraf, %51 saldırısı yoluyla bir blok zincirinin hashrate'inin çoğunluk kontrolünü ele geçirir (URL-34, 2023). Çifte harcama yapmak için işlemleri tersine çevirme ve çoğunluk hashrate'ini kullanarak diğer madencilerin blokları doğrulamasını engelleme yeteneğine sahiptir.

Madencilik havuzları tarafından blok ödülleri artırmak için kullanılan bir diğer adil olmayan teknik de blok zinciri ağının bütünlüğünü tehlikeye atan bencil madenciliktir. Eyal ve Sirer, %51'den fazla işlem gücüne sahip kötü niyetli düğümlerin ağı ele geçirebileceği düşünülmese de, hala kullanıcı kontrolü altında olan bir blok zinciri ağı önermişlerdir. Bir blok zinciri ağı, minimum işlem gücüne sahip birinin bundan faydalanmak istemesi halinde yine de dolandırıcılığa açık olabilir (Eyal ve Sirer, 2018). Onaylanmış blokları ağın geri kalanından alıyarak, tek bir madenci veya bir grup madenci otonom madencilik sürecini başlatabilir. Avantajlarını korumak için, daha sonra gelecek blok için madencilığe devam ederler. Sadece belirli kriterler yerine getirildikten sonra çözülen bloklar halka açık hale getirilir. Sonuç olarak ağ, kendine hizmet eden madencinin çözümlerini benimseyerek onun zincirini daha uzun ve zorlu hale getirirken, diğer madenciler de gereksiz bir dal için enerji harcar. Nihayetinde, benmerkezci madenciler daha yüksek ücret talep eder. Bu, daha mantıklı madencileri daha uzun zincire katılmaya ikna ederek bencil havuzun %51 gücü aşmasına neden olabilir.

Çok sayıda başka bencil madencilik tekniğinin ortaya atılmış olması, blok zinciri teknolojisinin ne kadar güvensiz olduğunu göstermektedir. Bazı araştırmacılara göre inatçı bir madencilik stratejisi, bencil madencilığe kıyasla %13 kazanç sağlayabilir (Nayak vd., 2016). Araştırmacıların stratejisi, madencilik saldırılarını ağ düzeyinde tutulma saldırılarıyla üçlü olmayan bir şekilde birleştirerek bir madencinin kazancını nasıl daha da artırabileceğini göstermiştir. Sapirshtein'in araştırmasına göre saldırganlar, bilgi işlem kaynaklarının %25'inden daha azıyla bile bencil madencilikten kâr elde edebilir (Sapirshtein vd., 2016). Yakın zamanda yaşanan bir olay bu tür bir saldırıyı örneklemektedir. Ocak 2019'da ikincil bir kripto para birimi olan Ethereum Classic'e (ETC) karşı %51 oranında bir saldırı gerçekleştirilmiş ve 1,1 milyon doların çalınmasıyla sonuçlanmıştır.

5.3 Halka Açık Blok Zincirinin Güçsüz Olmasının Nedenleri

5.3.1. Çözülemediği Problemler

Dört tür belirsizlik, finans sektöründe halka açık blok zinciri ile karşılaşılan zorlukları anlamaya yardımcı olabilir (Andriy, 2019):

- Güvenin merkezsizleşmesi, bugüne kadar güvenlikten yasal olarak sorumlu

olan ve müşteriler ile düzenleyici makamlara (temerrüt, geri ödeme vb.) karşı sorumlu olan bir oyuncunun belirlenememesiyle sonuçlanmıştır. Bu durum sorumluluk kavramının tam tersi bir durumdur.

- Blok zinciri teknolojisi, teoride herkesin katılabileceği, bağımlılığın tersine kendi kendini yöneten bir alternatif sunuyor. Ancak ortaya çıktığı üzere, aslında programcıların yanı sıra veri madenciliği kurumlarına da büyük ölçüde bağımlılık söz konusudur.
- Halka açık blok zinciri sayesinde işlemler izlenebilir ve şeffaf hale getirilebilir. Bu özellik, katılımcı kurumların kendilerini ve müşterilerini belirli işlemlerden koruma arzusu olan ticari gizlilik fikrine ters düşmektedir.
- Halka açık blok zincirinin özgürlükçü ilkeleri, katılımcı kimliğini önleyen takma adların kullanılmasını zorunlu kılar. Kara para aklama ve terörizmin finansmanı ile mücadelede bankacılık kurumları bu karanlığı kabul etmemektedir.

5.3.2. Sürdürülebilir Olmayan Bir Ekonomi Modeli

Blok zinciri teknolojisine dayalı kripto para birimlerinin önemli fiyat dalgalanmaları, uzun vadeli iş modellerinin geliştirilmesini engellemektedir. Bu kripto varlıkların spekülasyon doğası, 2017 yılında Bitcoin fiyatındaki artış ve ardından gelen düzeltme ile gün ışığına çıkmıştır. Banque de France bu aşırı oynaklığı sağlam bir ekonomik temel olmayışıyla açıklıyor. Bitcoin'in küçük bir yatırımcı grubu tarafından neredeyse tekelleri bir şekilde sahiplenilmesi yatırımcıların sadece %2,5'i kripto para biriminin değerinin %95'ini elinde tutuyor kuruluşun fiyat manipülasyonu riskinin yüksek olduğu konusunda da uyarıda bulunmasına neden oluyor. Bu riskleri azaltmak için kripto para birimi faaliyetlerine ilişkin düzenleyici bir çerçeve gereklidir. Bu çerçeve kara para aklama ve terörizmin finansmanını önlemeye, yatırımcıları korumaya, çevre düzenlemelerine uymaya ve piyasa bütünlüğünü korumaya yönelik tedbirleri içermelidir. Yatırımların şeffaflığı, halka açık blok zincirlerinin anonimliği ile doğrulanmaktadır (Andriy, 2019). Halka açık bir blok zincirinin kuralsız yapısı, temelinden kaynaklanır ve bu da operasyonlarının gözetimini son derece zorlaştırır. Son olarak, halka açık blok zinciri işlemleri için tüm zincirin kapsamlı bir denetimi gereklidir, bu nedenle bazı araştırmacılar bu süreçlerin zahmetli olduğunu belirtmiştir. Daha uzun zincirlerde daha yavaş doğrulama gerçekleşir.

5.3.3. Yasalardaki Belirsizlik

Hukuk ve finans bir arada var olmak zorundadır. Bu nedenle, en azından mülkiyet değişikliğini içeren bir blok zincirindeki bazı işlemler için, belirli yasaların "kod" olarak tanınması ve bunun tersinin de geçerli olması gerekir (Varma, 2019). Aslında, blok zinciri teknolojisini destekleyen bir yasal çerçeve oluşturulamazsa, geleneksel güvenilir üçüncü tarafın kullanılması gerekecektir. Bu, çok talep edilen güvenilirliği sağlamak için blok zinciri kanıtlarına yasal bir kapsam verilmesi gerektiği anlamına gelir. Blok Zinciri'nin zorlukları üzerine hazırlanan bir raporda iki temel yasal zorluk olduğu ortaya çıkmaktadır (Toleno ve Janin, 2018):

- Vergi: Faaliyetlerin nasıl vergilendirileceği konusunda var olan belirsizliktir. Bazı ülkelerde bu durum teknolojik ilerlemenin önünde önemli bir engel teşkil etmektedir. Bu sorunun çözülmemiş olması, dijital varlıkları çevreleyen yasal belirsizlikten kaynaklanmaktadır.
- Hesap hakkı: Geleneksel bankalar kripto para birimlerine ve diğer dijital varlıklara aşina olmadıkları için, piyasadaki oyuncular bankalarda bir hesap tutamamakta ve sonuçta işletmelerinin büyümesini engellemektedir. Ayrıca, bankalar, fon kaynağını doğrulama gerekliliği nedeniyle kripto para varlıklarına sahip işletmelerin hesaplarını işlemeyi reddetmeye zorlanmaktadır.

Bu teknolojiye yasal açıdan da olgunluk eksikliği bulunmaktadır. Bu yeni teknolojinin ilerlemesini garantilemek için şüphesiz düzenleme yapmak gereklidir.

5.4. Düzenlemelere Yönelik Çıkarımlar

Yasal kodlar ve bilgisayar/donanım/teknik kodlar dijital ortamdaki faaliyetleri düzenlemek için etkileşim halindedir. Yasal kodların çoğu dışsaldır, yani kurallar ihlal edilebilse de bunun yansımaları uyumu garanti edebilir. Teknik kodlar ise çoğunlukla içseldir; yani kurallar ihlal edildiğinde hatalar geri döner ve herhangi bir eylem gerçekleşmez; dolayısıyla kodların kullanımı uyumu sağlar. Teknik kodlar doğaları gereği katıdır, yani istenmeyen veya beklenmeyen sonuçların ortaya çıktığı durumlarda bile takip edilirler (Yeoh, 2017).

Teknik kodlar ve yasal kodlar günümüzün modern finans sistemini yönetmektedir. Teknik kodlar tarafından belirlenen ve desteklenen kurallar Bitcoin ortamındaki katılımcılar

tarafından takip edilmektedir. Bu nedenle, Bitcoin'e güç veren ve yakında çok sayıda başka uygulamada da kullanılacak olan blok zinciri teknolojisi için katılımcıların uyum maliyetleri azalır, çünkü tek gereksinim uyumlu yazılım paketleridir (Walpor, 2016). Sistem kullanıcılarının önemli hesaplama kaynakları için ödeme yapması gerekse de uygulama maliyetleri tartışılabilir özellikle de en yaygın kullanılan dağıtık defter sistemlerindedir.

Bu, teknolojik ve yasal kodların dağıtık defterleri yönetebileceğini daha da fazla ima etmektedir. Bitcoin gibi yetkisiz sistemleri yasal kodlarla düzenlemenin daha zor olduğu kanıtlanmış olsa da dikkatler şu anda Bitcoin ile ilgilenen şirketleri düzenlemeye yönelmiş durumdadır. Yetkili dağıtık defter sistemleri için bu, basitçe sahibine yasal yükümlülükler getirmek anlamına gelebilir. Bitcoin borsaları ve cüzdan sağlayıcıları ile çalışan işletmelerin düzenlenmesi şu anda odak noktasıdır.

Dijital para hizmetleri sunan işletmelere verilen Bit Lisansları, yasaların Bitcoin'i nasıl düzenlediğinin mükemmel bir örneğidir. Ad hoc süreçler, Bitcoin gibi dağıtık defter sistemleri için teknik kod sağlayan özel katılımcıları içerir. Kamu sektörü kuruluşları, yazılım ve protokollerden oluşan teknik kod üretebilir. Son olarak, yasal kodların aksine, teknik kodlar demokratik temsile ve kamu düzenlemeleri oluşturma sürecine halkın katılımına izin verir (Walpor, 2016).

Blok zinciri teknolojisi, 702 farklı siber para biriminde bulunan dijital olarak depolanmış değer transferlerinin ötesine geçerek işlem doğrulama veya güvenilir bir bilgi havuzuna ihtiyaç duyan uygulamalara doğru genişlemiştir (Trautman, 2016). Merkezi olmayan eşler arası uygulamalar ve akıllı sözleşmeler, merkezi olmayan uygulamaları desteklemek için altyapı oluşturmak üzere blok zinciri teknolojisini kullanmaya başlayan birçok kuruluştan biri olan Ethereum Vakfı'nın blok zinciri altyapısından geliştirilebilir. Hem kolluk kuvvetleri hem de hukuk sistemi bu uygulamalar karşısında zorlanmaktadır.

Bununla birlikte, bireylerin ya da grupların bu uygulamaları yasaları ihlal etmek için kullandığı durumların aksine, örneğin merkezi olmayan pazar yerlerinde yasadışı mallar satmak, pazar yerinin web sunucularında barındırıldığı durumların aksine, sistemi çökertmek için şu anda bilinen bir yöntem yoktur. Dolayısıyla, finansal transferler, çoklu imza işlemleri, "renkli paralar", mülkiyet kayıtları, fikri mülkiyet, akıllı sözleşmeler, blok zincirinde saklanan ek veriler, merkezi olmayan kuruluşlar ve finansal ve güvenlik ürünleri

gibi gelişen alanlardaki bu tür uygulamalar sonucunda yasal ortam daha karmaşık hale gelebilir (URL-33, 2016). Günümüz yasaları esnetilmiş ve kripto para düzenlemeleri stratejide bir değişimi zorunlu kılmıştır.

Blok zinciri teknolojisinin kullanımının yaygınlaştırılması, mevcut yasal çerçevelerin yeni yasal yaklaşımlarla birlikte dikkatli bir şekilde uygulanmasını gerektirebilir. Merkezi olmayan teknoloji savunucularına göre, gelecekte bilgi ve iletişim merkezi bir otorite tarafından kısıtlanmayacaktır. Eşler arası teknoloji uzun bir geçmişe sahip olduğundan ve blok zincirlerinin gerçeğe dönüşmesi uzun yıllar alabileceğinden, inovasyon döngüsünün bu erken aşamasında blok zincirlerini düzenlemenin ters etki yaratabileceğini iddia etmektedir (Yeoh, 2017).

Bu bakış açısına göre düzenleyiciler, gereğinden fazla kuralcı düzenlemelerle inovasyonu boğma riskini almak yerine, yeni fikirleri halihazırda yürürlükte olan çerçevelere dahil etmenin yollarını aramalıdır. Bazıları otomatikleştirilmiş yasal belgelere, sözleşmelere ve bilgi alışverişine aşırı güvenmenin kodların diktatörlüğüne yol açabileceğini savunmaktadır. Bu da hukuk sistemlerinin ne kadar esnek olabileceği sorusunu gündeme getirmektedir (Kakavand ve Sevres, 2017).

Düzenlemenin yönetimden farklı olduğunu belirtmek de önemlidir. Birincisi davranışları kontrol etmek için tasarlanmış yasalarla ilgiliyken, ikincisi ortak çıkarlar doğrultusunda hareket etmek için yönetim, iş birliği ve teşviklerle ilgilidir. Geçmiş deneyimler, hükümetlerin yasaların ağır eli olmak yerine toplumun diğer bileşenleriyle iş birliği yapan bir akran olarak işlev görerek teknolojileri dikkatli bir şekilde düzenlemesinin daha iyi olacağını göstermektedir (Yeoh, 2017).

5.4.1. Düzenleyici Kurumların Endişeleri

Düzenlilik sorunları, kripto para birimi de dahil olmak üzere blok zinciri platformlarını rahatsız etmektedir. Bunun nedeni, merkez bankalarının ekonomi politikasını kontrol etme gücünü azalttığı için hükümetleri blok zinciri teknolojisine karşı temkinli hale getiren merkezi olmayan sistemin özellikleridir. Örneğin, bazı hükümetler kendi topraklarında kripto para birimini yasaklamakla ve hatta kullanmakla tehdit etmiştir. Bitcoin, Ekvator, Bolivya, Pakistan, İran, Fas ve Cezayir de dahil olmak üzere bir dizi ülkede yasaklanmıştır

(Monrat vd., 2019). Bangladeşli Bitcoin sahipleri gözaltına alınmıştır.

Blok zinciri teknolojisinin düzenlemelerden çok daha hızlı geliştiği gerçeği ışığında, İngiltere Merkez Bankası ve Avrupa Menkul Kıymetler ve Piyasalar Otoritesi gibi AB düzenleyicilerinin bu gerçeği kabul etmeleri gerekmektedir. Finansal işlemlerin Mifid II ve Emir gibi mevcut yasalar tarafından belirlenen kurallara uymasını zorunlu kılmanın uygun olup olmadığını ve bunu yapmanın blok zinciri teknolojisinin avantajlarını engelleme olasılığından daha ağır basacak kadar ekonomik istikrar ve yatırımcı koruması sağlayıp sağlamayacağını dikkatlice düşünmeleri gerekebilir. Ya da düzenleyici hedeflerine ulaşmaya devam ederken sofistike bir blok zinciri tabanlı finansal ekonominin büyümesini destekleyecek özel bir rejim oluşturmanın daha iyi olup olmayacağını düşünebilirler (Yeoh, 2017).

Sanal para birimleri üzerine bir çalışma grubu ve sanal para ticaretinin AB kara para aklamayı önleme direktifine dahil edilmesi, Avrupa Parlamentosu'nun bir araya getirdiği iki ayrı girişimdir. Bu iki girişim sonucunda yeni bir düzenleyici kurum oluşturulmayacaktır. Avrupa Komisyonu'ndan önleyici bir gözetim sistemi kurması istendi çünkü BT yenilikleri hızla yayılma ve sistemik bir risk oluşturma potansiyeline sahip. Buna rağmen AB, inovasyonu engellemekten kaçınmak için önleyici düzenleme yerine ihtiyati denetimi tercih etmektedir (URL-11, 2016). Avrupa Komisyonu'ndan, teknolojik gelişmeleri yakından takip etmek ve zamanı geldiğinde bilgi ve iletişim teknolojisi düzenlemeleri için teklifler sunmak üzere bir çalışma grubu oluşturması talep edilmiştir.

Federal Rezerv, Menkul Kıymetler ve Borsa Komisyonu, Hazine Bakanlığı ve ilgili eyalet düzenleyicileri, Amerika Birleşik Devletleri'nde blok zincirine ilişkin düzenleyici politikayı etkileyen ana kuruluşlardır. Genel olarak, piyasa katılımcılarının blok zincirleri konusunda çok az deneyimi olduğu ya da hiç deneyimi olmadığı için, teknolojinin operasyonel kusurlarının yaygın olarak uygulanana kadar keşfedilmeyeceğine inanmaktadırlar (Yeoh, 2017).

Bu faydalı uygulamalar gün yüzüne çıkmaya başlasa da, bazı kanun yapıcılar ve düzenleyiciler kara para aklama ile bağlantılı olduğu iddiaları nedeniyle blok zinciri teknolojisinin Bitcoin ile olan yakın bağlarına şüpheyle yaklaşmaktadır. Örneğin, 2015 yılında Kara Para Aklama Mali Eylem Görev Gücü, Liberty Rezerve kurucularının altı yıllık

bir süre zarfında yüz milyonlarca ABD dolarını aklayarak suç örgütlerinin yararına katkıda bulunduklarını ortaya çıkarmıştır. Blok zincirinin daha kapsamlı ve derin kullanımları, ölçeklenebilirlik ve teknoloji, iş modelleri, kamuoyu ve skandallar, kişisel verilerle ilgili gizlilik endişeleri ve yasal kısıtlamalarla ilgili sorunlar nedeniyle kısıtlanabilir (Monrat vd., 2019). Daha açık bir ifadeyle, blok zinciri'nin finansal hizmetler sektöründe işletmeler tarafından benimsenmeden önce aşması gereken on önemli engel bulunmaktadır. Maliyetler ve faydalar, maliyet paylaşımı, teşvik uyumu, standartların gelişimi, ölçeklenebilirlik, yönetim, yasal riskler, güvenlik, basitleştirme ve düzenleyici müdahaleler bu endişelerden bazılarıdır. Teknolojik ilerlemenin kapsamı ve hızı yasa ve yönetmeliklerden etkilenebilir. Teknolojinin finansal sistemdeki sistemik riskleri istemeden artırma potansiyeli ışığında, düzenleyici stratejiler teknolojinin yenilikçi ruhuna karşı dikkatle tartılmalıdır.

5.5. Geleceğin Teknolojileri Kapsamında Blok Zincirinin Potansiyeli

Araştırmalara göre blok zinciri hem akademide hem de iş dünyasında muazzam bir potansiyele sahip olarak görülmektedir.

Blok zinciri teknolojisi, yatırımcılara muazzam kâr olanakları sunarak yatırımcıları kendine çekmeyi başarıyor. Bu teknolojiyi bir iş çözümünde kullanmak için öncelikle gereksinimleri karşılayıp karşılamadığının belirlenmesi gerekir. Blok zinciri tabanlı çözümler için bu, sistemin faydalarını ve dezavantajlarını değerlendirmek için standart bir test prosedürüne ihtiyaç duyulduğu anlamına gelir. Standardizasyon aşaması ve test aşaması, bu sürecin ikiye ayrılabilceği iki aşamadır (Monrat vd., 2019). Bir dizi kesin kritere dayanan ilk aşama, geliştiricilerin blok zinciri çözümleriyle ilgili iddialarını doğrulayacaktır. Blok zinciri tabanlı çözümün performansının belirlenmesi test aşamasının amacıdır. Örneğin, blok zinciri tabanlı çözümün performansı bir online perakende şirketinin sahibini endişelendirmektedir. Bu nedenle, edinilen çözüm platformunun verimini, kapasitesini ve gecikme süresini değerlendirmek için test ve standardizasyon prosedürlerine sahip olmak gerekir (URL-9, 2019).

Blok zinciri teknolojisinin kullanımıyla işletmeler artık buluşlarını dijital olarak belgeleyebilir ve blok zinciri teknolojisinin geçerliliğini, güvenilirliğini ve etkinliğini ve ayrıca herhangi bir fikri mülkiyet varlığının varlığını, sahipliğini ve bütünlüğünü gösteren yeni patentler, kavram kanıtları ve tasarımlar için sertifikalar düzenleyebilir. Ticari sırlar ve

telif hakları, diğer noter onaylı verilerin yanı sıra, özel kriptografi katmanı kullanılarak gizli ve güvenli tutulabilir.

Buna ek olarak, blok zinciri teknolojisi ve büyük veri analitiği, özellikle veri yönetimi ve analizi söz konusu olduğunda birlikte iyi çalışacaktır. Blok zinciri teknolojisi, veri yönetimi amacıyla veri depolamayı güvenli bir şekilde dağıtmak için kullanılabilir. Buna ek olarak, verilerin gerçekliği blok zincirinin değişmezliği ile garanti altına alınabilir. Örneğin, dağıtılmış defterde saklanan hasta tıbbi kayıtlarını tahrif etmek zor olacaktır ve hiç kimse sahibinin izni olmadan bu bilgileri ele geçiremez. Veri analizi blok zinciri işlemleri kullanılarak gerçekleştirilebilir. Blok zinciri ağındaki potansiyel ortakların iş stratejileri ve eylemleri bu süreç aracılığıyla doğrulanabilir (Monrat vd., 2019).

Akıllı sözleşmeler, blok zinciri için gelişmekte olan bir başka uygulama alanıdır. Blok zinciri tabanlı akıllı sözleşmeler, bankacılık hizmetleri ve Nesnelerin İnterneti platformları da dahil olmak üzere çeşitli potansiyel kullanım alanlarına sahiptir. Geliştirme ve değerlendirme, akıllı sözleşme araştırmalarının girdiği iki kategoridir. Zaman içinde akıllı sözleşmeler için bir platform oluşturulması tamamlanabilir (URL-11, 1999). Online alışveriş ve araba açık artırmaları da dahil olmak üzere birçok akıllı sözleşme tabanlı uygulama Ethereum'un altyapısı ile hayata geçirilebilir. Değerlendirme, performansın yanı sıra kod analizini de kapsar. Gösterdiğimiz gibi, akıllı sözleşmeler oluşturulurken yapılacak küçük bir hata bile yıkıcı sonuçlar doğurabilir.

Bununla birlikte, akıllı sözleşme performansı önemli bir çalışma alanı haline gelebilir. Blok zinciri teknolojisi kamusal ve özel alanlarda ilgi gördükçe, giderek artan sayıda akıllı sözleşme oluşturulmaktadır.

5.5.1. Dağıtık Defter Teknolojisinin Gelecekteki Üç Uygulaması

Danışmanlık firması McKinsey'e göre, dağıtık defter teknolojisinin değer yaratabileceği üç farklı alan aşağıdaki gibidir (URL-2, 2019):

1. Özel kullanımları olan uygulamalar: Bunlar, varlıkların sahipliğini ve durumunu izlemek için veri entegrasyonunu içerebilir. Tedarik zincirleri, sigorta ve piyasa finansmanı bu uygulamaların bazı örnekleridir. Bu piyasalar, dağıtık

defterleri bütünleştirerek üretkenliği, şeffaflığı ve sahtekarlığı önlemeyi artırabilir.

2. Modernizasyon yoluyla değer yaratma: Bunların hedeflediği sektörler, stratejik olarak inovasyona odaklanan sektörlerdir ve blok zinciri teknolojisi, dijitalleşme, süreç basitleştirme ve iş birliğini içeren modernizasyon hedeflerine ulaşmalarına yardımcı olmaktadır. Özellikle ödemeler ve ticaret finansmanı akla gelmektedir. Ancak, bu özel durumda, teknoloji çeşitliliğin yalnızca bir ucudur ve gerçek dağıtılmış kayıtlara bağlı olması gerekmemektedir.

3. İtibar için değer: İtibar nedeniyle, bazı oyuncular hala bu teknolojiyi geliştirmekte ve finanse etmektedir. Bunun amacı, rakiplere ve yatırımcılara projeyi piyasaya sunmadan da yenilik yapabileceklerini göstermektir. Anlık oylama, IoT ağları ve müşteri sadakatine odaklanan projeler bu kategoriye girmektedir.

Ancak bugün hala pek çok oyuncu bu teknoloji hakkında yanlış kanılara sahiptir. Bu bilgisizliğin yanı sıra yatırımın geri dönüşünü sağlamak için artan bir baskı da bulunmaktadır. Bununla beraber bu teknoloji, halen yönetim, çevresel etki, hukuk sistemi, güvenlik yönetimi ve değerın yalnızca itibara dayalı olarak belirlenmesi gibi bir dizi zorlukla karşı karşıyadır. Dahası, merkeziyetsiz bir ortam ilkesi gereğince kurumsal hedefler yeniden değerlendirilmek zorunda kalmaktadır (Andriy, 2019). Ekonominin temeli olan finansal sistem, dijital teknolojiyi benimsediğini yeni yeni göstermeye başlamaktadır.

6. SONUÇ VE TARTIŞMALAR

İlk kez 2008 yılında Satoshi Nakamoto, bilgisayar bilimi ve kriptografi alanındaki bir dizi gelişmeyi bir araya getirerek inanılmaz derecede zarif bir çözüm olarak dağıtık defter teknolojisini üretmeyi başardı. Bu, blok zinciri teknolojisini kullanmanın ilk yöntemi olsa da, bununla sınırlı değildir. Kripto para birimlerine güç veren teknoloji olan blok zinciri, sanal paranın ötesine geçen bakış açıları sağlar. Karşılıklı güvene dayalı merkezi olmayan bir yapıyı teşvik eder. Blok zinciri, alış verişi özgürleştirmek ve araçlar olmadan değer akışına izin vermek için bir fırsattır. Üçüncü bir tarafa ihtiyaç duymadan eşler arası bir mimari üzerinde çalışan bu meta-teknoloji şu özellikleriyle öne çıkmaktadır:

- İşlemlerin doğrulanmadan kaydedilmesini sağlayan bir mutabakat algoritması belirli bir aktör tarafından değil, bir uzlaşım tarafından onaylanan bir protokol tarafından tanımlanır.
- Asimetrik kriptografi, bir alışverişin şifrelenerek bilginin güvence altına alınmasını sağlar.
- Bir sistemin sürekliliğini ve tutarlılığını sağlayan bir ağ oluşturan bir dizi düğüm bulunan dağıtılmış bir kayıttır.

Öte yandan, Nick Szabo'nun Ethereum tabanlı akıllı sözleşmeleri, insan müdahalesine gerek kalmadan bir blok zinciri içinde bir bilgisayar programını özerk olarak çalıştırabilir. Bu programlanabilir "kayıt" veya "defter" onu ölçeklenebilir ve akıllı hale getirir. Sonuç olarak, bu akıllı sözleşmeler, oyuncular arası güven veya merkezi katılım gereksizdir sözleşmeye dayalı bir bağlantı oluşturma fırsatı sunar.

Kurumlara duyulan güvensizliğin ve kolektif zekanın internet aracılığıyla yayılmasının bir sonucu olarak ortaya çıkan dağıtık defter teknolojisi bir tesadüf değildir. Güvenin hassas dengesi hem çaba hem de bilgi gerektirmektedir. Günümüzün sözde "dışsallaştırılmış" güven modelleri, etkileşimlerdeki artışla başa çıkamadıkları ve azalan verim yasasıyla mücadele etmek zorunda kaldıkları için sınırlılıkları bulunmaktadır. Topluluk güven modelini kolaylaştıran ağlar sayesinde, ölçeklenebilir olduğu için daha yüksek hacimli etkileşimler yönetilebilmektedir. Blok zinciri bu ayrışmayı güçlendirmektedir. Buna ek

olarak, algoritmalar her zamankinden daha fazla güvenilmektedir. Günlük hayattaki önemleri arttıkça, organizasyon yapılarının yeniden gözden geçirilmesi gerekmektedir. Aracılık maliyetlerinin düşürülmesi, blok zinciri teknolojisinin ekonomik ilkelerinden biridir. Banka benzeri bir aracı, katılımcılar arasındaki bilgi asimetrisini azalttığına piyasa değeri kazanmaktadır.

Aracı, onaylama ve doğrulama işlemleri sayesinde ahlaki tehlike olasılığını da azaltmaktadır. Aracının işlevi, ekonomik risklerin seviyesiyle birlikte artmaktadır. Blok zinciri teknolojisinin kullanım alanları çoktur ve şunları içerir:

- Bilgi veya değerin aracısız iletimi
- Bilgi depolama ve paylaşımı
- Veri ve değerlerin güvenliğini sağlama
- Malların veya hakların sahipliğinin doğrulanması

Blok zinciri, finans da dahil olmak üzere bir dizi sektörü tamamen değiştirme gücüne sahip çığır açan bir buluş olarak duyurulmuştur.

Blok zinciri teknolojisinin finansal piyasalarda çeşitli kullanımları vardır ve yerleşik finansal kurumları altüst etme potansiyeline sahiptir. Para maddi olmayan bir öge olduğundan, onu bir blok zinciri ağına entegre etmek mantıklı bir uyumdur. Bitcoin, ulusal para birimlerinin yerine dünya çapında, merkezi olmayan bir para koymayı amaçlamaktadır. Dijital para birimi ve ödeme uygulamaları, blok zincirinin finans sektöründeki başlıca kullanım alanları arasındadır. Blok zinciri teknolojisinin mümkün kıldığı Bitcoin gibi kripto para birimlerinin gelişimi, değer alışverişi ve iş yapma şeklimizi tamamen dönüştürme potansiyeline sahiptir.

Akıllı sözleşmeler, blok zincirinin finans piyasalarında kullanılmasının bir başka yoludur. Kendi kendini yürüten sözleşmeler ya da akıllı sözleşmelerin şartları doğrudan koda kodlanmıştır. Bu, sözleşmelerin otomatik olarak ve güven olmadan yürütülmesini mümkün kılarak aracılara olan ihtiyacı ortadan kaldırır ve finansal piyasa prosedürlerini basitleştirir.

Blok zinciri teknolojisinin bir özelliği olan akıllı sözleşmeler, ticari işlemler ve belirli yasal veya sözleşmesel gerekliliklerin uygulanması için bir dizi yeni olasılık getirebilir.

- Blok zinciri teknolojisini kullanarak izin, önalım veya devredilemezlik hükümlerine uyumu garanti edebilir.
- Hisse senedi opsiyonları veya temettüler üzerinden sermaye kazançlarını otomatik olarak ödeyin.
- Hissedarlık eşiklerini yönetin.
- Hissedarların anında ifşa edilmesi, aktivist hissedarlar tarafından düşmanca devralmaların azalmasına yol açmıştır.
- Durum tespiti ve denetimler, doğru hissedar kayıtları ile kolaylaştırılır, çünkü sağladıkları ilgili ve güvenilir yasal bilgiler onları birleşme işlemleri ve varlıkların kısmi katkıları için yararlı kılar.

Hem borsada işlem gören hem de görmeyen hisse senetleri için blok zinciri, piyasa ve piyasa sonrası faaliyetlerde geniş bir potansiyel yelpazesi sunmaktadır.

Menkul kıymetler piyasasında uygulama şunları içerir: katılımcılar arasında çok taraflı ticaret sisteminin geliştirilmesi; bir menkul kıymetin alım/satım döngüsünün hızlandırılması; borsaların şeffaflığının ve güvenliğinin artırılması, likidite riskinin azaltılması; daha basit denetim prosedürleri yoluyla düzenlemenin geliştirilmesi; maliyetlerin ve sürtünmenin azaltılması ve piyasanın daha fazla katılımcıyı kapsayacak şekilde genişletilmesidir.

Mutabakat/teslimat işlemleri: gelişmiş izlenebilirlik ve doğrulanmış işlem gerçekliği ile finansal piyasada menkul kıymet borsaları; daha düşük karşı taraf ve sistemik risktir.

Varlık yönetimi şunları içerir: kısaltılmış uygulama süreleri; azaltılmış komisyon maliyetleri; ve daha iyi hisse aboneliği ve itfa yönetimidir.

Finansal piyasaların güvenliği ve şeffaflığı da blok zinciri teknolojisi ile geliştirilebilir. Blok Zinciri'nin merkezi olmayan yapısı, her işlemi halka açık bir deftere kaydederek daha fazla şeffaflık ve değişmezlik sağlar. Dolandırıcılığın azaltılması ve finansal sistemlere olan güvenin artırılması bundan faydalanabilir.

Blok zinciri teknolojisi aynı zamanda masrafları azaltma ve finansal piyasaların etkinliğini artırma yeteneğine de sahiptir. Blok zinciri teknolojisi, aracılara olan ihtiyacı ortadan

kaldırarak ve prosedürleri basitleştirerek işlem maliyetlerini düşürmeye ve finansal işlemleri hızlandırmaya yardımcı olabilir.

Blok zincirinin önümüzdeki yıllarda, özellikle ticaret finansmanının operasyonel karmaşıklığı nedeniyle birçok paydaşın dahil olduğu uluslararası ticarete ticaret finansmanının bozulmasında önemli bir rol oynaması bekleniyor. Ödeme araçlarının dijitalleştirilmesi, kredi araçlarına dönüştüklerinden beri oldukça kolaylaştı. Bankalar bu işlemlerde karşılıklı güven sağlayan üçüncü taraf katılımcılardır.

- Satıcının ödemesinin kanıtını anında sağlayan akreditif; akıllı sözleşmelerin mümkün kıldığı uyumluluk görevlerinin otomatik olarak yürütülmesi; akıllı sözleşme doğrulamasını takiben ödemelerin otomatik olarak gerçekleştirilmesi.
- Tokenleştirme yoluyla teslimat ve takip kanıtı: bu, zimmete para geçirme riskini azaltır, paydaş doğrulamasını hızlandırır, sigorta maliyetlerini düşürür ve işletmelere kargonun taşıma sırasındaki durumuna ilişkin görünürlük sağlar. Ayrıca tüm süreci dijitalleştirir ve kâğıt belgeleri ortadan kaldırır.

Sınır ötesi ödeme verimliliği blok zinciri teknolojisi kullanılarak büyük ölçüde artırılabilir. "Bankalararası Bilgi Ağı" (INN), JP Morgan'ın öncülük ettiği ve dünya çapında 75 kurumu kurmaya ikna edebildiği yeni bir ağıdır. Bu ağ, ödeme sürelerinin birkaç güne kadar kısılmasını sağlayacaktır.

Son olarak, bankalar tarafından sunulan "Müşterini Tanı" (KYC) müşteri doğrulama süreci yoluyla seçenekler bulunmaktadır. Dağıtık kayıtlarla mümkün kılınan bankalar arası işbirliği, blok zinciri teknolojisi ile mümkün kılınmakta olup, hedefler düzenleyici gerekliliklerin karşılanmasıyla ilgili maliyetlerin azaltılması, şeffaflığın artırılması ve daha iyi müşteri deneyimi olarak belirlenmiştir.

Blok zinciri teknolojisi de bir dizi önemli sorun ve kısıtlama ile kuşatılmıştır.

Ölçeklenebilirlik, blok zinciri teknolojisi için büyük bir sorundur. Bir blok zinciri ağındaki işlem hacmi arttığında sistemin işlemleri işleme ve doğrulama kabiliyeti vergilendirilir, bu da işlem sürelerinin gecikmesine ve ücretlerin artmasına neden olur. Kapsamlı uygulamalar için blok zinciri teknolojisinin geniş çapta uygulanması, bu ölçeklendirme sorunu nedeniyle engellenmiştir.

Blok zinciri teknolojisinin enerji tüketimi de bir başka dezavantajdır. Bir blok zinciri ağının madencilik ve doğrulama süreçleri çok fazla işlem gücü gerektirir ve bu da enerji kullanımını artırır. Bu durum, özellikle daha enerji verimli ikameler arandıkça, blok zinciri teknolojisinin çevreyi nasıl etkileyebileceğine dair sorulara yol açmıştır.

Blok zinciri teknolojisinin başa çıkması gereken yasal ve düzenleyici sorunlar da vardır. Blok zinciri ağlarının merkezi olmayan ve sözde anonim özellikleri, özellikle müşterini tanı ve kara para aklamayı önleme yasalarına uymak söz konusu olduğunda, kolluk kuvvetleri ve düzenleyici kurumlar için zorluklar yaratmaktadır. Bu durum, finans gibi yüksek düzeyde düzenlemeye tabi sektörlerin blok zinciri teknolojisini kullanmasını daha da zorlaştırmıştır.

Güvenlik ve gizlilik sorunları blok zinciri teknolojisiyle ilgili bir başka sorundur. Blok zinciri ağları merkezi olmayan yapıları nedeniyle bir ölçüde güvenlidir, ancak yine de güvenlik kusurlarına ve siber saldırılara karşı hassastırlar. Ayrıca, RGPD gibi kişisel verilerin korunmasını düzenleyen yasaların arka planı göz önüne alındığında, bir blok zincirinde depolanan verilerin değişmezliği, gizlilik ve unutulma hakkı ile ilgili sorular ortaya çıkarmaktadır.

Kısacası blok zinciri teknolojisi, gelecekte çeşitli sektörlerde devrim yaratma potansiyeli ile 21. yüzyılın en umut verici yeniliklerinden biri haline gelmiştir. Blok zinciri teknolojisinin merkezi olmayan ve güvenli yapısı, iş yapma, verileri yönetme ve birbirimizle etkileşim kurma şeklimiz üzerinde önemli bir etkiye sahip olabilecek geniş bir uygulama yelpazesi sunmaktadır. Geleceğe baktığımızda, blok zinciri teknolojisinin dijital ortamın evriminde çok önemli bir rol oynayacağı açıktır.

Blok zinciri teknolojisinin derin bir etki yaratması beklenen en önemli alanlardan biri finans sektörüdür. Finans sektöründe blok zinciri teknolojisinin kullanılması, süreçleri kolaylaştırma ve otomatikleştirme, maliyetleri azaltma ve şeffaflık ile güvenliği artırma potansiyeline sahiptir.

Buna ek olarak, blok zinciri teknolojisi tedarik zinciri yönetimi, sağlık hizmetleri, gayrimenkul ve dijital kimlik doğrulama gibi diğer sektörlerde de devrim yaratacaktır.

Dahası, blok zinciri teknolojisinin geleceđi, merkezi olmayan uygulamalar ve akıllı sözleşmeler için de umut vaat etmektedir.

Bunlar arasında mevzuat belirsizliđi, ölçeklenebilirlik sorunları ve farklı blok zinciri ađları arasında birlikte çalışabilirlik ihtiyacı yer almaktadır. Buna ek olarak, blok zinciri teknolojisinin çevresel etkileri, özellikle de kripto para madenciliđiyle ilişkili enerji tüketimi konusunda endişeler bulunmaktadır.

Sonuç olarak, blok zinciri teknolojisinin geleceđi parlaktır ve çeşitli sektörleri dönüştürme ve iş yapma ve birbirimizle etkileşim kurma şeklimizde devrim yaratma potansiyeline sahiptir. Teknoloji gelişmeye ve olgunlaşmaya devam ettikçe, yaygın olarak benimsenmesini ve toplum üzerindeki olumlu etkisini sağlamak için paydaşların iş birliđi yapması ve zorlukları ele alması çok önemlidir. Doğru yaklaşımla, blok zinciri teknolojisi daha şeffaf, verimli ve kapsayıcı bir dijital gelecek yaratma potansiyeline sahiptir.

Bu konuda gelecekteki tez çalışmaları için aşağıdaki önerileri düşünebilir.

- Farklı Finansal Sektörlerde Dağıtık Defter Teknolojisi (DDT) Uygulamalarının Karşılaştırılması: Bankacılık, sigortacılık, yatırım gibi farklı finansal sektörlerde DDT'nin nasıl uygulandığını ve sektörel farklılıkları inceleyebilir. Her sektörün karşılaştığı özel engelleri ve fırsatları belirleyerek analiz edebilir. Bu konuda gelecekteki tez çalışmaları için aşağıdaki önerileri düşünebilir.
- Regülasyon ve Yasal Çerçeve Üzerine Bir İnceleme: Finans sektöründe DDT'nin yaygınlaşmasını engelleyebilir veya teşvik eden yasal düzenlemeleri araştırabilir. Farklı ülkelerdeki regülasyonların DDT uygulamaları üzerindeki etkisini değerlendirebilir.
- Gizlilik ve Güvenlik Konularının İncelenmesi: Finansal verilerin güvenliđi ve kullanıcı gizliliđi DDT uygulamaları için kritik öneme sahiptir. Bu konuları mercek altına alarak, mevcut güvenlik önlemlerinin yeterliliđini ve geliştirme alanlarını tartışabilir.
- DDT ve Finansal Dahil Etme (Financial Inclusion): Düşük gelir grupları veya kırsal bölgeler gibi finansal sistemden uzak kesimlerin DDT aracılığıyla finansal hizmetlere erişimini nasıl iyileştirebileceğini inceleyebilirsiniz.

- Gelecekteki Trendler ve Öngörüler: Finans sektöründe DDT'nin geleceği hakkında öngörülerde bulunmaktadır. Yapay zeka, IoT gibi diğer teknolojilerle entegrasyonu ve bu entegrasyonun finans sektörüne etkilerini değerlendir.
- Uygulama Örnekleri ve Başarı Faktörleri: Başarılı DDT uygulamalarını inceleyerek, bu uygulamaların arkasındaki başarı faktörleri ve bu faktörlerin diğer organizasyonlar için nasıl uyarlanabileceğini araştırabilir.
- Sürdürülebilirlik ve Çevresel Etkiler: DDT'nin enerji tüketimi ve çevresel etkileri üzerine bir değerlendirme yaparak, bu teknolojinin sürdürülebilirlik açısından nasıl optimize edilebileceğini araştırabilir.



KAYNAKLAR

- Andriy, G. (2019). Rôle et enjeux de la technologie de la Blockchain dans les activités d'intermediation bancaires. s.80-84.
- Ashik, M. H., Shahriar, M.M.S.Maswood., Alharbi,A.G., & Medhi,D.(2020). FPoW: An ASIC-resistant Proof-of-Work for Blockchain Applications. IEEE Xplore, s.4.
- Avunduk, H., & Aşan, H. (2018). Blok Zinciri (Blockchain) Teknolojisi ve İşletme Uygulamaları: Genel Bir Değerlendirme. Dokuz Eylül Üniversitesi İktisadi İdari Bilimler Fakültesi Dergisi, 33(1), 369-384. <https://doi.org/10.24988/deuiibf.2018331746>.
- Back, A., & al. (2002). Hashcash-a denial of service counter-measure.
- Banerjee, S. S., & Chandani, A. (2022). Challenges of blockchain application in the financial sector: a qualitative study. *Journal of economic and administrative science*, s.8.
- Basumatary, A., & Joshi, S. (2022) Adoption Of Blockchain In Trade Finance And Its Impact On Financial Decision Making. *2022 International Conference on Decision Aid Sciences and Applications (DASA)*, Chiangrai Thailan. [10.1109/DASA54658.2022.9765150](https://doi.org/10.1109/DASA54658.2022.9765150).
- Bayer, D., Haber, S., & Stornetta, W. S. (1993). Improving the efficiency and reliability of digitaltime-stamping. *In Sequences II*. Springer, 329–334.
- Brands, S. (1993). Untraceable off-line cash in wallet with observers. *In Annual international cryptology conference*. Springer, 302–318.
- Buterin, V., & al. (2013). Ethereum white paper. *GitHub repository*, vol. 1, s. 22–23.
- Biryukov, A., & Pustogarov, I. (2015). Bitcoin over tor isn't a good idea. *IEEE Symp. Secur. Privacy*, S. 122–134.
- Cao, B., & al. (2019). When Internet of Things Meets Blockchain: Challenges in DistributedConsensus. *Journals & Magazines*, (33). S. 133-139.
- Carson, B., Higginson, M., & London, S. (2018). Blockchain explained: What it is and isn't, and why it matters. McKinsey and Company, s. 7.
- Caseau , S ., & Soudoplatoff, S. (2016). La Blockchain ou la confiance partagée. *Fondation pour l'innovation politique*. s.12-14.
- Catalin, C., & Gans, J. (2020). Some simple economics of the Blockchain. *Digital library*, 63(79). s. 80-90. <https://doi.org/10.1145/3359552>.
- Chaum, D. (1983). Blind signatures for untraceable payments. *In Advances in cryptology*. Springer, s. 199–203.
- Chaum, D., Fiat, A., & Naor, M. (1988). Untraceable electronic cash. *In Conference on the*

- Theory and Application of Cryptography*. Springer, 319–327.
- Collomb, A., & Sok, k. (2016). Blockchain/Distributed ledger technology (DLT): what impact on the financial sector? , *Digiworld economic journal*, s. 1.
- Collomb, S., & Sok, K. (2017). Blockchain: A Monetary and Financial Revolution, *Economie politique*, s. 70-82.
- Dai, W. (1998). Cryptocurrencies: Are Disruptive Financial Innovations Here? *Modern Economy*, 6(7). <http://www.weidai.com/bmoney.txt>.
- Dinçel, C., (2020). Blok Zinciri Teknolojisinin Muhasebe ve denetim mesleğine etkisi. *Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı, İstanbul*, 58s.
- De soto, H., (2000). Integrating the poor into official legal system can unleash their economic potential. *International Monetary Fund*, s 16. <https://doi.org/10.5089/9781451926088.023>.
- Eduardo Demarco, A (2020). Analysing blockchain/distributed ledger technology in capital markets and know your customer process. *Journal of Securities Operations & Custody*, 12 (1), s 58-71.
- Eyal, I., & Sirer, E. G., (2018). Majority is not enough: Bitcoin mining is vulnerable. *Digital library*, (7), s.95-102.
- Ferguson, N., (1993). Single term off-line coins. In *Workshop on the Theory and application of Cryptographic Techniques*. Springer, s. 318–328.
- Gan,Q. Q., Lau. R.Y.K., & Hong, J. (2021). A critical review of blockchain applications to banking and finance: a qualitative thematic analysis approach. *Technology Analysis & Strategic Management*, s.11 <https://doi.org/10.1080/09537325.2021.1979509>.
- Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Springer open: Financial innovation*, s.6.
- Haber, S., & Stornetta, W. S. (1990). How to time-stamp a digital document, in Conference on the Theory and Application of Cryptography. *Springer*, 437–455. s.12-13.
- Henry, R., Herzbberg, A., & Kate, A. (2018). Blockchain Access Privacy: Challenges and Directions. *IEE Security & Privacy*, s.39.
- Higginson, M., Nadeau, M., & Rajgopal, K. (2019). Blockchain's Occam problem. *McKinsey and Company*, s. 41-43.
- Jalan, A., & al. (2023). The role of interpersonal trust in cryptocurrency adoption. *Journal of international financial markets, Institutions and money*, (83).
- Joy, J.G., & Sebastian, K. (2020). Blockchain in Real Estate. *International Journal of Applied Engineering Research*, s.930-932.

- Kakavand, H., De Sevres, N. K., & Chilton, B. (2017). The blockchain revolution: An analysis of regulation and technology related to distributed ledger technologies, *SSRN*, s.17.
- Kapsoulis, Nikolaos., ve diğerleri. (2020). Know Your Customer (KYC) Implementation with Smart Contracts on a Privacy-Oriented Decentralized Architecture. *Future internet*, 12 (2), s 41 <https://doi.org/10.3390/fi12020041>.
- Kumar, N., Aggarwal, S., & Raj, P. (2021). The blockchain technology for secure and smart applications across industry verticals. *Science direct*, s.14.
- Laurent, M. (2018). La blockchain est-elle une technologie de confiance, *HAL Archives ouvertes*, s.6. hal-01778949.
- Law, L., Sabett, S., & Solinas, J. (1996). How to make a mint: the cryptography of anonymous electronic cash, Amsterdam. *UL Rev.*, vol. 46, s. 1131.
- Malviya, H. (2017). Blockchain for Real Estate. White Paper, s.6.
- Monrat, A. A., Schelén, O., & Andersson, K. (2019). A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. *IEEE ACCESS*, 117-145.
- Morgan, J.P. (2018). Blockchain and the decentralization revolution. s.12-13.
- Moyano, J.M., & Ross, O. (2017). KYC Optimization Using Distributed Ledger Technology. Edition. *Springer*, s.2.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Unpublished manuscript*.
- Nayak, K., Kumar, S., Miller, A., & Shi, E. (2016). Stubborn mining: Generalizing selfish mining and combining with an eclips attack. *cryptology ePrint Archive*, s.3-9.
- Oerel, J.V., & Lemmens, P. (2016). Distributed ledger technology for the financial industry. *White paper for professional investor*, s.2.
- Oerel, J.V., & Lammens, P. (2016). Distributed ledger technology for the financial industry Robecco: the investment ingeneers, s.12.
- O'Dwyert, K. J., & Malone, D. (2018). Bitcoin Mining and its Energy Footprint. *IEEE Xplore*, s. 6.
- Oh, J., & Shong, I. (2017). A case study on business model innovations using blockchains: focusing on financial institutions. *Asia Pacific Journal of Innovation and entrepreneurship*, s.7-8.
- Pignel, M. (2019). La technologie blockchain une opportunité pour l'économie sociale? *Pour la solidarité*, s.3.
- Rao, S., & Saritha, K. (2022). Blockchain technology for emerging application. *Science*

direct, s.33-6.

- Rossignol, E., & Laurent, X. (2017). La blockchain, un levier de digitalisation pour les banques de financement et d'investissement, Cairn.info: Réalités industrielles, s.4.
- Ruffing, T., Moreno-Sanchez, P., & Kate, A. (2014). CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. Springer Link, s. 345-364.
- Sapirshtein, A., Sompolinsky, Y., & Zohar, A. (2016). Optimal selfish mining strategies in Bitcoin. *arXiv*, s.19-20.
- Sedlmeir, J., Buhl, H.U., Fridgen, G., & Keller, R. (2020). The Energy Consumption of Blockchain Technology: Beyond. *Springer*, s.601.
- Slepak, G., & Petrova, A. (2017). The DCS Theorem. *Computer science*, s.2.
- Smith, S.M., & Khovratovich, D. (2016). *Identity system Essentials*. Evernym, S.8.
- Swan, M. (2015). Blockchain blueprint for a new economy. Ed. O'reilly, s.14.
- Szabo, N. (1999). Micropayments and Mental Transaction Costs. *Satoshi Nakamoto Institute*.
- Toledano, J., & Janin, L. (2018). Rapport sur les enjeux de la Blockchain. *France Stratégie*, s. 49.
- Vamparys, X. (2018). La Blockchain au service de la Finance. *Edition RB*, s. 137
- Varma, J.R. (2019), Blockchain in finance, the journal for decision maker, s.5.
- Vukolic, M. (2016). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. *Springer*, s.4-10.
- Wayman, O. (2016). Blockchain in Capital Markets: *The Prize and the Journey*. Ed. Euroclear, s.10.
- Wu, B., & Duan, T. (2019). The Application of Blockchain Technology in Financial markets. *Journal of Physics: Conference Series*, s.3.
- Yeoh, P. (2017). Regulatory issues in blockchain technology. *Emerald Insight*, s.196-208.
- Yermack, D. (2019). Blockchain technology's potential in the financial system. *National Bureau of Economic Research*, s.3.
- URL-1 (2016). [\(https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain\)](https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain). (19.1.2024).
- URL-2 (2019). <https://www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem>. (4.1.2024).
- URL-3 (2017). <https://limechain.tech/blockchain-development/blockchain-poc-development/>. (4.1.2024).

- URL-4 (2023). <https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html>. (11.7. 2023).
- URL-5 (2022). <https://start-in-blockchain.fr/blockchain-interoperabilite-crosschain/>. (30.12.2022).
- URL-6 (2018). <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lshc-ehr-convergence-and-interoperability.pdf>. (6.11.2023).
- URL-7 (2022). <https://coinacademy.fr/academie/interoperabilite-blockchain-crypto-monnaie/>. (5.9.2022).
- URL-8 (2023). <https://digiconomist.net/bitcoin-energy-consumption>. (15.11.2023).
- URL-9 (2019). <https://www.wipro.com/blogs/hitarshi-buch/improving-performance-and-scalability-of-blockchain-networks/>. (5.11.2023).
- URL-10 (2016). <https://www.coindesk.com/markets/2016/04/29/europes-regulatory-blockchain-shift-on-display-at-private-parliament-event/>. (29.4.2024).
- URL-11 (1999) <https://nakamotoinstitute.org/library/micropayments-and-mental-transaction-costs/> . Satoshi Nakamoto Instituteş, (7.5.2023).
- URL-12 (2016). <https://www.pwc.co.uk/financial-services/fintech/assets/blockchain-in-capital-markets.pdf>. (28.4.2023).
- URL-13 (2017). <https://www.latribune.fr/entreprises-finance/banques-finance/la-blockchain-a-le-potentiel-de-transformer-le-trading-actions-selon-moody-s-686575.html>. (14.4.2024).
- URL-14 (2023). <https://4irelabs.com/articles/blockchain-tecnology-in-trade-finance/>. (30.1.2024).
- URL- 15 (2022). <https://phemex.com/academy/blockchain-in-trade-finance>. (10.2.2022).
- URL-16 (2022). <https://www.emeribanque.com/blogs/blockchain-technology-for-the-trade-finance>. (7.7.2022).
- URL-17 (2019). <https://www.coindesk.com/markets/2019/05/07/thai-central-bank-builds-blockchain-solution-for-digital-currency-project/>. (12.12.2022).
- URL- 18 (2020). <https://confirm.ie/how-does-a-blockchain-work/>. (25.4.2024).
- URL-19 (2023). <https://cointelegraph.com/learn/what-is-tokenized-realestate#:~:text=What%20is%20tokenization%20of%20real,used%20to%20define%20contractual%20specifics>. (14.2.2024).
- URL-20 (2019). <https://sanctionsscanner.com/blog/what-are-kyc-and-blockchain-why-is-kyc-important-for-crypto-exchanges-636>. (21.11.2023).

- URL-21 (2019). <https://actualiteinformatique.fr/blockchain/la-technologie-du-grand-livre-distribue-dlt>, (5.10.2023).
- URL-22 (2018). <https://etopia.be/blog:2018/04/09/blockhcaain-introduction-et-applications/> (9.4.2023).
- URL-23 (2021). <https://coinacademy.fr/academie/differents-algorithmes-consensus-blockchain/>, (17.4.2024).
- URL-24 (2022). <https://www.ironhack.com/fr/blog/qu-est-ce-qu-un-contrat-intelligent-ou-smart-contract>. (4.1.2022).
- URL- 25 (2023). <https://ts2.space/fr/architecture-b-spacelockchain-des-noeuds-aux-blocs/>, (22.4.2023).
- URL-26 (2023). <https://www.cointribune.com/cryptographie-la-cle-des-technologies-de-chiffrement-et-d-authentication/>, (13.4.2023).
- URL- 27 (2018). <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/blockchain-explained-what-it-is-and-isnt-and-why-it-matters>, (28.9.2023).
- URL-28 (2024), <https://hackernoon.com/fr/les-cypherpunks-%C3%A9crivent-du-code-pour-les-contrats-intelligents-de-Nick-Szabo-et-Bitgold>. (4.1.2024).
- URL-29 (2016), <https://www.theguardian.com/world/2016/jul/07/blockchain-answer-life-universe-everything-bitcoin-technology>(4.1.2024).
- URL-30 (2023),<https://www.financemagnates.com/fintech/payments/interbank-lockchains-and-the-on-chain-payments-horizon/>. (21.07.2023).
- URL-31 (2019), <https://www.sanctionsanner.com/knowledge-base/know-your-customer-kyc-46> (21.07.2023).
- URL-32 (2023), <https://4irelabs.com/articles/blockchain-technology-in-trade-finance/>. (30.12.2023).
- URL-33 (2016) <https://www.weblaw.co.uk/ebooks/eGuide-BlockchainTheConceptandtheLaw.pdf>(21.07.2023).
- URL-34 (2023) <https://swisscyberinstitute.com/blog/how-blockchain-providers-protect-themselves-from-cyberattacks/> (4.1.24).

