T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

BLOK ZİNCİR TEKNOLOJİSİ ve %51 SORUNSALI

Yüksek Lisans Tezi

Tezi Hazırlayan:
Ali Osman TİKVEŞLİ

İstanbul, 2019

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

BLOK ZİNCİR TEKNOLOJİSİ ve %51 SORUNSALI

Yüksek Lisans Tezi

Tezi Hazırlayan:
Ali Osman TİKVEŞLİ

Öğrenci No:
160820815

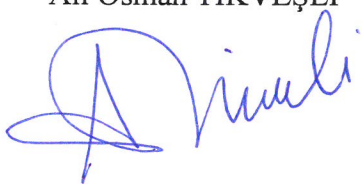
Danışman:
Dr. Öğr. Üyesi Atınç YILMAZ

İstanbul, 2019

YEMİN METNİ

Yüksek Lisans Tezi olarak hazırladığım "Blok Zincir Teknolojisi ve %51 Sorunsalı" isimli çalışmamın tüm belge ve bilgilerini akademik kurallar ve bilimsel ahlak kurallarına uyarak hazırladığımı, faydalandığım tüm kaynak ve eserlere bilimsel kurallar çerçevesinde atıfta bulunduğumu belirtir ve tarafımdan özgün bir şekilde yazıldığını açıkça beyan ederim.11/05/2019

Ali Osman TİKVEŞLİ



T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZ SAVUNMA SINAVI SONUÇ TUTANAĞI

Beykent Üniversitesi
Fen Bilimleri Enstitüsü Müdürlüğü'ne,

Aşağıda tez adı belirtilen yüksek lisans öğrencisi 160820815 no'lu Ali Osman Tikveşli'in 13/06/2019 tarihinde yapılan tez savunma sınavı[1] sonucunda 45 dakika süreyle sunduğu ve savunduğu tezi hakkında[2] oybirliğiyle, BAŞARILI kararı verilmiştir.

Bilgilerinize saygılarımızla arz ederiz.

Anabilim Dalı : Bilgisayar Mühendisliği
Programı : Bilgisayar Mühendisliği
Tez Başlığı[3] : Blok Zincir Teknolojisi ve %51 Sorunsalı

Tez Sınav Jürisi	Öğretim Üyesi	İmza
Danışman	: Dr.Öğr.Üyesi Atınç Yılmaz	
Üye	: Dr.Öğr.Üyesi Yusuf Bahtiyar SALMAN	
Üye	: Dr.Öğr.Üyesi Edip SAHKOL	

---

[1] Jüri üyeleri, söz konusu tezin kendilerine teslim edildiği tarihten itibaren en geç bir ay içinde toplanarak öğrenciyi tez sınavına alır. Tez savunma sınav süresi en az 45, en çok 90 dakikadır. Jüri üyeleri, sınav öncesi yapılacak toplantıda, kendi aralarından danışman dışında bir üyeyi başkan seçer. Tez sınavı, tez çalışmasının sunulması ve bunu izleyen soru-cevap bölümünden oluşur. Tez sınavı, öğretim elemanları, lisansüstü öğrenciler ve alanın uzmanlarından oluşan dinleyicilerin katılımına açık ortamlarda gerçekleştirilir. Belirlenen günde yapılamayan jüri toplantısı, katılanların hazırladığı bir tutanakla enstitü yönetimine bildirilir. Bu durumda, jüri en geç on beş gün içinde toplanarak adayı tez savunma sınavına alır. (05 Ağustos 2017 tarihli 30145 sayılı Resmi Gazetede Yayınlanan Değişiklik-Madde 29-3)

[2] Tez sınavının tamamlanmasından sonra jüri, tez hakkında salt çoğunlukla "kabul", "düzeltme" veya "ret" kararı verir. Jüri başkanı, jüri üyelerince imzalanmış karar tutanağını, tez sınavını izleyen üç gün içinde ilgili enstitü yönetimine teslim eder. Tezi hakkında düzeltme kararı verilen öğrenci en geç üç ay içinde gerekli düzeltmeleri yaparak ve birinci fıkradaki usule göre tezini aynı jüri önünde yeniden savunur. Süresi içerisinde "düzeltme" savunmasına girmeyen öğrencinin enstitü ile ilişiği kesilir. (Beykent Üniversitesi Lisansüstü Eğitim ve Öğretim Yönetmeliği-Madde 29-4)

[3] İleride doğabilecek aksaklıkların engellenmesi için tezin başlığının yazılması gerekmektedir.

Adı ve Soyadı : Ali Osman TİKVEŞLİ
Danışmanı : Dr. Öğr.Üyesi Atınç YILMAZ
Türü ve Tarihi : Yüksek Lisans, 2019
Alanı : Bilgisayar Mühendisliği
Anahtar Kelimeler : Blok Zincir, Blok, SHA256, Kriptografi, Özetleme, Merkle Ağacı, Çatallaşma, %51 Atağı

ÖZ

BLOK ZİNCİR TEKNOLOJİSİ VE %51 SORUNSALI

Çalışmanın amacı, dünya da gittikçe artan bir ilgi ve kullanım alanıyla önemli bir gündem oluşturan Blok Zincir teknolojisinin temel ve teknik anlamda detaylı olarak incelenerek, ülkemizde ve dünyadaki kullanım alanlarını göstermek, gelecekte öngörülen kullanım alanlarına değinmek. Bunların yanında Blok Zincir teknolojisinin avantaj ve dezavantajlarını değerlendirip, en önemli özelliklerinden biri olan dayanıklılık ve güvenlik politikasını teknik olarak incelemektir.

Blok Zincir yapısının mevcut sistemlere göre üstünlüğünü anlatarak, şu an 10 yılı aşkın süredir en büyük Blok Zincir olan ve İşin İspatı uzlaşı yöntemine göre çalışmakta olan Bitcoin yapısı ile blok zincir yapılarının en büyük riski olarak anılan "%51 Saldırısını" teknik anlamda incelenecek olup, hali hazırda kullanılan örnek blok zincir uygulamalarında %51 riskinin ne kadar olduğu matematiksel olarak gösterilecektir.

Name and Surname : Ali Osman TİKVEŞLİ
Supervisor : Assist.Prof. Dr. Atınç YILMAZ
Degree and Date : Master, 2019
Major : Computer Engineering
Key Words : Blockchain, Block,Hash,Mine, SHA256, Hashing, Concensus Algorithms, Merkle Tree, %51 Attack

ABSTRACT

BLOCK CHAIN TECHNOLOGY AND %51 ATTACK

The purpose of the study is to show the usage areas of our country and the world for both today and the future by examining in detail the basic and technical aspects of Block Chain technology which is an important agenda with an increasing interest and usage area in the world. In addition to these, it is to evaluate the advantages and disadvantages of Block Chain technology and to examine the strength and security policy which is one of the most important features by technically.

51% Attack, which is the biggest risk of block chain structures with the Bitcoin example, which has been the largest Block Chain application for more than 10 years and working according to the proof of work consensus method, is going to be examined in technical sense. The percentage of 51% risk in the sample block chain applications will be shown statistically.

.

İÇİNDEKİLER

Sayfa No.

BİRİNCİ BÖLÜM

İKİNCİ BÖLÜM

ÜÇÜNCÜ BÖLÜM

DÖRDÜNCÜ BÖLÜM

TABLOLAR LİSTESİ

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

KISALTMALAR

B2B **:** Business to Business (İşletmeler arası)

BKM **:** Bankalararası Kart Merkezi

BTC : Bitcoin

BZLab **:** Blokzincir Araştırma Laboratuvarı

CPU **:** Central Process Unit

FAS **:** Federal Antimonopoly Service

Hash : Özetleme

P2P **:** Peer to Peer (Kişiden kişiye)

PoS : Proof of Stake

PoW : Proof of Work

RPoW **:** Yeniden Kullanılabilir İş İspatı

SHA **:** Secure Hash Algorithm

TC **:** Türkiye Cumhuriyeti

GİRİŞ

21.yüzyıl da yaşamakta olduğumuz Dijital Çağ büyük teknolojik gelişmeleri ve devrimleri de beraberin de getirmiştir. Bu gelişmeler karşısında sahip olduğumuz alışkanlıklarımız da değişmektedir. Gerçek anlamda İnternet ile başlayan bu dijitalleşme dönüşümü, Veri Madenciliği, Mobil Cihazlar, Derin Öğrenme, Yapay Zeka, Robotlar ile devam ederken, karşımıza kimi görüşlere göre internetten sonraki en büyük keşif olarak görülen Blok Zinciri Teknolojisi gelmektedir.

Özellikle karşılıklı güven mekanizmasının teknolojik olarak sağlanması, bilgilerin tek merkezi bir kaynakta toplanması yerine dağıtık yapıda olması gibi gerçekten büyük bir fikir mimarisi üzerine kurulmuş, bütün verilerin yazılım aracılığıyla birbirileriyle konuşan binlerce farklı bilgisayarda eşlenik bir şekilde tutulması gibi büyük avantajları bulunan Blok Zincir giderek artan bir ilgi ve kullanım alanıyla karşımıza çıkmaktadır.

Blok Zincir konusunda, teknoloji dünyasındaki son gelişmelerden biri olması sebebiyle akademik ve bilimsel içeriği olan kaynaklar henüz sınırlı sayıdadırlar. Çalışmamın önemli amaçlarından bir tanesi de ülkemizdeki bu boşluğa katkı sağlayabilmektir.

Ayrıca, yapılan araştırmalarda aynı kavram için kullanılan çok farklı ifadelerin olduğu görülmüştür. Bu farklılıkların yarattığı anlam karmaşalarının önüne geçilmesi hedeflenmiştir. Bu doğrultuda, bazı konulardaki kavramlar anlatılırken hem İngilizce hem de Türkçe kullanılan tüm karşılıklarından bahsedilecektir. Böylece farklı akademik kaynaklarda anlatılan ve birbirinden farklıymış gibi görünen konuların aslında benzer içerikler olduğu, bu çalışmadan faydalanan kişilerce tespit edilebilecektir.

Çalışmadaki bir diğer önemli nokta ise; blok zincir konusunun anlaşılması noktasında iddialı bir şekilde kapsamlı bir içeriğe sahip olmasıdır. Yaptığım akademik incelemelerde blok zincirinin mimarisi, çalışma mekanizması, kullanım alanları, avantaj/dezavantajları ve teknolojinin geleceği ile ilgili bilgileri hep birlikte inceleyen başka bir çalışmayla karşılaşılmamıştır.

Çalışmanın ilk bölümünde Blok zincir yapısı ve çalışma mekanizması detaylı olarak ele alınacaktır. Bir blokta hangi bilgilerin yer aldığı, bloğun nasıl oluştuğu, blok oluşurken karşılaşılan farklı durumlarda nasıl hareket edileceği ve uygulamadaki yazılım güncellemelerinin ne gibi sonuçlar doğuracağı ile ilgili konulara değinilecektir.

Çalışmanın 2. Bölümünde, blok zincir uygulamalarının kullanıldığı çok farklı sektörler hakkında bilgiler verilerek Türkiye ve Dünya'da bu uygulamaların hayata geçirildiği ya da geçirilmesinin planlandığı şirket ve organizasyonlar hakkında güncel örnekler aktarılacaktır. Bu örnekler blok zincirinin uygulandığı alanlar hakkında bilgi vereceği gibi, blok zincir teknolojisine olan ilginin ve desteğin nasıl hızla arttığına dair canlı kanıtlar olacaklardır.

3. bölümde bu teknolojinin avantaj ve dezavantajlarına değinerek, bu teknolojiyi kullanmak isteyen grup ya da kurumların akıllarındaki soru işaretlerine ayna tutulacak ve araştırmalarının devamının ne kadar önemli olduğuna değinilecektir.

Son bölümde ise, her teknolojide olduğu gibi bu teknolojide de güvenliğin önemi ile blok zincir teknolojisinde güvenlik açısından büyük avantaj gibi görünen %51 çoğunluğuna dayanarak işletilen protokollerin, aslında en büyük sorunlardan birine dönüşebileceğinden bahsedilecektir. Bu anlamda küçük yapılarda %51 saldırısının mümkün olabileceği durumlar öngörülerek, gelişmiş yapılarda sorun yaratma olasılığının imkansıza yaklaştığı, en gelişmiş blok zincir uygulaması olan Bitcoin örneği üzerinden verilerle incelenecektir.

BENZER ÇALIŞMALAR

Blok zinciri konusunda (blockchain anahtar kelimesiyle yapılan tarama sonuçlarına göre) Türkiye'de 9 adet Yüksek Lisans Tezi ve 1 adet doktora tezi mevcuttur. Dünyadaki tercihlere benzer şekilde, bu tezlerden çoğunluğu (6 adet) blok zincir teknolojisini ekonomi ve finans alanında incelemiştir [1].

Bitcoin ve Blok zinciri kavramları birlikte akademik olarak değerlendirildiğinde ise, daha bir yıl öncesine kadar sınırlı sayıda yayınların olduğu görülmektedir. Bu sınırlı yayınların çoğunluğunun ise blok zincir teknolojisiyle ilgili olmadığını, Bitcoin ve diğer kripto paraların konu olduğu ekonomi ve finans odaklı yayınlar olduğu görülmektedir. 2019 yılı itibariyle yayın sayısı artsa da hala yeterli seviyede olmadığı gözlenmektedir. 2018 yılında, uluslararası akademik yayınların yer aldığı farklı veri tabanlarında, "blockchain" ve "bitcoin" anahtar kelimeleri kullanılarak yapılan taramalarda, yayınların çoğu "bitcoin" kelimesini içerirken "blokchain" kelimesini içerenlerin azınlıkta olduğu görülmektedir. 2019 yılı itibariyle bu durum değişmeye başlamıştır (Tablo 1)[2].

Tablo 1: Bitcoin ve Blok Zinciri Kelimelerinin Arama Sonuçları

	Anahtar Kelime Taramalarında Çıkan Toplam Yayın/Sonuç Sayısı			
	2018		**2019**	
Veritabanı	**Bitcoin**	**Blockchain**	**Bitcoin**	**Blockchain**
Google Scholar	31700	23000	55400	56200
ScienceDirect	691	339	1272	1290
JStor	180	52	456	217
SpringerLink	1386	991	2828	3101

Türkiye'de, Nisan 2019 itibariyle Tübitak Ulakbim ve YÖK Tez Veritabanlarında "Blok zinciri", "blockchain" ve "bitcoin" anahtar kelimeleriyle yapılan taramalarda, 1 adet doktora tezi, 15 adet yüksek lisans tezi ve toplam 250 adet makale bulunmuştur. Yeni ortaya çıkan her teknolojide olduğu gibi, Blok zinciri teknolojisinin uygun şekilde gelişmesi ve yaygınlaşması ancak akademik çalışmalarla desteklenirse mümkün olacaktır. Bu sebeple, sistematik incelemeler yapan, açık konular ile araştırma ve kullanım alanlarını tartışan akademik çalışmalara ihtiyaç olduğu gözlemlenmektedir [3].

Muhammed Emin Aydın'ın 2018 yılında "Blok zincir Tabanlı Oy Verme Sistemi Önerisi" konulu tezinde, blok zincirinin kamu sektöründeki kullanım alanlarından birine değinmiştir. Merkezi olmayan yapısı nedeniyle, bir online seçim sisteminin sahip olması gereken bazı güvenlik özelliklerini sağladığı görülmüştür. Ancak çevrimiçi yapıda tamamen güvenli bir sistemin oluşması için daha fazla araştırma yapılması kanaatine varılmıştır [4].

Zaman ilerledikçe blok zincirinin farklı kullanım alanları ile ilgili araştırmalar yapılmakta ve makalelere yer verilmektedir. Bunlara örnek olarak, 2018 yılı sonlarında Eğitim Teknolojileri Zirvesi için hazırlanan ve researchgate'te yayınlanan "Yapılandırılmış ve Yapılandırılmamış Öğrenme Süreçlerinde Blok Zinciri Teknolojisi" ile dergi park'ta 2019 yılında yayınlanan "Spor Sektöründe Blok Zinciri Uygulamaları" makalelerini örnek olarak gösterebiliriz.

"Yapılandırılmış ve Yapılandırılmamış Öğrenme Süreçlerinde Blok Zinciri Teknolojisi" makalesinde, yapılandırılmış öğrenme (yani kayıt altına alınan öğrenmeler) ve yapılandırılmamış öğrenmeleri (yani kayıt altına alınmayan, öğrenmenin bireysel düzeyde kaldığı öğrenmeleri) bütünsel bir bakış açısı ile ele alan, yaşam boyu öğrenme deneyimini kayıt altına alabilecek bir mekanizma ihtiyacını blok zinciri teknolojisinin karşılayıp karşılamayacağı sorgulanmıştır. Altyapı gereksinimlerinin bu teknoloji ile karşılanabildiği fakat küresel politikalarla desteklenmesi gerektiği sonucuna varılmıştır [5].

"Spor Sektöründe Blok Zinciri Uygulamaları" makalesi, blok zincir teknolojisi ile spor sektörüne yenilik kazandırarak maliyetlerin azaltılmasını, arşivlemeyi, ileriye yönelik analizlerin yapılmasını ve veri güvenliğini üst seviyeye çıkarmayı hedeflemektedir. Bu teknolojinin spor sektörü için uygun olduğu sonucuna varılmaktadır [6].

Genel olarak incelediğim çalışmalar, blok zincirinin farklı kullanım alanlarına olan uygunluğu ile ilgili yapılan araştırmaları içermektedir. Bu çalışmada ise bir kullanım alanına yoğunlaşmak yerine farklı kullanım alanlarına değinilerek blok zincir teknolojisi kavramının gerçekten anlaşılması ve hem avantaj hem de dezavantaj gibi görünen %51 durumunun, gelişmiş uygulama yapılarında artık bir sorun teşkil etmeyeceği rakamlarla anlatılacaktır.

BİRİNCİ BÖLÜM

1. BLOK ZİNCİRİ TEKNOLOJİSİ

1.1. Tarihçesi

Blok zinciri teknolojisi temelindeki fikir, 1991 yılında bilim insanları W. Scott Stornetta ve Stuart Haber tarafından, hesaplama yöntemi olarak pratik bir çözüm ile dijital belgelerin zaman damgası ile değiştirilemez veya geçmişe yönelik düzenlenememesini sağlayacak şekilde ortaya konmuştur.

Sistem ilerleyen aşamalarında, zaman damgası olan belgelerin saklanması için kriptolanmış güvenli bir blok zinciri kullanımına gitmiştir.1992 yılında birden fazla belgenin bir blok halinde toplanmasını sağlarken, Merkle ağaçları yapısını dizayna dahil etmiş ve ciddi anlamda verimliliğini arttırmıştır. Fakat sonralarında bu teknoloji kullanılmamış ve 2004 yılında patent sona ermiştir.

2004 yılı sonlarında kriptografi aktivisti ve bilgisayar bilimcisi Hal Finney Yeniden Kullanılabilir İş İspatı (RPoW) isimli değiştirilemeyen ve tamamen özgün bir Hashcash alt yapısı olan, iş ispatı tokenı alarak çalışmaya başlayan ve karşılığında kişiden kişiye aktarılabilen bir RSA imzalı token oluşturan bir sistem tanıtmıştır. Bu sistemin tokenlarının sahiplikleri, dünyanın herhangi bir yerindeki kullanıcıların gerçek zamanlı olarak, verilerin bütünlüğünü ve doğruluklarını teyit etmesini sağlayacak şekilde dizayn edilmiş, güvenli bir sunucuda bulundurmak şartıyla, çifte harcama problemini çözmüştür. RPoW sistemi dünya kripto para tarihinde başlangıç bir prototip ve çok önemli bir kilometre taşı olarak değerlendirilmektedir.

31 Ekim 2008 yılında Satoshi Nakamoto adıyla bilinen anonim bir mucit Bitcoin ile ilgili bir makale kaleme almış ve 2009 yılında ilk Bitcoin yazılımını geliştirerek Bitcoin ekosistemini kurmuştur. Blok zinciri esas ilgiyi, Bitcoin geliştirildiğinde elde etmiştir. 2010 yılının ortalarına gelene kadar bu ekosistemin gelişmesi direkt olarak bu anonim mucit tarafından desteklenmiş sonrasında bu mucit ortadan kaybolmuştur. 2019 yılı nisan ayı itibariyle sadece Bitcoin'in piyasa değeri 90 milyar dolara yaklaşırken bu anonim mucit esrarengiz sırrını halen daha korumaktadır.

The Economist, New York Times ve Wired gibi birçok dünyaca ünlü haber dergisinde Bitcoin'in bu esrarengiz öyküsü ve anonim mucit hakkında birçok kez yayınlar yapılmıştır. Tüm bu teknolojik yenilikler, dünyadaki para yaratımı ve kullanımı konusunu oldukça ciddi etkiler yaratmaktadır. Bu gelişmeler yaşanırken, Satoshi Nakamoto olduğunu iddia eden bilişim alanında lisans ve doktora derecelerine sahip Craig Steven Right isimli eski bir akademisyen ortaya çıkmıştır.

Bitcoin bu anonim icadının sırlı ve fantastik bir hikâye olmasının yanında özellikle 2017 yılı sonlarında tarihi bir rekor değer olan 20.000$'a çıkarak oluşturmuş olduğu bu ekonomik değer ve finansal fonksiyonları itibariyle büyük bir ilgi ve merak konusu olmuştur. Bu başarılı gelişmelerin akabinde, Bitcoin'in temelin de olan blok zinciri teknolojisi ile de başta finans aktörleri olmak üzere ciddi anlamda ilgi artmış ve bu teknoloji mimarisi üzerine inşa edilen birçok farklı alanda yeni ürün ve hizmetler icat edilmiştir.

Bugün gelinen noktada, devletler birçok kurumlarında, özellikle merkez bankaları, özel büyük finans kuruluşları ve teknoloji şirketleri blok zincir teknolojisine yatırım yapmakta ve ciddi projeler planlamaktadırlar.

1.2. Blok Zinciri Tanımı

Blok zinciri teknolojisi, internetin icadından sonra gelen yıkıcı ve devrim niteliğindeki yeniliklerden biri olarak kabul edilmektedir. Blok zincir teknolojisi günden güne iş dünyasında önemli bir yer edinmeye devam etmektedir. Birçok blok zinciri uygulaması, dijital verileri kriptografi kullanımı yoluyla kaydeden ve koruyan dağıtılmış bir defter olarak işlev görür. Bu nedenle dağıtık hesap defteri (distributed ledger) olarak nitelendirilebilecek olan blok zinciri; temelde birden fazla tarafın kendi aralarında önden mutabakata vararak hataları sıfıra indirip, işlemi farklı veri tabanları üzerinde kaydederek değiştirilememesini garanti altına aldıkları bir veri saklama yaklaşımı özelliğini taşır. Bir değer taşıyan her işlem, matematik ve kriptoloji aracılığıyla dağıtık ve bir otoritenin yönetmediği bağımsız veri zincirleridir.

Kriptografi kullanımı ile kullanıcılarına çoğunlukla bir merkez olmaksızın, aynı anda birden fazla noktadan kontrol edilebilen ve olguların durumu hakkında güvenilir fikir birlikleri sağlamayı garanti eden blok zinciri teknolojisi sayesinde;

veri, yetkilendirmeler ölçüsünde paydaşlar ile paylaşılmakta olup işlemlerin tutarlılığı ve doğruluğu sağlanmaktadır. Diğer bir deyişle; bir işlemin gerçekleşmesi ekosistem içerisinde yetkisi olan paydaşların onayına tabi olup, işlem bilgisi merkezi olmayan bir yapıda tüm paydaşlarda kayıt altına alınmakta ve sistem içerisinde gerçekleştirilen her işlem bir önceki işleme bağlı tutulmaktadır.

Blok zinciri teknolojisi, taraflar arasındaki güven sorununu ve sistemlerin pahalı güvenlik ihtiyacını ortadan kaldırarak, verimliliğin artmasını sağlar.

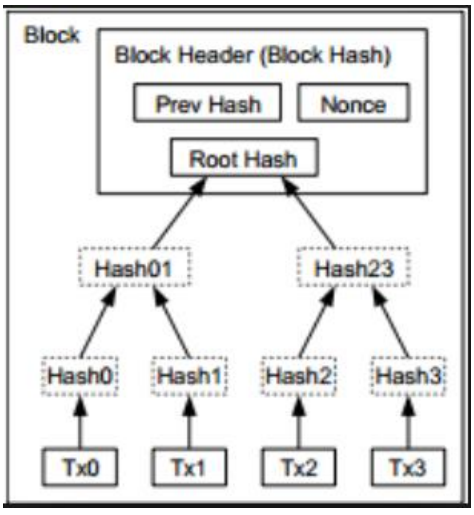
1.3. Blok Zincir Yapısı

Bir blok zinciri sistemi, çalışma mekanizması ve mutabakata varmak için hangi yöntemlerin kullanılacağı konusunda düzenlenebilmektedir. Bu sistem küçük gruplar arasında ya da çok fazla üyesi olan yapılarda da kullanılabilmektedir. Bu yapıya en güzel örneklerden biri olarak milyonlarca üyesi olan Bitcoin verilebilir.

1.3.1. Blok

Blok zincirini, onaylanmış ve güvenli bir şekilde birbirine bağlanmış bilgi blokları oluşturmaktadır.

Blok zincirindeki her bir blok, başlık ve gövde olarak 2 ana bölümden oluşmaktadır. Blok başlığı içerisinde; Blok Versiyon Numarası, Önceki Blok Özet Değeri, Zaman Damgası, Zorluk Derecesi, Nonce ve Merkle Kök Özeti bulunmaktadır. Blok gövdesinde; Blok Özet Değeri ve Blok işlemleri yer almaktadır.



Şekil 1: Blok Başlığı ve Gövdesi

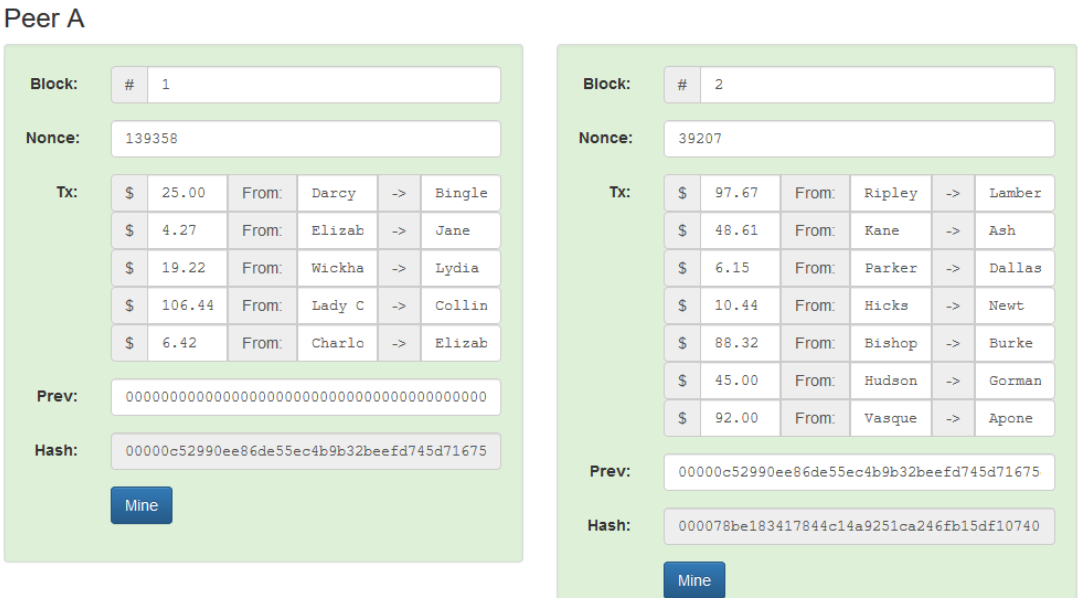
1.3.2. İşlem/Hesap Hareketi

Bilgi bloklarının içerisinde tutulan veriler, hesap defter girişini ya da hesap hareket kayıtlarını (işlemleri) temsil etmektedir. Her hesap hareketinin dijital olarak imzalanarak gerçekliğinin korunması sağlanmaktadır. Böylece kayıt üzerinde kimse değişiklik yapamaz ve verinin güvenilir olduğu varsayılır.

Blok zincir ağında terminaller arasındaki varlık transferlerinin kayıtlarına işlem denir. Bu işlemler blokların gövdesinde saklanır.

Temel olarak bir işlem; Toplam Miktar, Girdi Listesi, Çıktı Listesi, Özet Değeri bilgilerinden meydana gelir.

- Toplam miktar, transfer edilecek dijital varlıkların toplam miktarı bilgisini tutar.
- Girdi listesi bilgi olarak transfer edilecek varlıkların listesini, miktarlarını ve gönderici hesap adresini tutar.
- Çıktı listesi bilgi olarak transfer edilecek varlıkların miktarlarını, alıcı adresini ve yeni sahiplerini tutar.
- Özet Değer, işlem içeriğinin hesaplanmış kriptografik özet değeridir. Özet değer kullanılarak, saklı anahtar ile işlemler imzalanır ve göndericinin açık anahtarı kullanılarak doğrulanır.



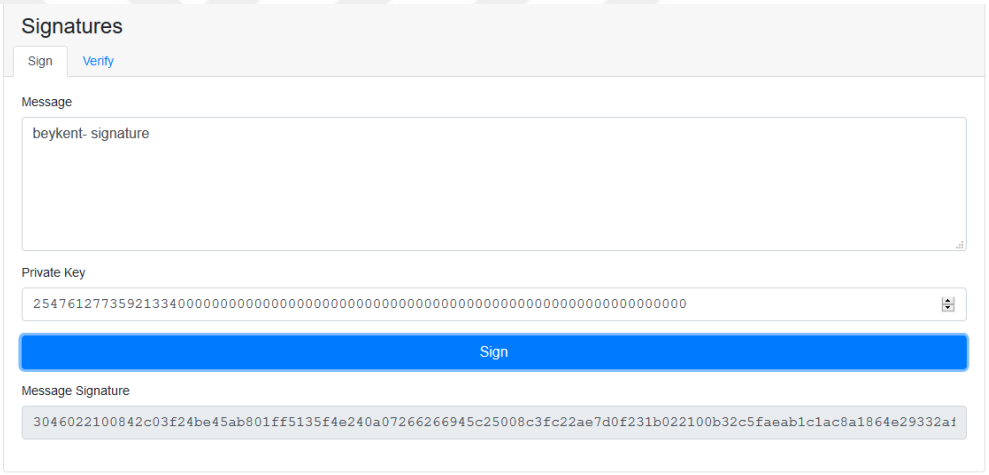
Şekil 2: Bloklardaki İşlemler

1.3.3. Hesap Adresleri

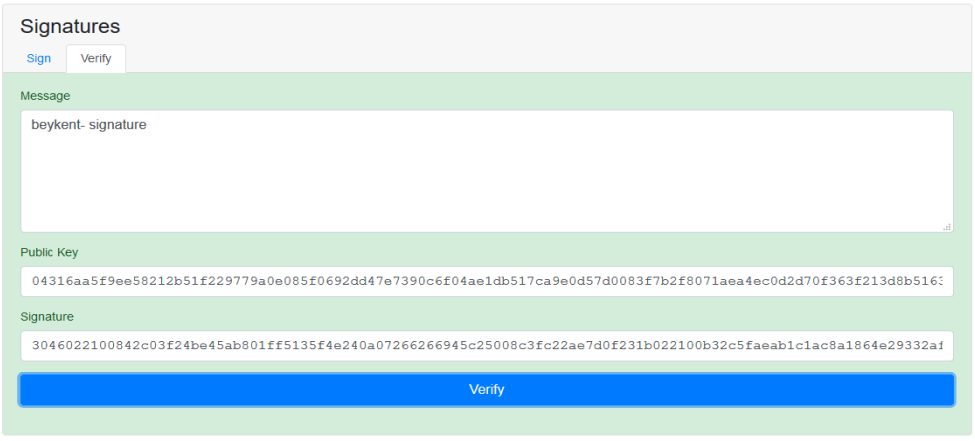
Blok zincirinde yer alan bir işlemde, gönderici ve alıcının hesap adresleri yer almaktadır.

Sisteme dahil olan her yeni kullanıcı için yeni bir adres üretilir. Bu adresler blok zincir sisteminde kullanıcıların kimlikleri niteliğindedir. Kullanıcının açık anahtarları kullanılarak hesap adresleri oluşturulur.

Bu adreslerde, dijital bir varlığın sahiplik bilgisi tutulur. Bir kullanıcının sahip olduğu dijital varlığı kullanarak işlem yapabilmesi için, o hesaba ait saklı anahtarının olması gerekir. Çünkü işlemlerin, kullanıcının saklı anahtarı ile imzalanmış olması gerekmektedir. Yaratılan bu işlemin doğrulanmasında hesap adresinden oluşturulan açık anahtar kullanılmaktadır.



Şekil 3: İşlemlerin İmzalanması



Şekil 4: Doğrulama

1.3.4. Kayıt Defteri/Hesap Defteri

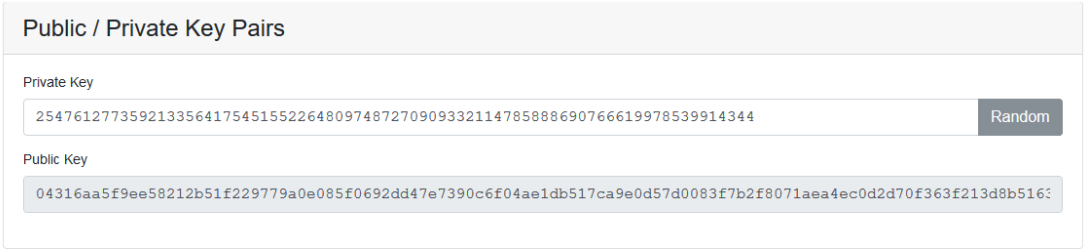
Veriler, her terminalde yer alan herkese açık hesap defterlerinde tutulmaktadır. Bu hesap defterleri içerisinde blok zincir ağında oluşturulan ve doğrulanan işlemler yer almaktadır.

Sistem güvenliği, dijital hesap defterlerinin bir altyapı ya da ağ üzerinde dağıtılmasıyla sağlanmaktadır. Altyapıdaki bu ek katmanlar, bir hesap hareketinin durumu ile ilgili istenilen her an mutabakat sağlanabilmesi amacına hizmet etmektedir. Her katmanda, gerçekliği korunan hesap defterlerinin kopyası yer almaktadır.

Sisteme yeni bir hesap hareketi geldiğinde ya da mevcut bir işlemde değişiklik yapıldığında, altyapıda yer alan tüm kayıtlarda belirli bir algoritma çalışarak bu yeni işlemin doğruluğunu kontrol etmektedir. Hesap defterleri kopyalarının çoğunluğu bu kaydın doğruluğunu onaylarsa, yeni bir blok sisteme dahil edilmektedir. Eğer sistemdeki kopyaların çoğunluğu yeni işlemi reddederse, bu hesap hareketi sistem üzerine kaydedilemeyecektir. Bu dağıtık sistem sayesinde, Blok zinciri merkezi bir yapı ile kontrol edilmeden etkili bir şekilde çalışmaktadır.

1.3.5. Cüzdan

Kişilerin saklı anahtarları çok önemlidir. Dijital varlıkların güvenliği için bu anahtarın çok sağlam ve güvenli bir şekilde saklanması gerekmektedir. Cüzdan, bu anahtarların saklandığı uygulamalardır. Cüzdanlar, ek olarak kullanıcıya ait dijital varlık bilgilerini ve açık anahtarı da gösterir. Uygulama, yerel diskler üzerinde ya da bulut içerisinde yer alır.



Şekil 5: Saklı Anahtar'dan Açık Anahtar Üretilmesi

1.3.6. Kriptografik Hash Fonksiyonu

Kriptografi, kısaca bir verinin şifrelenmesi anlamına gelmektedir. Bu şifreleme işlemi, karmaşık olan birçok gelişmiş matematiksel tekniği kullanan derin bir akademik araştırma alanını kapsamaktadır. Burada bilinmesi gereken ilk şifreleme tekniği temel bir şifreleme olan hash işlevidir. Hash birçok kaynak ve uygulamada İngilizce olarak kullanılsa da Türkçe karşılığı itibariyle bilişim dünyasında özetleme olarak ifade edilmektedir. MD-5, SHA-1, SHA-2, SHA-3, BLAKE gibi farklı özetleme algoritmaları bulunmaktadır. Bir hash, üç temel özelliğe sahip matematiksel yöntemdir. Bunlar;

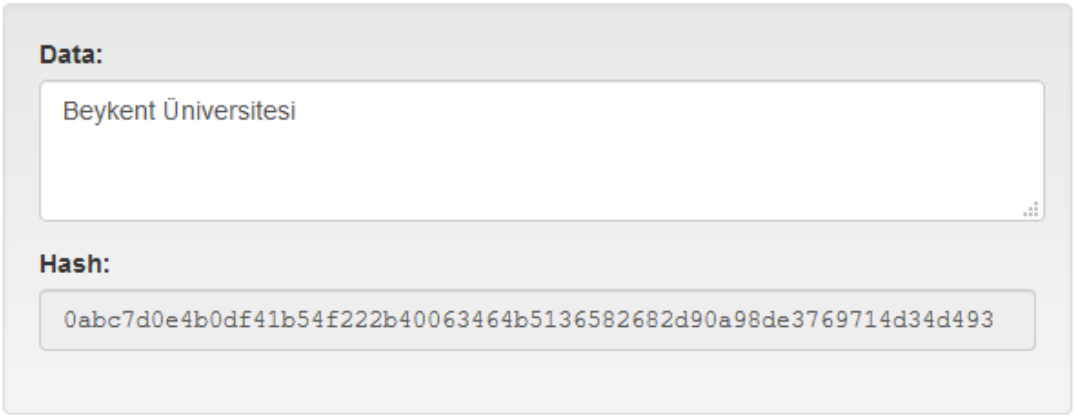
- Girdi verileri herhangi bir boyutta herhangi bir dize olabilir.
- Sabit boyutta bir çıktı üretmektedir. Örneğin; 64, 128, 256 bit çıktı boyutu.
- Verimli olarak hesaplanabilmektedir. Sezgisel olarak, belirli bir girdi dizgesi için, hash çıktısının makul bir süre içerisinde ne olduğunu bulabileceğiniz anlamına gelmektedir.

Bir kriptografik işlem özet fonksiyonun da $H : \{0,1\} * \rightarrow \{0,1\}n$ herhangi bir istenilen uzunluktaki mesaj olan M için n bitlik bir sabit uzunlukta hash değerini hesaplayan bir fonksiyondur. Kriptografik hash fonksiyonu, dijital imza şemaları, kimlik doğrulama kodları, parola işlem özet fonksiyonları ve içerik adresli depolama da dahil olmak üzere pek çok uygulamada kullanılan temel bir kriptografi yöntemidir. Bu uygulamaların birçoğunun güvenliği veya düzgün işleyişi, kırılmasının (çarpışmaların bulunmasının) pratik olarak mümkün olmadığı varsayımına dayanmaktadır. Güvenli Hash Algoritması (SHA-Secure Hash Algorithm), bir dizi kriptografik hash işlevinden oluşmaktadır. Özetle kriptografik hash, bir metin veya veri dosyası için bir imza gibidir.

SHA-2 Hash Algoritmasının, 6 farklı fonksiyonundan biri olan ve yüksek güvenliğe sahip olanı SHA-256 algoritmasıdır. Bu algoritmada farklı boyut ve büyüklükteki yazı, sayı veya değişik formattaki bilgisayar dosyası verileri, tek yönlü olmak üzere standart büyüklükte, 256 bit (32 byte – 64 hexadecimal) boyutunda özetleme değerlerine dönüştürülmektedir. Aynı veri için hesaplanan SHA-256 değeri

her zaman aynı sonucu vermektedir ve sadece veri de değişikliği olması durumunda sonuç özetleme değeri değişmektedir.

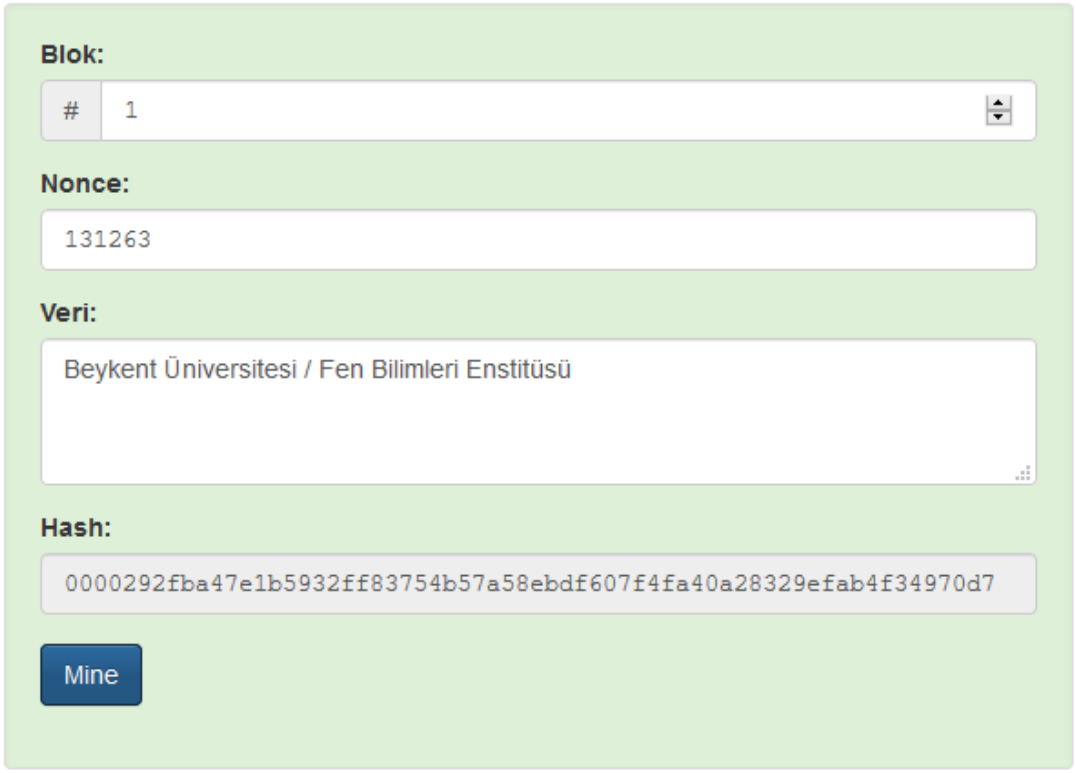
SHA-256 özetleme algoritmasının tek yönlü olması sebebiyle, geriye dönük olarak özetleme değerlerine bakılarak girdi olarak belirlenen verinin ne olduğu tespit edilemez. Veri sadece tahmin edilebilir ve bu tahmin oranı da 2^{256} da 1 olduğu için, mevcut bilgisayar güçleriyle bunun hesaplanması imkansız kabul edilmektedir.



Şekil 6: Örnek SHA-256 Özetleme Fonksiyonu

Blok zincir teknolojilerinde özetleme fonksiyonları çok sıklıkla kullanılmakta olup özellikle Bitcoin işlemlerindeki PoW hesaplamalarında ve adres oluşturma adımlarında SHA-256 özetleme algoritmasından faydalanılmaktadır.

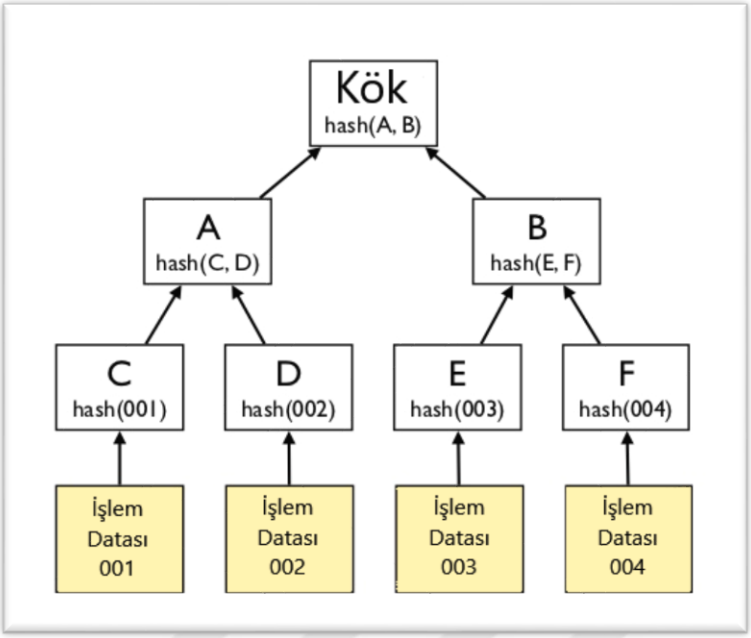
Bitcoin blok zincir yapısındaki blokların üretilmesinde, blok içerisindeki verinin SHA-256 algoritmasına bağlı olarak özetleme değeri hesaplanırken, ağdaki hesaplanma gücüne göre değişen zorluk derecesini gösteren başında 0 ile başlama koşulu getirilmiştir. Ayrıca özetleme değeri oluşturulurken, rastgele bir sayı olan Nonce –(Number Used Once) diye ifade edilen bir sayı parametresi de algoritmaya eklenmektedir.



Şekil 7: Örnek bir Bloğa ait oluşturulan SHA-256 Özetleme Fonksiyonu

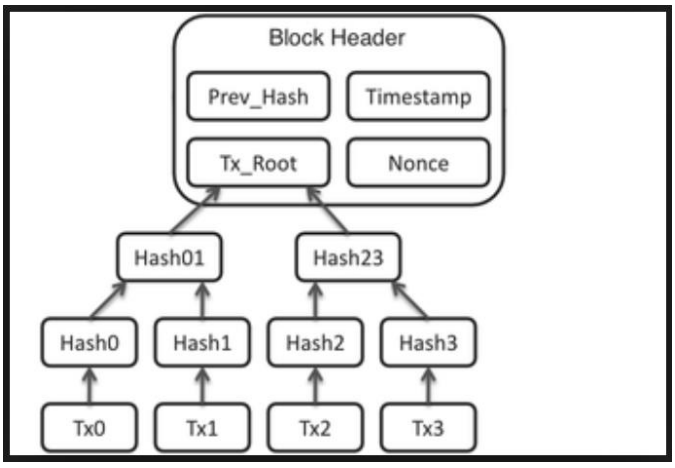
1.3.7. Merkle Tree (Ağacı)

İngilizce ifadesiyle Merkle Tree, Merkle Root veya Root Hash, Türkçe ifadesiyle ise Merkle Ağacı, Merkle Kökü veya Kök Özet tanımları aynı anlamda kullanılmaktadır. Genel anlamda, Merkle Ağacı büyük veri yığınlarının bir araya getirilip özet olarak gösterilmesi ve bunun güvenli bir şekilde doğruluğunun sağlanabilmesidir. Çalışma prensibi açısından bir ağacın yapısına benzemektedir. Ağacın yaprakları veri bloklarını temsil etmekte, bu veri blokları özetleme fonksiyonundan geçirilerek özet değerleri oluşmakta ve bunlar da ağacın dallarını temsil etmektedir. Oluşan özet değerlerde tekrar özetleme fonksiyonlarından geçirilerek yeni özet değerler elde edilir. Bu döngü aynı şekilde devam ederek en son kök özet değerine ulaşılır. Bu da ağacın köküne ulaşmak olarak yorumlanmaktadır. Anlatılan bu yapı Şekil 8'de gösterilmiştir.



Şekil 8: Örnek Merkle Ağacı Yapısı

Merkle kökü ile blok zincirler arasında oldukça sıkı bir ilişki bulunmaktadır. Blok başlığı içerisindeki Merkle Kök Özeti, blok gövdesi içerisindeki işlemlere ait kök özet değerdir. Şekil 8'de bu ilişki grafik olarak gösterilmiştir.



Şekil 9: Örnek Merkle Kökü ve Blok İşlemleri ilişkisi

1.4. Blok Zincir Çeşitleri

Üç farklı blok zincir vardır.

1.4.1. Genel Blok Zincirleri

Bir genel blok zincirini, dünyadaki herhangi bir kişi okuyabilmekte, işlem yapabilmekte, yapılan işlemin geçerli olması durumunda sonuçlarını görebilmekte ve uzlaşma sürecine (mevcut durumun ne olduğu ve hangi blokların zincire ekleneceğinin belirlenmesi sürecine) katılabilmektedir. Kimseye erişim kısıtlaması yapılmamaktadır.

En gelişmiş ve en çok bilinen genel blok zincirlerine örnek olarak Bitcoin ve Ethereum verilebilir.

1.4.2. Özel Blok Zincirleri

Özel blok zincirinde ağa katılacak ve onay işlemi yapacak kişilere izin verilmesi gereklidir. Ağ yöneticileri tarafından davet edilmedikçe katılım sağlanamayacaktır.

Hassas verileri, herkese açık olan bir yapıda riskle karşı karşıya bırakmamaktadırlar. Herhangi bir muhasebe mevzuat sistemine ve resmi kayıt işleme prosedürlerine bağlı olmadan kendi içerisinde kayıt tutmaya çalışmaktadırlar.

1.4.3. Konsorsiyum Blok Zincirleri

Bir konsorsiyum blok zincirinde ağa katılacak kişilere izin verilmesi gereklidir. Fakat bunu, özel blok zincirindeki gibi tek bir kuruluş kontrol etmez. Ortak yapıya dahil olan her şirket, ağ üzerinde bir düğüm işletebilmektedir.

Konsorsiyum blok zincirinde, zincirin yöneticileri tarafından kullanıcıların okuma hakları kısıtlanmaktadır ve az sayıda güvenilir düğümlerin bir konsorsiyum protokolü işletmesine izin vermektedir.

1.5. Mutabakat Yöntemleri

İngilizce ifadesiyle “Consensus Algorithms” Türkçe ifadesiyle “Mutabakat Yöntemleri”, “Mutabakat Algoritmaları”, “Uzlaşı Algoritmaları” tanımları

kullanılmaktadırlar. Blok zincir sistemlerin dağıtık yapıda olmaları, merkezi bir otoritenin olmaması ve bir tek yönetici anlayışı olmaması sebebiyle ekosistem içerisinde bulunan katılımcı eşlerin mutabakatı, blok zincir sisteminin güvenli ve sağlıklı çalışabilmesi için çok önemlidir. Blok zincir yapılarındaki ilk mutabakat kavramı şu an için en büyük blok zincir ekosistemine sahip Bitcoin'in anonim mucidi Satoshi Nakamoto tarafından uygulanan "İş İspatı Mutabakatı" (Proof of Work – PoW) dır.

Bitcoin blok zincir yapısında dağıtık olarak yerleşim gösteren birbirinden çok farklı terminallerin, yapılacak işlemlerin geçerliliği ve yeni üretilecek blokların onayı konularında mutabakat yöntemleri kullanılarak anlaşma sağlanmaktadır. Zamanla gelişen blok zincir yapılarıyla birlikte PoW dışında farklı mutabakat yöntemleri yaratılmıştır.

1.5.1. İş İspatı (PoW)

İş İspatı mutabakat yöntemi blok zincir teknolojilerinden çok daha önce 1993 yılın da Cynthia Dwork and Moni Naor tarafından ağdaki spam emailleri gönderilmesini engellemek amacıyla keşfedilmiştir. Blok zincir dünyasında ilk olarak 2009 yılında Bitcoin ekosisteminde kullanılmıştır.

PoW mutabakat algoritması, blok zincir ekosistemlerinde, talep edilen transfer işlemlerini doğrulama ve yeni üretilen bloğun onayının alınıp zincire ekleme yapılması aşamalarında kullanılmaktadır. Özetle bu algoritma; blok üreticisi terminalin, yeni blok üretimi için gerekli olan ve harcamış olduğu bilgisayar hesaplama gücünü, diğer üretici terminallere onaylatması olarak yorumlanmaktadır.

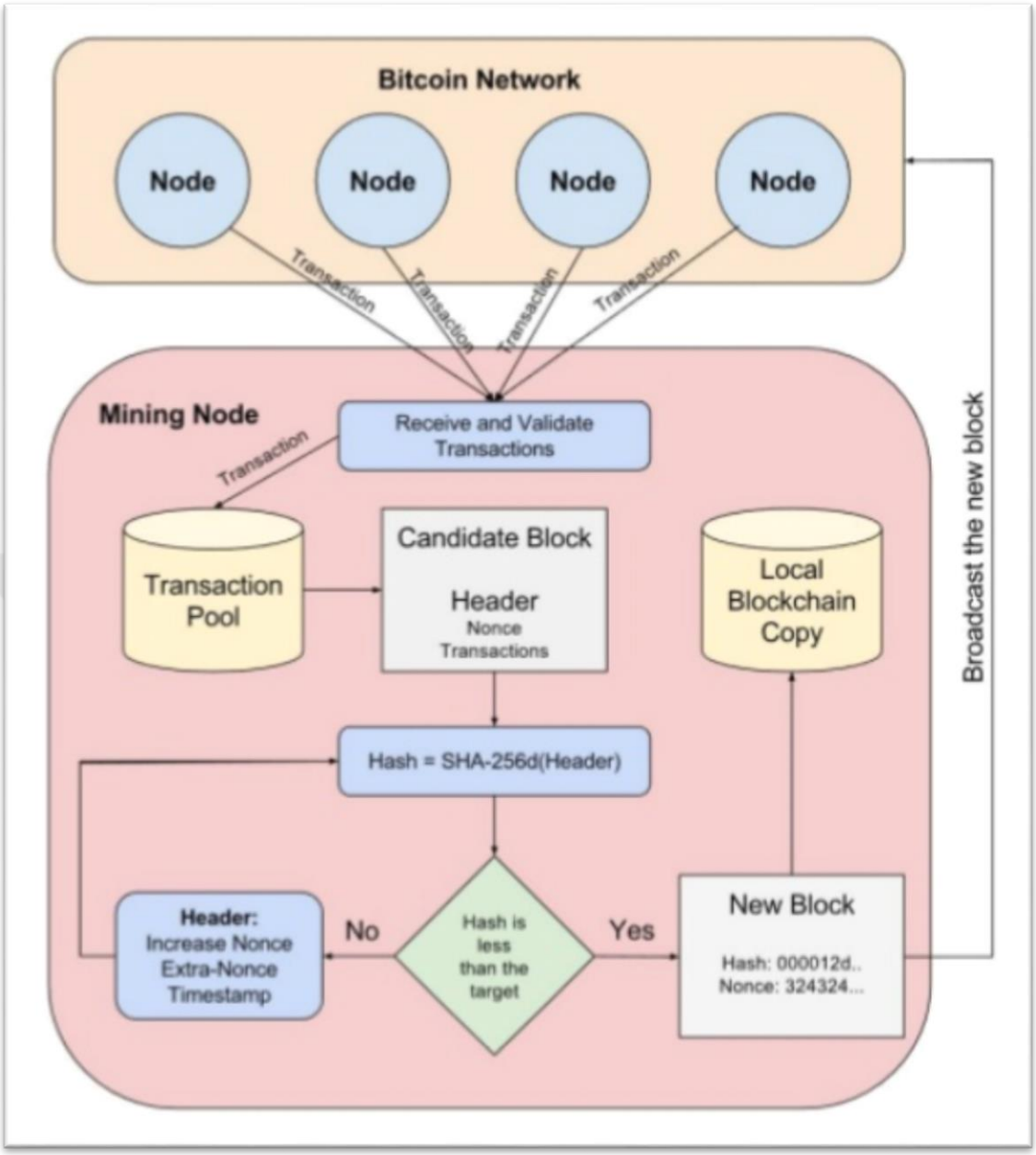
Blok üretilmesi kavramı teorik olarak, asimetrik özellikte olan bir matematik probleminin çözülmesi olarak düşünülebilir. Bu matematik probleminin çözülmesi yüksek seviyede zor olmalı ancak doğruluğunun kontrolü kolay ve hızlı olabilmelidir. Bu üretim işi ayrıca CPU Maliyet Fonksiyonu (CPU cost function), İstemci Problemi (Client Puzzle), Bilgisayar Problemi (Computational Puzzle) veya CPU Değeri Hesaplama Fonksiyonu (CPU Pricing Function) olarak da bilinmektedir.

Ekosistemdeki üretici terminaller matematik problemini ilk çözen olmak için birbirleriyle yarışa başlarlar. Terminaller çok sayıda denemeler yaparak cevabı elde

edebileceklerdir ve buna “Brute Force” da denilmektedir. Problemi çözen ilk terminal, tüm blok zincir ekosistemindeki terminallere aynı anda sonucu duyurur. Diğer üretici terminallerde çözümü onaylayacaklardır. Üretici terminal de, belirli protokoller çerçevesinde sistemin verdiği ödülü elde eder.

Blok üretilmesi kavramı teknik olarak ise; belirli bir zorluk derecesi parametresinde ve belli bir zaman dilimi içerisinde, hedefledikleri işlemler için belirli bir Nonce(rastgele bir sayı) blok değerleri aralığında olacak Nonce değerini bulabilmek için Özetleme Fonksiyonu işlemi gerçekleştirilmesidir. Zorluk derecesi parametresi blok üretme işinin önemli bir parçasıdır. Ekosisteme daha fazla hesaplama gücü eklendikçe zorluk derecesi yükselmekte böylece bir bloğun üretilmesi için yapılacak hesaplama sayısı da artmaktadır. Dolayısıyla, bir blok üretim maliyeti de yükselecektir. Aynı zamanda bu durum, üretici terminalleri de sistemlerini efektif bir şekilde geliştirmeleri için teşvik etmektedir. Zorluk derecesi parametresi 14 günde bir güncellenmekte ve her 10 dakikada bir yeni blok üretilmektedir.

PoW mutabakat yöntemi blok zincirleri için yüksek işlemci gücüne sahip pahalı donanımlara ve bu donanımları çalıştıracak çok fazla enerjiye ihtiyaç duymasına rağmen en çok tercih edilen algoritmadır. Aşağıda PoW algoritması ile çalışan en büyük blok zincir olan Bitcoin’in blok üretim iş akış şeması örnek olarak gösterilmiştir.



Şekil 10: Pow algoritması ile çalışan Bitcoin Blok Üretim İş Akış Şeması

1.5.2. Hisse İspatı (PoS)

PoS mutabakat yöntemi, 2011 yılında bitcointalk forumunda en yaygın algoritma olan PoW'un sorunlarını çözmek amacıyla gündeme gelmiştir. 2012 yılında ilk defa Peercoin isimli dijital para bu metodu kullanmıştır.

PoS algoritmasında yeni oluşacak bloğun onaylayıcısı olacak terminali belirlemek için "hisse yaşı", "rastlantısallık" ve terminalin sahip olduğu "hisse miktarı" gibi faktörlerin kombinasyonlarından oluşan rastgele bir seçim süreci

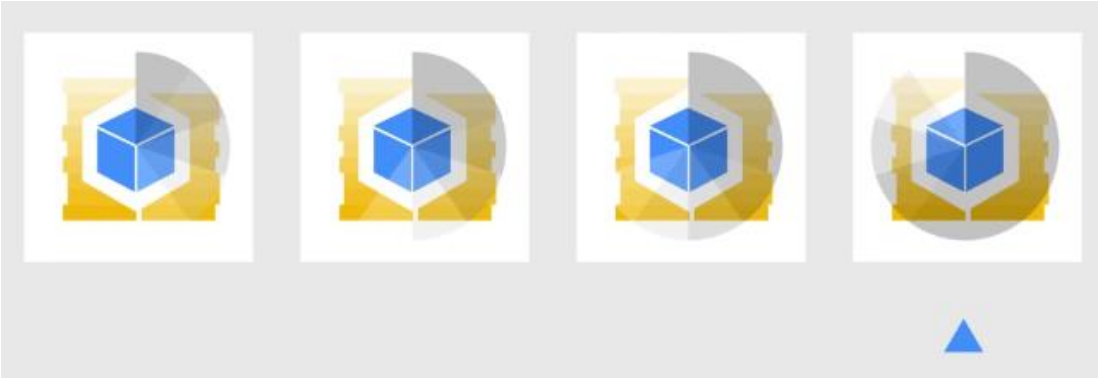
kullanılmaktadır. PoW yapılarında blok kazılması kavramı kullanılırken PoS yapılarında blok oluşturulması kavramı tercih edilmektedir. PoS algoritmasıyla çalışan blok zincir sistemleri genellikle daha önceden oluşturulan coinleri satarlar. Blok zincir sistemlerine bakıldığında önce PoS algoritmasıyla başlayıp sonrasında PoS algoritmasına dönmüş birçok yapı mevcuttur. PoW sistemlerinde blok üreticisi terminalleri ödüllendirmek amacıyla yeni kripto paralar üretilirken PoS'ta işlemlerden kesilen komisyon ücretleri ödül olarak verilmektedir.

Blok oluşturma sürecinde bulunmak isteyen terminallerin belirli sayıda coini kendi hisseleri olarak ekosistemde bloke olarak tutmaları gerekmektedir. Ortaya koyulan hissenin büyüklüğü o terminalin bloğun oluşturulmasının onayında seçilme şansını daha yüksek olarak belirlemektedir. Hisse oranı en yüksek terminalin sürekli onaylayıcı olarak seçilmesini engellemek için seçim sürecine farklı metotlar da dahil edilmiştir. "Rastgele Blok Seçimi" ve "Coin Yaşı Seçimi" en sık kullanılan metotlardan başlıca olanlarıdır.

Rastgele blok seçimi metodunda, onaylayıcılar en düşük hash değeri ve en yüksek hisse değerinin birleşimine sahip terminaller arasından seçilmektedir. Koyulan hisse miktarları herkes tarafından görülebildiğinden bir sonraki onaylayıcı (forger) diğer terminaller tarafından tahmin edilebilmektedir.

Şekil 11: Rastgele Blok Seçim Metodu

Coin yaşına göre seçim metodunda ise, terminallerin ne kadar süredir tokenlarını hisse olarak tuttuklarına göre seçerler. Coin yaşı, coinlerin hisse olarak tutulmaya başladığı gün sayısı ile hisse olarak ayrılan coin sayısının çarpımı ile hesaplanır.



Şekil 12: Coin Yaşına Göre Seçim Metodu

Bir terminal yeni bir blok oluşturduğunda, coin yaşları sıfırlanmakta ve tekrar bir blok oluşturabilmeleri için belirli süre bekleme pozisyonuna alınmaktadırlar. Bu sistem daha çok varlıklı terminallerin blok zincirinde blok oluşturmasını domine etmelerinin önüne geçer.

Blok oluşturulması için, PoS algoritmasındaki yöntemlerden biriyle bir terminal seçildiğinde, seçilen terminal bloğun kapsamındaki işlemlerin doğruluğunu kontrol edip, bloğu imzalayarak ve zincire eklemektedir. Ödül olarak, ilgili bloktaki işlemlerle ilgili masraflar terminale verilir. Bir terminalin blok yapıcısı durumundan ayrılmak isterse, başta koymuş olduğu varlığı ve kazanmış olduğu ödüller belirli biz zaman geçtikten sonra serbest bırakılmaktadır. Bunun nedeni ise, blok zincirine sahte blokların eklenip eklenmediğini anlayabilmek için ekosisteme yeterli süreyi sağlamaktır.

Güvenlik açısından değerlendirildiğinde, ilk başta koyulan varlık, onaylayıcı terminalin kendi sahte işlemleri yaratıp onaylamasını engellemek için finansal bir tedbir olmaktadır. Eğer ekosistem sahte işlemleri fark ederse onaylayıcı terminal varlığının bir kısmını ve gelecekte yeni blok oluşturma hakkını kaybetmiş olacaktır. Bu sebepten varlık ödülden daha fazla olduğu durumlarda, onaylayıcı terminal sahte bir işleme girişmesi durumunda, kazandığından daha fazla varlığı kaybedecektir. Ekosistemi etkin bir şekilde kontrol etmek ve sahte işlemleri onaylamak için terminalin ağdaki çoğunluk hisseyi elinde bulundurması gerekmektedir. Bu durum %51 saldırısı olarak da bilinir. Kripto paranın değerine bağlı olarak, ağın kontrolünü sağlamak dolaşımda olan arzın %51'ine sahip olmayı gerektirdiğinden uygulanması çok zordur.

PoS algoritmasının başlıca avantajları olarak güvenlik ve verimli enerji tüketimi ifade edilebilir. Basit ve düşük maliyetli olduğu için daha çok kullanıcının terminal olması teşvik edilmektedir. Bunların yanında, sistem sürecinin rastgele olmasın, yeni blok üretimleri için havuz yapılarının ihtiyacını ortadan kaldırmaktadır. Böylece ekosistemi merkezi olmayan daha dağınık bir yapıya dönüştürmektedir. Bu yapıda ödül coin oluşumuna da daha az gereksinim duyulduğu için, coin fiyatlarının daha dengeli olması gibi bir etkisi de bulunmaktadır.

1.6. Çakışma Durumu

Mutabakat yöntemlerine rağmen, aynı anda farklı terminaller tarafından farklı bloklar yaratılabilmektedir. Bu tip durumlar oluştuğu zaman, karışıklığın çok hızlı şekilde çözülmesi gerekmektedir. Çünkü terminallerin oluşturduğu bloklardaki işlem listeleri farklı olacaktır. Her iki terminal de ekledikleri blokları kayıt defterlerine ekleyip diğer terminallere onaya gönderecekleri için ağ genelinde iki farklı kayıt defteri ortaya çıkacaktır. İşlemlerin farklı olması, aslında harcanmış olan kripto paraların harcanmamış olarak görünmesine neden olabilir.

Çakışma durumları çözülürken, sistem bir sonraki bloğun yaratılmasını bekleyecektir. Bir sonraki bloğu yaratan terminal hangi zincire sahip ise o zincir doğru kabul edilmekte ve sistem bu zincir üzerinden devam etmektedir. Diğer zincirdeki işlemler, kullanılmamış işlem havuzuna yeniden gönderilmekte ve karmaşıklıktan doğan iki versiyonlu blok zinciri sisteminde kayıt defterleri tek versiyona düşürülmüş olmaktadır.

1.7. Çatallaşma

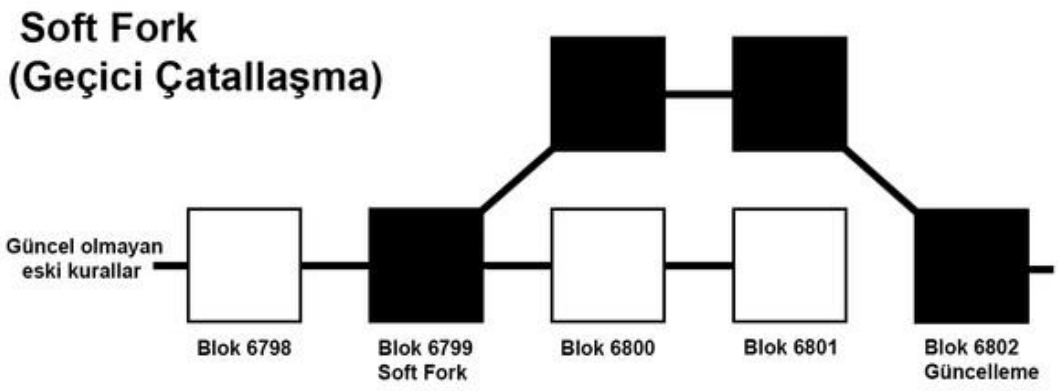
Merkezi olmayan blok zincir ağında, terminal olarak bilinen tüm katılımcıların birbirleriyle uyumlu çalışmaları için aynı kurallar dizisini(protokol) izlemeleri gerekmektedir. Çeşitli sebeplerle yapılan yazılım değişiklikleri sonrasında, protokollerin işleme şekli temelden değişir. Blok zincirinin yapısı gereği, her blok kendinden önceki bloğa bağlanmakta ve bir bloğa bağlı birden fazla blok olmamaktadır. Yazılım değişiklikleri/güncellemeleri sebebiyle böyle bir yapının oluşması durumuna çatallaşma (fork) adı verilmektedir. Çatallaşma 2 şekilde oluşmaktadır ve oluşma şekline göre de farklı yöntemlerle normal blok zincir yapısına uygun hale getirilmektedir.

1.7.1. Geçici/Yumuşak Çatallaşma (Soft Fork)

Yazılım üzerinde yapılan değişikliğin geçmişle uyumlu olması durumuna geçici/yumuşak çatallaşma adı verilmektedir. Geçmişle uyumlu olması demek; güncellenmemiş terminallerin, yeni protokol kurallarına uygun olduğu sürece hala işlem yapabilmesi ve zincire yeni bloklar ekleyebilmesi demektir.

Çatalda geçerli olan zincire karar verirken, zincirdeki terminallerin çoğunluğunun bu değişikliği onaylaması beklenmektedir.

Örnek olarak; blok boyutunu 2MB'dan 1MB'a indiren bir değişikliği düşünecek olursak, güncellenmemiş terminaller işlem gerçekleştirmeye ve 1MB boyut altında yeni bloklar eklemeye devam edebileceklerdir.



Şekil 13: Geçici Çatallaşma

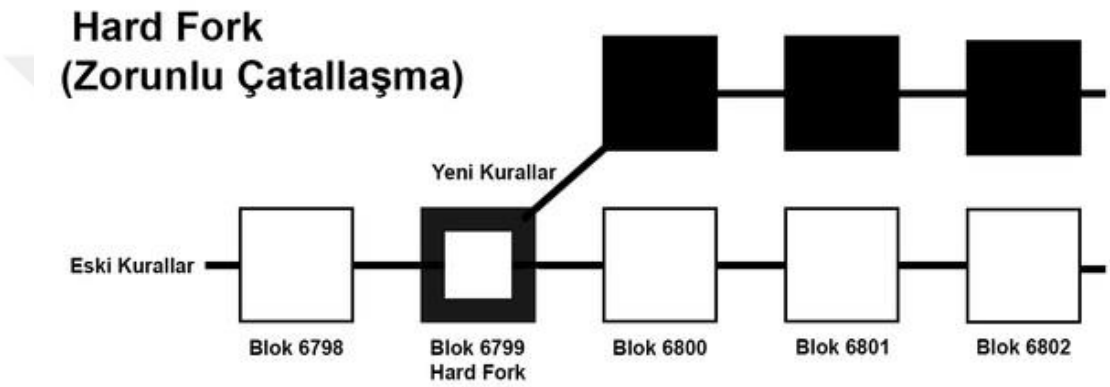
1.7.2. Zorunlu/Sert Çatallaşma (Hard Fork)

Yazılım üzerinde yapılan değişiklik, önceki versiyonlarla uyumlu olmayacak bir değişiklik ise buna zorunlu çatallaşma adı verilmektedir. Bu durum güncelleme yapmayan terminallerin artık işlem yapamayacakları ve zincire yeni blok ekleyemeyecekleri anlamına gelmektedir.

Terminaller, zorunlu olarak, güncellemeyi yaptıktan sonra devam edebileceklerdir. Örnek olarak, blok boyutunu 1MB'dan 3MB'a yükselten bir protokol değişikliğinde, eğer güncellenmiş bir terminal 2MB'lık bir blok oluşturup

ağa eklemeye çalışırsa, bu durum eski, güncellenmemiş terminaller tarafından geçersiz sayılarak reddedilecektir.

Güncellemenin yapılması konusunda terminaller arasında ayrılıkların oluşması durumunda ise, uygulama yeni bir isimle zincirini geçerli hale getirmektedir. Örnek olarak, Ethereum çatallaşması sonrasında Ethereum ve Ethereum Classic olarak iki kripto para, Bitcoin çatallaşması sonucunda Bitcoin Cash ortaya çıkmıştır.



Şekil 14: Zorunlu Çatallaşma

İKİNCİ BÖLÜM

2. BLOK ZİNCİR KULLANIM ALANLARI

Blok zinciri teknolojisi genellikle dijital para birimlerine (kripto para birimlerine) uygulanmakta, ancak dağıtık (merkezi olmayan) şeffaf yapısı, güvenli doğası ve yüksek performansı onu sadece kripto para birimleri için değil daha birçok endüstri ve kuruluşta (örneğin, yardım kuruluşlarında, tedarik zinciri, sağlık hizmeti vb.) güçlü bir araç haline getirmektedir.

Blok zinciri mahremiyeti arttırıp, güven ihtiyacını ortadan kaldırmaktadır. Uluslararası ödeme işlemlerinin aracısız/eşler arası gerçekleştirebileceği ve internet üzerinde değer transferi yapabileceği bir ortam oluşturur.

Hemen hemen her gün yeni bir kullanım alanında daha adının duyulduğu Blok zinciri sistemi için bugün kullanım alanlarının sınırsız olduğunu söyleyebiliriz. Para, ürün, mal, hizmet, iş, mülkiyet, hatta oy işlemleri bile aracısız yapılabilir durumdadır. Hatta 10 yıldan daha az bir sürede vergilerin toplanmasında dahi kullanılabileceği öngörülmektedir. Vasiyetlerin, dilekçelerin, sözleşmelerin, aracısız işlem görebilmesini, fikirlerin koruma altına alınmasını ve patent işlemlerinin aracısız yapılabilmesini de örneklere ekleyebiliriz.

2.1. Finans

Birçok kurum, Blok zinciri teknolojisinin kripto para haricindeki kullanım alanlarını araştırmakta ve yenilik yaratacak çözümlere yatırım yapmaktadır. Araştırmalar sonucunda ortaya çıkan Finansal kullanım alanlarını şu şekilde özetleyebiliriz; Alış/Satış Platformları, Takas Yönetimi, Para Transferleri, Yetkilendirme, Doğrulama, Dijital Kimlik Yönetimi, Doküman Yönetimi, Ödeme İşlemleri, İslami Bankacılık [7].

Bankacılık alanındaki örnek uygulamalardan, özellikle uluslararası para transferinin ve uluslararası ticaret finansmanının öne çıktığı gözlemlenmektedir. Örneğin Ripple uluslararası para transferi konusunda önce çıkan bir Blok zinciri çözümüdür ve Türkiye'de bir banka da buna dahil olmuştur. Uluslararası ticaretin

finansmanı alanında ise çeşitli bankaların bir araya gelip ortak yapılar oluşturduğu duyurulmaktadır.

Dünya çapında para gönderme söz konusu olduğunda, Blok zinciri teknolojisinin çok verimli olduğu kanıtlanmıştır. Kripto paraları arkadaşlara, ailelere ve dünyanın dört bir yanındaki kişilere göndermek, merkezi bankalara ve ödeme sistemlerine kıyasla daha ucuz ve hızlı olmaktadır.

Dahası, merkezi uygulamalar ve web siteleri kullanıcıların verilerini kontrol etmelerine izin vermez ve çoğu zaman platforma getirdikleri gerçek değere göre ödüllendirilmezler. Blok zinciri tabanlı merkezi olmayan uygulamalar (dApps), aradaki aracıları çıkararak, kullanıcılara daha düşük ücretler, daha iyi teşvikler ve daha fazla işlem verimliliğinin keyfini çıkarma potansiyelini verirken, aynı zamanda dijital para gönderip alabilme potansiyelini de vermektedir.

Örnek kullanım alanları:

2.1.1. Bankalar

Don Tapscott, iş stratejileri ve organizasyonel değişimler konusunda uzman olan Kanadalı bir danışmandır. Blok zincir teknolojisinin, önemli verileri (para, unvan, iş, müzik, sanat, bilimsel keşifler, fikri mülkler ve oylar gibi) sunucularda güvenli bir şekilde nasıl taşıdığını ve depolayabileceğini ortaya çıkarmak için iki yıllık bir araştırma projesi yürütmüştür [8].

Dünyanın en büyük finans şirketlerinden biri olan UBS bankası gibi bankalar, blok zincirinin maliyetlerini düşürmeyi, verimliliğini arttırmayı ve finansal hizmetlerde kullanım alanlarını araştırmayı hedef edinen yeni araştırma laboratuvarları kurmaktadırlar [9].

Rusya devlet bankası Sberbank, 2017 yılı sonunda, Rusya'nın Federal Tekel Karşıtı Servisi (FAS) ile blok zinciri teknolojisini kullanarak, belge transferlerinde ve depolama işlemleri için ortaklık kurduğunu açıklamıştır [10].

Dünyadaki en büyük vergi ve yönetim danışmanlığı firması olan Deloitte, blok zinciri yazılımı teknoloji şirketi olan ConsenSys ile 2016 yılında ConsenSys adını verdikleri bir dijital banka oluşturma planlarını açıklamışlardır [11].

R3, IBM, Chain.com, Ethereum, Intel ve Monax tarafından üretilen dağıtılmış defterlere R3 üyesi 42 banka bağlanmaktadır [12].

Zürih Cantonal Bankası, Swisscom ve İsviçre borsası blok zinciri teknolojisi olan Ethereum uygulamasını kullanan ortak bir sanayi birliği oluşturmuştur. Bu yapı, karşılıklı anlaşma yoluyla gerçekleşen varlık alım satımını prototip haline getirmektedir [13].

2.1.2. Diğer Finans Şirketleri

1996 yılında Amerika'da kurulan, kredi kartı ve ödeme sistemleri ile ilgilenen finans şirketi MasterCard, kişiden kişiye (P2P) ve işletmeler arası (B2B) ödeme sistemlerini geliştirmek için blok zinciri tabanlı üç tane API eklemiştir [14].

Döviz piyasasında uzlaşma hizmetleri sağlayan CLS Group şirketinin blok zincir tabanlı ödeme ağı hizmetleri CLSNet, blok zinciri teknolojisi ile çalışan ilk dünya döviz piyasası girişimi uygulaması olmuştur. CLSNet, Devlet tarafından yönetilen Çin Merkez Bankasının Hong Kong şubesi gibi küresel kuruluşlardan ortaklık taahhüt etmiştir [15].

Mastercard, SWIFT, VISA ödeme sistemleri ve Unionpay şirketleri, blok zincir teknolojisini kullanma planlarını ve konuyla ilgili kaydettikleri gelişmeleri açıklamıştır [16].

Denizcilikte dünyanın ilk ödeme ekosistemi olan Prime Shipping Vakfı, nakliye endüstrisindeki ödemelere ilişkin sorunları çözmek için yapılan her işlemde (%100) blok zincir teknolojisini kullanmaktadır [17].

2.2. Tedarik Zinciri

Tedarik zinciri sistemlerinin çoğu şeffaflık ve verimlilik açısından engellerle karşı karşıyadır. Geleneksel tedarik zinciri anlayışında bilgi paylaşımı çoğunlukla sadece birbirleriyle doğrudan ilişki kuran taraflar arasında mevcuttur. Zincir ilerledikçe bu bilgiler kaybolmakta, son tüketici veya daha önceki aşamalarda rol alanların elindeki veriler yetersiz kalmaktadır. Teknolojik gelişmeler geleneksel tedarik zincirlerini dinamik ve bağlı dijital tedarik ağlarına dönüştürme fırsatı sunsa da kağıt üzerindeki işlemler halen çok yaygındır ve bu da ağlar arasında

entegrasyonun ve iş birliğinin azalmasına neden olmaktadır. Tedarik zinciri yönetimini iyileştirmek isteyen kuruluşların yaşadığı sorunların büyük ölçüde izlenebilirlik, uyumluluk, esneklik ve paydaş yönetimi konularında olduğu görülmektedir.

Blok zinciri teknolojisi, bir tedarik zinciri ağı içinde malzemelerin oluşturulma ve dağıtılma sürecinin tamamını takip etmek için kullanılabilir. Dağıtık bir veri tabanı, ilgili verilerin güvenli bir şekilde kaydedilmesi, ürünlerin orijinalliğinden emin olunması ve ödemelerin ve ulaşımın şeffaflığını sağlanması için de uygun olmaktadır.

Akıllı sözleşmeler ile mümkün kılınan gerçek zamanlı izlenebilirlik, tedarik zinciri paydaşlarına hızlı karar alabilme ve azalan maliyetler ile stok seviyelerini sürekli olarak güncelleme esnekliği sağlamaktadır. Blok zinciri, güvenilir dijital imzalar ile doğrudan taraflar arası (peer-to-peer) etkileşimleri mümkün kılarak aracıları ortadan kaldırmakta, ilgili taraflar arasında iletişimi ve güveni sağlayan etkin bir yönetişim oluşturmaktadır.

Blok zinciri tabanlı, tedarik zinciri çözümlerine; Opporty, Tracr (mücevher endüstrisi), TradeLens (sevkiyat), Walmart (gıda güvenliği) örnekleri verilebilir.

2.3. Sağlık Hizmetleri

Operasyonel engeller, veri hataları ve bürokrasi, sağlık sektörü için önemli bir endişe kaynağıdır. Blok zinciri, tedarik zinciri aracılığıyla ilaçları izlemek ve hasta verilerini yönetmek de dahil olmak üzere sağlık hizmetlerinde çeşitli kullanım alanına sahiptir.

Ayrıca, Blok zinciri teknolojisi hastanelere önemli güvenlik faydaları sunabilir, çünkü bu kurumlar genellikle sahip oldukları verilerin yüksek değeri ve bu verilere bağımlılığı nedeniyle bilgisayar korsanları tarafından saldırıya uğramaktadır.

Şirketler, dijital sağlık kayıtlarını saklamanın bir yolu olarak Blok zinciri kullanımını incelemektedirler. Bu tür çözümler, veri gizliliğini ve doğruluğunu arttırırken genel giderleri azaltmaktadır.

2.4. Telif Ödemeleri

Genel olarak müzisyenler, video oyun yaratıcıları ve sanatçılar, dijital korsanlık, üçüncü tarafın haksız kullanımları ya da hak edilmiş telif haklarının ödenmemesi nedeniyle hak ettikleri ödemeyi almakta zorluk çekmektedirler.

Blok zinciri teknolojisi, yaratıcı yeteneklerin içeriklerini kiralamalarına, satmalarına ve / veya içeriklerini kullanan kişilerin değişmez ve şeffaf bir kayda sahip olabilecekleri bir platform oluşturmak için kullanılabilir. Böyle bir platform, akıllı sözleşmeler (temelde kendi kendine çalışan / işlerlik kazanan dijital sözleşmeler) yoluyla ödemeleri de kolaylaştırabilmektedir.

Örnek Kullanım Alanları:

Yazarların platformu olarak 2017 yılında kurulan Publiq, sahte haberlerle mücadele etmek, sansürden kaçınmak ve metinlerin gerçekliğini garanti etmek için blok zinciri teknolojisini kullanmaktadır [18].

2.5. Yardım Kuruluşları

Dünya çapında birçok yardım kuruluşu kaynak yönetimi, operasyonel şeffaflık ve yönetişim zorluklarının üstesinden gelmeye çalışmaktadır. Blok zinciri teknolojisi, bu kurumların fon alma ve yönetme sürecinin optimize edilmesine de yardımcı olabilecektir.

Örnek Kullanım Alanları:

Blok zinciri Yardım Vakfı (BCF), yoksulluk ve eşitsizlikle mücadele ederek sürdürülebilir kalkınma hedeflerini gerçekleştirmeye çalışan, dünya çapında Blok zinciri destekli yardım sağlamayı amaçlayan ve kar amacı olmayan bir organizasyondur.

Bill & Melinda Gates Vakfı, Level One Project adını verdikleri proje ile bankacılığı herkese ulaşılabilir hale getirmeyi, bunun için de blok zinciri teknolojisini kullanarak dünyada banka hesabı olmayan iki milyar insana yardım etmeyi amaçlamaktadır [19].

2.6. Kamu Sektörü

Kamu sektöründe blok zinciri teknolojisinin kullanılabileceği alanlara örnek olarak Dijital Kimlik, Dijital Pasaport, Oylama, Sosyal Güvenlik Sistemi, Doküman Yönetimi, Akıllı Kontratlar, Vergi Sistemi ve Enerji Dağıtımı verilebilir.

Blok zinciri teknolojisi, çeşitli farklı sektörlerde yönetişimi büyük ölçüde geliştirme potansiyeline sahiptir. Blok zinciri tabanlı sistemler, ağları ve işlemleri daha demokratik, adil ve güvenli bir şekilde yöneterek, oy sahtekarlığını önlemede ve seçimler ya da diğer anayasa süreçlerine olan güven artışını sağlamak amacıyla araç olarak kullanabilmektedir. Ayrıca, yolsuzluğa karşı güçlü bir silah olarak da kullanılabilmekte, vergi tahsilatından mali yardım dağıtımlarına kadar çeşitli senaryolarda veri bütünlüğünü ve izlenebilirliğini arttırmaktadır.

Örnek Kullanım Alanları:

- İsveç, ülkenin tapu defterini blok zincirine almak için testler yapmaktadır [20].
- Gürcistan, mülk kayıtlarını yöneten bir blok zinciri uygulaması kullanmaktadır [21].
- Hindistan Hükümeti, arazi sahtekarlığını durdurabilmek için blok zinciri kullanmaktadır [22].
- 2017 yılında, ilk uluslararası mülk işlemi, BitBay'in blok zincir tabanlı akıllı sözleşme uygulaması kullanılarak başarıyla tamamlanmıştır [23].
- 2018'in ilk yarısında, Rusya Ekonomik Kalkınma Bakanlığı, tapu defterlerinde blok zincir teknolojisinin kullanımının ne kadar güvenilir olacağını test edebilmek için Moskova'da pilot bir proje yürüteceklerini açıklamıştır [24].
- Amerika Genel Hizmetler İdaresi'nde görevli olan BT Sözleşme Planlama Operasyon Müdürü Jose Arrieta, 2017'de dağıtılmış defter teknolojisinin BT Planlı 70 sözleşme için, otomasyon ve FASt Lane süreci kullanılarak nasıl hızlandırılabileceğini araştırdıklarını açıklamıştır [25].

- Tunus, 2015'in sonlarında, kendi dijital para birimi olan e-Dinar'ı, blok zincir tabanlı bir versiyon ile değiştirerek ulusal para birimini blok zinciri teknolojisi ile kullanan dünyadaki ilk ülke olmuştur.
- Senegal, blok zincir tabanlı olan ulusal dijital para birimi eCFA'yı oluşturarak, bunu gerçekleştiren dünyadaki ikinci ülke olmuştur.

2.7. Nesnelerin İnterneti (IoT)

Blok zinciri ve Nesnelerin İnterneti (IoT) doğal bir birlikteliktedir. Blok zinciri dağıtık yapıda bir teknolojidir ve IoT ağları ise genellikle birbirinden dağınık olan kaynaklardan veri toplamak için kullanılmaktadır.

Blok zinciri teknolojisi kurumlara, Nesnelerin İnterneti (IoT) cihazlarıyla ve nesnelerin birbirleriyle etkileşimleri vasıtasıyla topladıkları verileri, değişmez ve şeffaf bir defterde tutmasını sağlar. Güvenlik özelliklerinin ve kripto para uygulamalarının yanı sıra, Blok zinciri teknolojisi makineden makineye (M2M) gerçekleştirilecek işlemler için de ideal bir platform sunmaktadır.

Blok zinciri teknolojisi, işlemlerin doğru ve güvenli bir şekilde gerçekleşmesini kolaylaştıran bir teknoloji olduğundan, hesap verebilirlik, veri doğruluğu ve güvenliği sağlamak için IoT ile entegre olması oldukça mantıklıdır. Tam da bu nedenle birçok firma, Blok zinciri destekli IoT ağlarına çok fazla kaynak ayırmaktadır.

2.8. Ülkemizde Blok Zincir Kullanım Alanları

Ülkemizde akademik ve uygulama alanında, dünyadaki diğer gelişmelere nazaran blok zinciri konusundaki bilgi ve deneyim oldukça sınırlı kalmaktadır.

Blok zincir kavramı ile ilgili belirli bir farkındalık bulunmaktadır fakat bu teknolojiye olan derin bilgi birikimiyle ilgili gelişime açık noktalar olduğu görülmektedir. Gün geçtikçe bu açığı kapatmaya yönelik, bilgi alışverişini hızlandırabilmek ve daha çok kişiye ulaşabilmek için; kar amaçlamayan kuruluşlar, akademik çevreler, büyük ve küçük ölçekli şirketler çalışmalar yapmaktadır. Yapılan ve yapılması planlanan bu çalışmaların, Türkiye'nin blok zinciri yolculuğuna katma değer sağlayacağı düşünülmektedir.

Dünya çapında pek çok örneği olan blok zincir tabanlı servisler, Türkiye'de de giderek artmaktadır.

Akbank, 2018 Aralık ayında dağıtık defter teknolojisi şirketi Ripple'ın blok zinciri ağına katıldığını ve uluslararası para transferi işlemlerinde bu teknolojiyi kullanacağını açıklamıştır. Sterlin transferi için kullanılacak Ripple'ın küresel ödeme ağındaki 43 müşteri arasında, Türkiye'den yalnızca Akbank bulunmaktadır. Açıklamadan 1 hafta sonra, Akbank'ın mobil uygulamasında Ripple üzerinden transfer işlemleri başlamış ve tüm müşterilerin kullanımına sunulmuştur [28].

Türkiye'de 2017 yılında yapılan girişimcilik yarışması olan Webrazzi Arena'nın birincisi blok zinciri tabanlı dijital kimlik girişimi "Kimlic" olmuştur. Türkiye'nin ilk "Know Your Customer" uygulaması olmayı hedeflemiştir [29].

BKM (Bankalararası Kart Merkezi) şirketi, Türkiye'nin ilk blok zinciri projesi BBN'i şirket çalışanları için kullanıma açmıştır. Bu uygulama ile; dijital kimlik güvenli bir şekilde oluşturulmakta, saklanmakta ve paylaşılmaktadır. Dağıtık kayıt yapısı, akıllı sözleşmeler ve mutabakat kavramları test edilmiştir. BKM şirketi, Etherum uygulaması üzerinde de proje geliştirebilmek için araştırmalar yapmaktadır [30].

2017 yılından itibaren birçok üniversitede blok zinciri odaklı çalıştaylar yapılmaktadır.

Yine 2017 yılı itibariyle, TC (Türkiye Cumhuriyeti) Merkez Bankası ana sponsorluğunda TÜBİTAK Blokzincir Araştırma Laboratuvarı (BZLab) kurulmuştur [31].

Blok zinciri teknolojisinin ortaya çıkışı eski dönemlere dayansa da özellikle kripto paraların geliştirildiği dönemde bu teknolojiye ilgi artmıştır ve bireysel yatırımcıların da dikkatini çekmeye başlamıştır. Bu teknolojiye olan ilginin yoğun olarak artmasına rağmen, aktif uygulamaların sayısı henüz öngörülen seviyelere ulaşmamıştır. Türkiye'de ve küresel pazarlarda, bu durumun temel sebepleri arasında engeller ve belirsizlikler yer almaktadır.

ÜÇÜNCÜ BÖLÜM

3. GELECEĞİ, AVANTAJ VE DEZAVANTAJLARI

3.1. Blok Zincirin Geleceği

Küresel ekonominin geleceği, dağıtılmış varlık ve güvene dayanan Blok zinciri işlemlerine doğru yol almaktadır. Üçüncü parti denetlemenin ve onaylama mercilerinin Blok zinciri ile gelecekte gerekli olmayacağı öngörülmektedir. Bunun bir sonucu olarak, kamu kurumları Ticari ve Finansal kanunları dayatmakta zorlanacaklardır. Örnek olarak, Bitcoin'in sağladığı olanaklar daha şimdiden geleneksel Ticaret araçlarını gereksiz kılmaktadır.

Bu teknoloji bazı yorumlamalarda, 90'lı yılların başlarındaki internet ekosistemine benzetilmektedir. Google, arama motorlarının ilki değildir fakat internet ekosisteminde güçlü bir yer edinmiştir. Dahası Facebook da sosyal ağların ilki değildir ve en iyilerden biri olarak yer edinmiştir. Benzer eğilimin blok zinciri dünyasında da görüleceği düşünülmektedir.

Diğer taraftan, Blok zinciri teknolojisinin uygulandığı alanlarda küresel olarak kabul gören standartların oluşmaması, uygulanmasının önündeki önemli engellerden biri olarak görülmektedir. Regülasyon çerçevesinin henüz çizilmemiş olması ve uygulamada oluşabilecek operasyonel belirsizlikler ile finansal riskler, şirketlerin bu alanda yatırım yapma isteklerini azaltmaktadır. Belirsizliklerin giderilmesi için de uygulama alanlarındaki çalışma ve çalıştayların arttırılması ve hızlandırılması gerekmektedir. Ek olarak, teknolojilerin araştırmalarla ve uygulamalarla daha çok gelişebileceği ve yeni değerler kazandırabileceği unutulmamalıdır. Şirketler insan kaynağını ve finansal kaynaklarını bu alana yönlendirdikçe, uygulamaların hem finansal hem operasyonel etkilerini, nasıl tasarruf sağlanabileceğini ve rekabet avantajı yaratılabileceğini daha net şekilde ortaya koyabileceklerdir. Şirketlerin blok zinciri ekosistemlerinde aktif rol alarak konsorsiyumlara dahil olması bu süreci hızlandıracaktır.

Sadece kurum içi çözümlere odaklanmak, blok zincir teknolojisinin sunduğu asıl faydayı gözden kaçırmak anlamına gelecektir. Çünkü bu teknolojinin farklı kurumlar arasındaki süreçlerde sağlayacağı verimlilik, bunun çok daha ötesinde bir

etki yapacaktır. Ülkemizin geleceği ve daha iyi bir hizmet anlayışı için düzenleyiciden, bankalara ve teknoloji şirketlerine kadar tüm ekosistem olarak ideal çözüme götürecek yolu bulmak için odaklanılmalıdır.

Blok zinciri teknolojisi, ana konuları ve yetenekleri tek bir çözümde birleştirme olanağı sağlamaktadır. Böylece hali hazırda kabul gören iş süreçlerini daha şeffaf, sade ve verimli hale getirmek, hatta eldeki teknolojilerle uygulanamayacak iş modellerini hayata geçirmek mümkün olmaktadır. Bunun sonucu olarak da iş sonuçları bir adım öteye taşınarak yeni değer alanları yaratılabilecektir.

Özetle blok zinciri teknolojisiyle ilgili yapılabilecek en büyük hatanın, hiçbir şey yapmamak olduğu söylenebilir. İş alanları öngörülebilir olmasa da ve uygulamanın somut örnekleri olmasa da şirketler blok zinciri konusunda girişimlerde bulunarak konuya ilgilerini sürdürmelidir ve oluşabilecek fırsatları yakalamaya hazır olmalıdır.

3.2. Blok Zincirin Avantajları

- Kolay Takip

Blok zinciri, bir varlığın kaynağından çıktığı andan itibaren hangi kişilerin elinden geçtiğinin ve nereye ulaştığının takibinin yapılabilmesi için idealdir.

- Şeffaflık

İşletmelerin bu teknolojiyi kullanmasının nedenlerinden biri de açık kaynak yapısıyla ilgilidir. Bu, ağdaki diğer kullanıcıların bilgileri okuyabildiği ve onaylayabileceği (veya onaylayamayacağı) anlamına gelir. Açık kaynak olmasının en önemli avantajı, ağ kullanıcılarının çoğunluğu olmadan işlenen verileri kaydedememesidir.

Kayıtların her bir kopyası katılımcılar tarafından tutulduğu için erişimdeki şeffaflığın yanında verinin korunmasını da sağlamaktadır.

- Merkezi olmama

Merkezi bir otoriteye bağlı değildir ve aynı zamanda buna ihtiyaç duymamaktadır. Büyük bir veri merkezi çalıştırılması yerine, bilgiler merkezi olmayan ağa kaydedilirse, burada herhangi bir kullanıcı işlemleri otomatik olarak okuyabilir ve kontrol edebilir.

- Hızlı İşlem Süreleri

Blok zinciri teknolojisi günde 24 saat, haftada yedi gün çalışmaktadır, bu da Blok zinciri tabanlı işlemler için sürecin daha hızlı olduğunu göstermektedir.

Geleneksel bankalara işlem gönderildiğinde (para transferi gibi), işlemlerin tamamlanması birkaç günü bulabilmektedir. Bunun nedeni banka transfer yazılımlarındaki protokollerin yanı sıra finansal kurumların sadece haftada beş gün çalışması ve yalnızca mesai saatlerinde açık olmasıdır. Ayrıca dünyanın her yerinde yerel saatler farlılık gösterdiği için uluslararası bankacılık işlemleri birkaç hafta zaman alabilmektedir.

- Kullanıcı Kontrollü Ağlar

Bu avantaj, ağın merkezileşmesinin bir sonucudur. Veri işleme için üçüncü bir taraf tutmak yerine, paydaşlar birbirlerini kontrol etmeye ve bundan sonra ne yapacaklarına karar vermeye devam etmektedirler.

- İşlem Maliyetlerinin Azalması ve Tasarruf

Blok zinciri genellikle bir banka veya merkezi bir sunucu olan üçüncü bir tarafa ihtiyaç duymadan işlem yapılmasına izin vermektedir. Arabulucu bulunmadığından, onun gerektireceği masraf kalemlerinden kurtulmayı sağlamaktadır. Örnek olarak 2022 yılı itibariyle Blok zincirini bankaların kullanması durumunda masraflarını 15-20 milyar dolar azaltabileceği öngörülmektedir [32].

3.3. Blok Zincirinin Dezavantajları

- Yasallık ve regülasyonlar:

Blok zinciri uygulamasında tüm işlemlerin herkese açık olması, özellikle Bitcoin gibi kripto paraların terör finansmanı veya kara para aklama için kullanılabileceği çekincelerini oluşturmaktadır. Bu nedenle olumsuz bir imaja sahip olan Bitcoin, Merkez bankaları ve kamu otoriteleri tarafından henüz yeterli desteği alamamış ve bazı ülkelerde yasaklanmıştır. Bitcoin ve diğer kripto paralar blok zinciri teknolojisini kullandıkları için, bu olumsuz imaj blok zinciri teknolojisinin geleceği açısından da bir risk olarak görülmektedir.

Blok zinciri teknolojisinde, zincire eklenen işlemler değiştirilemez yapıdadır. Bu özellik güvenlik açısından önemli yapı taşlarından biridir fakat hırsızlık olması durumunda ortaya çıkan işlemlerin ya da yapılan hatalı işlemlerin temizlenememesi açısından bir dezavantaj olarak yorumlanabilmektedir. Aynı zamanda bu durumun, finans dünyasındaki bazı yasalar ve düzenlemeler ile çelişebileceği ve blok zinciri teknolojisinin yaygınlaşmasında zorluklar çıkarabileceği düşünülmektedir.

- Güvenlik:

Bitcoin takas merkezlerinde önemli hırsızlık olaylarının yaşanması, bu teknolojiye olan güvenin sarsılmasına neden olmaktadır.

Yaşanan hırsızlık olayının aslı, Bitcoin takas merkezlerinin çoklu-imza güvenlik teknolojisine gerekli hassasiyeti göstermemeleri ve entegrasyona soğuk cüzdanlar yerine sıcak cüzdanlara ağırlık vermeleri olduğu gözlemlenmektedir.

- Yazılım Değişiklikleri:

Blok zinciri dağıtık uzlaşı prensibiyle çalışır ve sistemin güvenli bir şekilde çalışabilmesi için bütün eşlerde aynı algoritmaları çalıştıran açık kaynaklı yazılımlar bulunmaktadır. Farklı sebeplerle bu yazılımın kullandığı algoritmalarda, parametrelerde veya özelliklerinde geliştirmeler yapılması gerekebilmektedir.

Merkezi olmayan dağıtık bir sistemde bu tip değişikliklerin yapılması; farklı sebeplerle (seçilen yöntem, tercih edilen zamanlama, vb.) dağıtık sistemin eşleri

arasında anlaşmazlık ya da krize neden olabilmektedir. Bu da sisteme olan güvenin azalmasına, dolayısıyla da blok zinciri teknolojisine yapılan desteğin azalmasına neden olabilmektedir.

- Teknik Altyapı Yeterliliği:

Bu teknolojinin, artan ölçekteki ihtiyaçları karşılayabilmek için yeterli bir teknik altyapısı olup olmadığı araştırılan konular arasında yer almaktadır. Böylesine büyük ve dağıtık bir sistemde çalışan algoritmalar, ölçeğin artmasıyla, saniyede binlerce işlem seviyesine ulaşma durumu ile karşı karşıya kalacaktır.

DÖRDÜNCÜ BÖLÜM

4. BLOK ZİNCİR YAPISINDA %51 SORUNSALI

Blok zincir yapılarında karşılaşılan belli başlı kötü niyetli saldırı ve problemleri Tablo 2'de sınıflandırılarak gösterilmiştir. Temel blok zincir yapısını sağlamış sistemler olduğu takdirde bu problemlerin büyük kısmı aşılmış olmaktadır. Ancak %51 saldırısı yöntem açısından diğerlerinden farklılık göstermektedir.

Tablo 2: Blok Zincir yapılarında Saldırı Tipleri

Kötü Niyetli Saldırı Tanımları	Açıklamaları	Savunma ve Önlemleri
Çifte Harcama	Birey, varlığı kullanarak birden fazla harcama yapar	Madencilik sürecinin karmaşık gelişmiş yapısı bu soruna cevaptır.
Sahte Kayıt	Blok Zincir defterindeki kayıtlar değiştirilir ya da deftere sahte işlemlerin eklenmesi	Dağıtık yapının mutabakat süreci bu soruna cevaptır.
Kimlik Hırsızlığı	Bireyin özel anahtarının çalınması	İtibarlı blok zincirlerde işlem yaparak aşılabilir.
Yasa dışı aktiviteler	Tarafların yasadışı malları işletmesi veya kara para aklama işlemlerini gerçekleştirmesi	Kanun ve yönetmeliklerin çıkarılarak önlenebilir.
Sistemin Ele Geçirilmes	Bir blok zinciri uygulayan programlama kodları ve sistemleri tehlikeye girmesi	Sağlam sistemler ve gelişmiş izinsiz giriş tespit yöntemleri ile önlenebilir
%51 Saldırısı	Ağ terminallerinin geri kalanından daha fazla hesaplama gücüne (% 51) sahip tek bir madenci terminalin, işlemlerin	Blok zincir teknolojisinin geniş kullanım alanı

%51 saldırısı, bir blok zincir ağında tek bir kuruluş veya kuruluşların, ağ üzerinde gerçekleşen %50 hashing (özetleme) gücünden fazlasını elde edebilme gücüne kavuşmasına denir. Diğer ifadeleriyle "%51 Sorunsalı", "%51 atağı", "%51 problemi" veya "Çoğunluk Atağı" da kullanılmaktadır.

Ağ üzerinde, %50 den fazla gücün bir kişi veya kişilerin kontrolüne geçmesi durumunda, potansiyel olarak ağda kesintiye neden olabilirler ve ekosistemin bozulmasını sağlayabilirler. Talep edilen transfer işlemlerinin sıralarını kasıtlı olarak değiştirebilir, işlemlerinin onaylanmasına müdahale edebilir, bir kısmını tersine çevirerek çifte harcama (double spending) yapabilirler. Ayrıca blok üreticilerinin, blok sonuçlarını değiştirebilirler. Blok üretimiyle elde edilecek blok ödüllerini kendilerine yazabilirler.

Bir blok zincirin yüksek güvenlikli anılmasının temel sebeplerinden biri, dünyanın herhangi bir yerine dağıtılmış terminallerin fikir birliğine varmış olmalarıdır. Ağ büyüdükçe yani terminal sayısı arttıkça, saldırı ve veri bozulmalarına karşı daha güçlü olurlar. Çünkü bir blok ne kadar fazla onay alırsa oradaki işlemleri değiştirme ve geri alma maliyetleri de o kadar yüksek olur.

4.1. Hashrate (Hesaplama Gücü)

Hashrate, POW yöntemiyle çalışan bir blok zincir ağında, üretilecek yeni bloğun özet değerini hesaplamak için harcanan gücü ifade etmektedir. Bu güç değeri, matematiksel problemi çözmek için özetleme algoritmasını çalıştıran donanımlara ait hızın ölçüsü olarak kabul edilmektedir.

Diğer bir ifadeyle POW yöntemiyle çalışan bir ağda, blok oluşumu için çalışan bir terminal cihazı düşündüğümüzde, hashrate değeri 1MH/S ise, bloğun özet değerini bulabilmek için 1 saniyede 1 milyon deneme yapacak güçte olduğu anlamına gelmektedir. Bugün Bitcoin ağında bulunan terminal sayıları 10 bine yaklaşırken ağın hashrate gücü 50 EH/s'nin üzerine çıkmıştır.

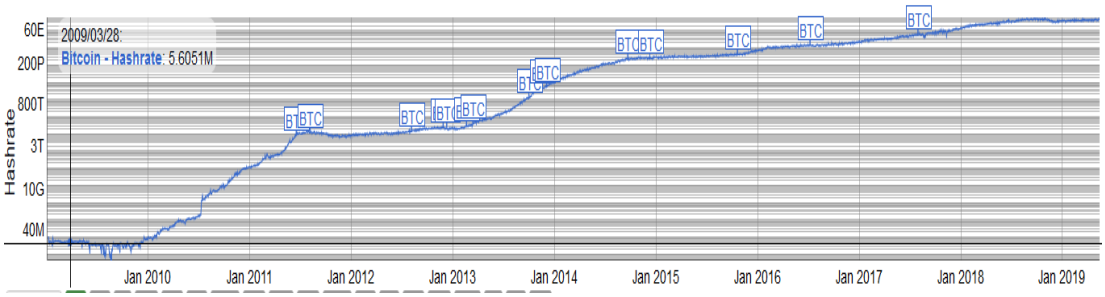
Tablo 3: Veri Ölçü Birim Tablosu

Sembol	Kısaltması	Açıklaması	Ondalık
mega	M	Milyon	1.000.000
giga	G	Milyar	1.000.000.000
tera	T	Trilyon	1.000.000.000.000
peta	P	Katriyon	1.000.000.000.000.000
exa	E	Kentilyon	1.000.000.000.000.000.000
zetta	Z	Sekstilyon	1.000.000.000.000.000.000.000

Hashrate türünden hesaplama değerleri de ayrıca aşağıda gösterilmektedir. Blok zincir yapılarına bakıldığında bu hesaplama değerlerini göz önünde bulundurarak ağın gücü yorumlanabilmektedir.

- 1 MH/s saniyede 1,000,000 (bir milyon) hesaplama gücü
- 1 GH/s saniyede 1,000,000,000 (bir milyar) hesaplama gücü
- 1 TH/s saniyede 1,000,000,000,000 (bir trilyon) hesaplama gücü
- 1 PH/s saniyede 1,000,000,000,000,000 (bir katrilyon) hesaplama gücü
- 1 EH/s saniyede 1,000,000,000,000,000,000 (bir kentilyon) hesaplama gücü

Şekil 15'te en büyük blok zincir ağına sahip BTC'nin 10 yıllık hashrate tarihçesi gösterilmektedir. MegaHash/saniyelerden başlayıp TeraHash/saniyelere ve son birkaç yıl içinde ağ terminallerinin güçlenmesiyle ExaHash/saniyelere ulaşmıştır.



Şekil 15: Bitcoin Hashrate Tarihçesi

4.2. %51 Saldırı Örnekleri

Özellikle kripto para piyasalarında düşüşlerin yaşandığı dönemlerde, üretici pozisyonundaki terminaller blok zincirlerinden ayrılmaları durumunda ağların hashrate değerleri düşmektedir ve %51 saldırılarına karşı savunmasız hale geldikleri görülmektedir. %51 saldırısını, BTC gibi büyük bir blok zincir ağına yapmak pratikte çok zor olmakla birlikte, saldırı küçük blok zincirlerinde nispeten daha mümkün olmaktadır. Son yıllarda %51 saldırısına maruz kalmış bazı blok zincirlerinden örnekler verilebilir.

3 Haziran 2018 tarihinde, ZenCash (ZEN) blok zincirine gerçekleştirilen %51 saldırısı sonucu 38 blok geri gitme işlemi gerçekleştirildi. Toplamda 550.000 Dolar değerinde 19.600 adet ZEN çalınmıştır. Saldırının 4 saat sürdüğü ve saldırı maliyetinin 30.000 Dolar olduğu bildirildi. ZenCash ekibi sonrasında %51 saldırılarından korunmak için birtakım yenilikler yaptıklarını duyurdular. Mutabakat algoritmalarında geliştirme yaparak blok bildiriminde gecikme yaşayan kullanıcıları cezalandıracak bir mekanizma eklediklerini bildirdiler. Büyük miktarlarda transfer işlemleri için onay sayısını arttırdılar.

2 Aralık 2018 tarihine kadar 4 aşamalı bir şekilde gerçekleşen bir başka %51 saldırısı Vertcoin (VTC)'e yapıldı. Güvenlik uzmanlarının saldırı sonrası yayınladığı rapora göre, blok zincirindeki 307 bloğun etkilendiği ve toplam 100.000 Dolarlık bir kayıp yaşandığı bildirilmiştir.

7 Ocak 2019 tarihinde, Ethereum Classic (ETC) blok zincirine %51 saldırısı gerçekleşmiş ve 250.816.191 Dolar değerinde 54.200 adet ETC çalınmıştır. Araştırmacılar tarafından daha sonra yapılan inceleme de ETC blok zincir mutabakat algoritmasının ve hashrate gücünün yeterli olmadığı, %51 gücünün kolaylıkla toplanabildiği tespit edilmiştir. ETC bu saldırıdan sonra onay sayısını 8 kat arttırarak 500'den 8000'e çıkarmıştır.

4.3. Bitcoin Blok Zincirinde % 51 Matematiği

POW blok zincirinde, bir blok üreticisi terminalin sahip olduğu hash hesaplama gücü arttıkça bir sonraki bloğu çözme şansı da artmaktadır. BTC de bazı madenciler blok zincirin büyüme ve güvenilirliğine katkıda bulunmak için ekosisteme dahil oldular. BTC'nin yükselen fiyatıyla birlikte blok ödüllerini elde etmek amacıyla rekabet edecek birçok yeni madenci sisteme girmiştir. Blok ödülü almak için bu kadar çok terminal oldukça sistemin güvenliği bir yandan artarken, bir yandan blok üretip ödül elde etme işlemi zorlaşmakta dolayısıyla daha fazla yatırım yapılarak yüksek hash gücüne sahip donanımlara ihtiyaç duyulmaktadır.

Bugün BTC ağına saldırmaya karar vermiş birinin bunun maliyet analizini iyi yapması gerekir. 2019 mayıs ayı itibariyle, BTC network hashrate değerleri 50 EH/s üzerinde seyretmektedir. Bir diğer ifadeyle, ekosistemin toplam özetleme gücü saniyede 50 Kentilyon (50.000.000.000.000.000.000) deneme yapacak değerdedir.

Şekil 16. BTC'nin Market ve Ağ Hashrate Değerleri

11 Mayıs 2019 itibariyle Blockchain isimli web sitesinden alınan Şekil 15' de BTC'nin network hash rate değeri: 52.242 PH/s olarak gösterilmiştir. BTC üretilmesi için çalışan cihazların satılması esnasında "Hash Rate" değerleri ve "Elektrik Tüketim" değerleri en önemli göstergelerdir. Bu cihazlar bugün itibariyle Tera Hash / Saniye cinsinden konuşulduğundan, BTC'nin network hash rate değerini de PH/s cinsinden TH/s cinsine çevirirsek, 52.242.000 TH/s olarak ifade edilebilir.

Şu an piyasada bulunan ve bitmainturkiye ve asicminertukery isimli web sitelerinde satılmakta olan 2 farklı gelişmiş cihazın fiyat, hash rate ve elektrik tüketim değerleri aşağıdaki Tablo 4'te gösterilmiştir.

Tablo 4: SHA256 Algoritması Çalıştıran 2 Cihaz Modeli

Cihaz Adı	Fiyat ($)	Hashrate (TH/s)	Elektrik Tüketimi (Watt)
Antminer S15 27Th	1.704	27	1596
BitFury B8	2100	49	6400

Bu örnek cihazlar kullanılarak, saldırı yapacak kişinin BTC ağında %50 lik güce ulaşabilmesi için, en az ağın toplam hash rate değeri (52.242.000 TH/s) kadar güce ihtiyaç duyacaktır. Dolayısıyla ihtiyaç duyulan cihaz sayısı aşağıdaki formül üzerinde gösterilmektedir.

Ağ Hash Rate / Cihaz Hash Rate = En az %50 Ağ gücünü elde edebilmek için ihtiyaç duyulan Cihaz Adeti

52.242.000 Ağ Terahash / 27 Cihaz Terahash = 1.934.889 Antminer S15
52.242.000 Ağ Terahash / 49 Cihaz Terahash = 1.066.163 BitFury B8

Toplam Gereken Cihaz Adeti X Birim Fiyatı = Toplam Cihaz Maliyeti

1.934.889 Adet Antminer S15 * 1.704 $ = 3.297.050.667 $
1.066.163 Adet BitFury B8 * 2.100 $ = 2.238.942.857 $

İlgili teknolojik cihazların yerleşim maliyetini hesaplayabilmek içinse, dünyanın farklı yerlerindeki terminal ve havuzların altyapı maliyetlerine bakıldığında cihazların toplam maliyetinin %22'si ile %40'ı arasında olduğu öngörülmektedir. Hesaplamamızda en alt oran olan %22'yi dikkate alınırsa;

*Cihaz Yerleşim Maliyeti = Cihaz Maliyeti * 0,22*

Antminer S15 Yerleşim Maliyeti = 3.297.050.667 * 0,22 = 725.351.147 $
BitFury B8 Yerleşim Maliyeti = 2.238.942.857 * 0,22 = 492.567.429 $

Toplam Sabit Maliyet = Cihaz Maliyeti + Yerleşim Maliyeti

Antminer S15 Sabit Maliyet = 3.297.050.667 + 725.351.147 = 4.022.401.813 $
BitFury B8 Sabit Maliyet = 2.238.942.857 + 492.567.429 = 2.731.510.286 $

Bugün BTC ağında %50'lik gücü elde edebilmek için gerekli olan toplam sabit maliyetlerin yanında Elektrik Tüketimi, Personel Giderleri gibi değişken maliyetlerde vardır. Bunlardan en önemli değişken maliyet olan elektrik tüketimi hesaplanırsa;

*Toplam Cihaz Adeti * Birim Elektrik Tüketimi = Toplam Elektrik Tüketimi*

1.934.889 Adet Antminer S15 * 1.596 Watt = 3.088.082.667 Watt
1.066.163 Adet BitFury B8 * 6.400 Watt = 6.823.444.898 Watt

Watt / 1000 = kWatt

1.934.889 Adet Antminer S15 3.088.082.667 Watt / 1000 = 3.088.083 kW
1.066.163 Adet BitFury B8 6.823.444.898 Watt / 1000 = 6.823.445 kW

*kWat * 24 Saat = Günlük Elektrik Tüketimi*

1.934.889 Adet Antminer S15 3.088.083 kW * 24 = 74.113.984 kWs
1.066.163 Adet BitFury B8 6.823.445 kW * 24 =163.762.678 kWs

2019 Yılı Sanayi için 1kWh Elektrik Ücreti 0,612972 TL = 0,102162 $

*Günlük Elektrik Tüketimi * 1 kWs $ Ücreti = Günlük Elektrik Maliyeti*

1.934.889 Adet Antminer S15 için 74.113.984 kWs * 0,102162 $= 7.571.633 $
1.066.163 Adet BitFury B8 için 163.762.678 kWs * 0,102162 $=16.730.323 $

İlgili teknolojik cihazların elektriksel bakım ve destek maliyetini hesaplayabilmek içinse, dünyanın farklı yerlerindeki terminal ve havuzların bakım ve destek maliyetlerine bakıldığında toplam elektrik maliyetinin minimum %10'u civarında olduğu öngörülmektedir. Hesaplamamızda en alt oran olan %10'nu dikkate alınırsa;

*Elektrik Bakım Maliyeti = Elektrik Maliyeti * 0,10*

1.934.889 Adet Antminer S15 için ; 7.571.633 $ * 0,10 = 757.163 $
1.066.163 Adet BitFury B8 için ; 16.730.323 $ * 0,10 =1.673.032 $

Günlük Elektrik Maliyeti = Elektrik Maliyeti + Elektrik Bakım Maliyeti

1.934.889 Adet Antminer S15 için ; 7.571.633 $ + 757.163 $ = 8.328.796 $
1.066.163 Adet BitFury B8 için ; 16.730.323 $ +1.673.032 $ =18.403.355 $

2018 yılındaki BTC ile BTC Cash arasındaki büyük savaş dikkate alındığında, blok üretim aşamasında diğer terminallere yaklaşabilmek için en az 10 günlük blok üretim süresine ihtiyaç duyulduğu öngörülmektedir. Bu da %51 saldırısını hedeflemiş kişi veya kişilerin en az 10 günlük Elektrik tüketimi gerçekleştirecek olması demektir.

*10 Günlük Elektrik Maliyeti = Günlük Elektrik Maliyeti * 10*

1.934.889 Adet Antminer S15 için ; 8.328.796 $ * 10 = 83.287.961 $
1.066.163 Adet BitFury B8 için ; 18.403.355 $ * 10 =184.033.549 $

Toplam Maliyet = Toplam Cihaz Maliyeti + 10 Günlük Elektrik Maliyeti

1.934.889 Adet Antminer S15 için ; 4.022.401.813 + 83.287.961 = 4.105.689.775 $
1.066.163 Adet BitFury B8 için ; 2.731.510.286 +184.033.549 = 2.915.543.835 $

Şuan piyasada olan 2 farklı cihaz seçerek cihaz başına maliyetleri hesapladık. 2 Cihazının ortalamasını alarak ortalama bir Maliyet hesabı gösterilebilir.

Ortalama Maliyet = (Antminer S15 Maliyeti + BitFury B8 Maliyeti) / 2

Ortalama Maliyet ($) = (4.105.689.775 + 2.915.543.835) / 2 = **3.510.616.805 $**
Ortalama Maliyet (TL) = 3.510.616.805 * 6 (1 Usd =6 TL) = **21.063.700.829 TL**

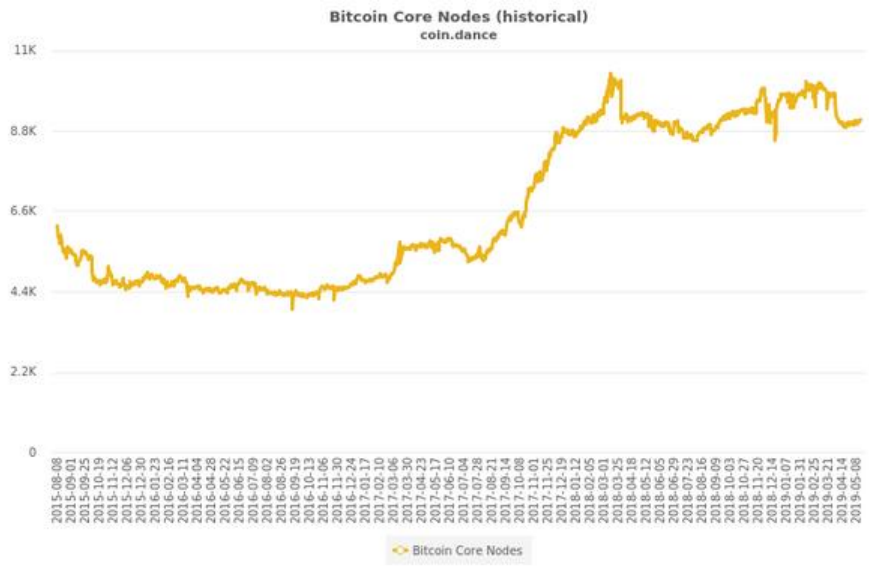
Yukarıda hesaplaması yapılan BTC ağındaki %51 saldırısı için gerekli minimum sabit cihaz maliyetlerini ve bunlara bağlı değişken maliyetlerini gösteren değerlere Tablo 5'te gösterilmiştir.

Tablo 5: BTC Ağında %51 Saldırısı İçin Gerekli Minimum Maliyet Tablosu

Ağ HashRate 52.242.000 TH/s	**Antminer S15 27Th** HashRate : 27 TH/s EnerjiTüketim: 1.596 W Fiyat : 1.704 $	**BitFury B8** HashRate : 49 TH/s EnerjiTüketim: 6.400 W Fiyat : 2.100 $
Gereken Cihaz Adeti	1.934.889	1.066.163
Cihaz Maliyeti ($)	3.297.050.667	2.238.942.857
Cihaz Yerleşim Maliyeti ($) (%22)	725.351.147	492.567.429
Toplam Sabit Maliyet	**4.022.401.813**	**2.731.510.286**
Elektrik Maliyeti ($)	7.571.633	16.730.323
Elektrik Bakım Maliyeti ($) (%10)	757.163	1.673.032
Toplam Değişken Maliyet (Günlük)	**8.328.796**	**18.403.355**
Toplam Değişken Maliyet (10 Günlük)	**83.287.961**	**184.033.549**
%51 Saldırısı için Minimum Toplam Maliyet ($)	4.105.689.775	2.915.543.835
%51 Saldırısı için Minimum Toplam Ortalama Maliyet ($)	**3.510.616.805**	
%51 Saldırısı için Minimum Toplam Maliyet (TL)	24.634.138.647	17.493.263.010
%51 Saldırısı için Minimum Toplam Ortalama Maliyet (TL)	**21.063.700.829**	

BTC blok zincir ağının hash rate değerinden yola çıkarak, %51 saldırısının gerçekleşebilmesi için gerekli olan maliyet analizi gösterilmiştir.

Zincirdeki blok sayısının uzunluğu ve sistemde bulunan blok üreticisi ve onaylayıcısı terminal sayıları da %51 riskine karşı destekleyici önlemler olarak değerlendirilmektedir.



Şekil 17: BTC ağındaki Terminal Sayısı

Şekil 16'da BTC blok zincirinde blok üreticisi ve onaylayıcısı olarak bulunan terminal sayısını göstermektedir. Bu sayı bugün itibariyle 10.000'lere yaklaşmaktadır ki aynı blok zincirine sahip aynı datayı tutan ve sistemin var olmasını destekleyen cihaz sayısıdır.

Bitcoin Blockchain Statistics

Statistic	Value
# of Blocks Mined	**576,807** (17,710,088 BTC)
Days Since Creation (first block)	**3,788** (2009-01-03)
Size	**227.77 GB** (+0.04% today)

Şekil 18: BTC blok zincir istatistikleri

Şekil 17'da 3 Ocak 2009 tarihinden günümüze kadar BTC blok zincirine ait istatistikler görülmektedir. Üretilen blok sayısı 576.807 olup , tüm blok zincirin boyutu da 277,77 GB erişmiştir. Blok zincirin bu uzunluğu da dayanıklılık açısından önemli bir göstergedir.

SONUÇ

Bu çalışmada teknoloji ve finans dünyasının yeni nesil kavramlarından "Blok Zincir" teknolojisi, başta teknik ve terminolojik olmak üzere birçok açıdan ele alınmıştır. Son 10 yılda olduğu kadar gelecek yıllarda da adından fazlasıyla söz ettirecek seviyede yeni blok zincir uygulamalarının farklı alanlarda kullanılabileceği anlatılmıştır.

Her sistemin olduğu gibi blok zincir sisteminin de teknik anlamda problem oluşturan konularından bahsedilmiştir. Bu konuların en önemlisi ve blok zincirlerin korkulu rüyası olan "%51 Sorununun", küçük blok zincir ağları için ciddi bir problem olabildiği, bunun yanında bugün on binlere yaklaşan blok zincir yapılarından birincisi ve en büyüğü olan Bitcoin ekosistemi üzerinde gerçekleşme olasılıkları değerlendirilmiştir.

"BTC'de %51 Matematiği" isimli çalışmamda elde edilen hesaplamalarıma göre, bugün itibariyle 8.000 Doları bulan birim fiyatı, 141 Milyar Doları aşan pazar değeri, 52 EH/s'lik hashrate oranı, 10 bine yaklaşan terminal sayısı ile Bitcoin'in %51 saldırısı görebilmesi için sadece "Donanım + Elektrik + Bakım" masrafları dahil minimum 3,5 Milyar Dolara (21 Milyar TL ye) ihtiyaç duyulduğu gösterilmiştir.

Yeni bir blok zincir yapısı kurma, mevcutta olan bir blok zincir yapısına dahil olma veya yatırım yaparken %51 sorunsalı açısından ne gibi detaylara dikkat edilmesi gerektiği aşağıda belirtilmiştir.

- Geniş katılımlı blok zincir ağ yapılarının olması
- Terminallerin merkezi olmayan dağıtık yapıda olmaları
- Blok üretim ve işlem onay mekanizmasında onay sayısının çok olması
- Blok zincir boyutunun uzun olması
- Ağ hashrate oranının yüksek seviyede bulunması

Bu çalışmamın sonunda elde edilen çıkarım, BTC ağının çok büyük olması, katılımcı sayısının çok fazla olması, ağ hashrate değerinin yüksek olması sebebiyle

ağ üzerinde %51'lik gücü elde edebilmek için ciddi maliyet gerektirdiği ve hakimiyet olasılığının oldukça düşük olduğudur.

Tüm bunlardan dolayı BTC her türlü saldırıya karşı çok dayanıklıdır ve blok zincirleri arasında en güvenli ve güvenilir şifrelenmiş para birimi olarak kabul görmektedir.

KAYNAKÇA

[1] Güleç, T. C. 2018, "Blockchain tabanlı kripto para birimlerinin mevcut durumuna dair finansal analizler ve geleceği", Manisa Celal Bayar Üniversitesi / Sosyal Bilimler Enstitüsü, Doktora Tezi, Manisa.

Aldemir, M. 2018, "Elektronik para ve Blockchain'in finansal yönetim üzerine etkileri", Maltepe Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul.

Durbilmez, S. E. 2018, "Blockchain teknolojisinin finans sektöründeki yeri ve uygulamaları", Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul.

Aslan, A. 2018, "Kripto para olgusu ve Blockchain teknolojisi: Ekonomik aktörlerin tepkisi, maliyet analizi, Var modeli ve Granger nedensellik testi", Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara.

Çetin, S. C. 2018, "Blockchain protokolü geliştirilmesi ve bu protokol üzerinde dijital değer transferi ortamı oluşturulması", Bahçeşehir Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, İstanbul.

Karaköse, İ. S. 2017, "Elektronik ödemelerde blok zinciri ve sistematiği ve uygulamaları", Erciyes Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Kayseri.

[2] Google Scholar - https://scholar.google.com.tr/. Erişim Tarihi: 8 Nisan 2019.

ScienceDirect - https://www.sciencedirect.com/. Erişim Tarihi: 8 Nisan 2019.

JStor - https://www.jstor.org/. Erişim Tarihi: 8 Nisan 2019.

Springer - https://link.springer.com/. Erişim Tarihi: 8 Nisan 2019.

[3] YÖK Tez Merkezi - https://tez.yok.gov.tr/UlusalTezMerkezi/giris.jsp. Erişim Tarihi: 8 Nisan 2019.

TÜBİTAK ULAKBİLİM Veritabanı - http://ulakbim.tubitak.gov.tr/. Erişim Tarihi: 8 Nisan 2019.

[4] Aydın, M. E. 2018, “Blokzincir Tabanlı Oy Verme Sistemi Önerisi”, Necmettin Erbakan Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Konya.

[5] Bozkurt, A., & Uçar, H. (2018). “Yapılandırılmış ve yapılandırılmamış öğrenme süreçlerinde blokzinciri teknolojisi”. Eğitimde FATİH Projesi Eğitim Teknolojileri Zirvesi 2018 (s. 47-53). 2-3 Kasım, Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü (YEGİTEK), Ankara. - researchgate.com

[6] Murathan, T., Murathan F. (2019). “Spor Sektöründe Blok Zinciri Uygulamaları”. Gaziantep Üniversitesi Spor Bilimleri Dergisi, 4(1), 64-74. - dergipark.org.tr

[7] Deloitte, 2015, Blockchain Distrupting the Financial Services Industry https://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/IE_Cons_Blockchain_1015.pdf .

Cognizant, 2016, Blockchain in Banking : A Measured Approach, https://www.cognizant.com/whitepapers/Blockchain-inBanking-A-Measured-Approach-codex1809.pdf .

Everis Next, 2016, 17 Blockchain Disruptive Use Cases, https://everisnext.com/2016/05/31/17-blockchain-disruptiveuse-cases/ .

Evans, C. W. 2015, Bitcoin in Islamic Banking and Finance, Journal of Islamic Banking and Finance, 3(1), 1-11.

[8] Tapscott, Don (10 May 2016). "The Impact of the Blockchain Goes Beyond Financial Services". Harvard Business Review. Erişim tarihi: 16 Nisan 2019.

[9] “UBS leads team of banks working on blockchain settlement system”. Reuters. 24 August 2016. Erişim tarihi: 16 Nisan 2019.

“Cryptocurrency Blockchain”. capgemini.com. 5 December 2016. Erişim tarihi: 16 Nisan 2019.

[10] "First Government Blockchain Implementation For Russia". Cointelegraph. 22 December 2017. Erişim Tarihi: 16 Nisan 2019.

[11] Allison, Ian (3 May 2016). "Deloitte to build Ethereum-based 'digital bank' with New York City's ConsenSys". International Business Times. Erişim tarihi: 16 Nisan 2019.

[12] Allison, Ian (20 January 2016). "R3 completes trial of five cloud-based blockchain technologies at 40 banks". International Business Times. Erişim tarihi: 16 Nisan 2019.

[13] Andrew Quentson (11 September 2016). “Swiss Industry Consortium to Use Ethereum's Blockchain” . Erişim tarihi: 16 Nisan 2019.

[14] "MasterCard pushes ahead into blockchain tech". Business Insider. 2 November 2016. Erişim tarihi: 16 Nisan 2019.

[15] “CLS Group Launches Blockchain-Based Payment Netting Service”. 28 November 2018. Erişim tarihi: 16 Nisan 2019.

[16] "World's Fastest Blockchain Tested in Australia". 15 November 2017. Erişim tarihi: 16 Nisan 2019.

"Mastercard Seeks Patent for Instant Blockchain Payments Processing". 14 November 2017. Erişim tarihi: 16 Nisan 2019.

"Swift Blockchain Success Sets Stage for Sibos". 15 November 2017. Erişim tarihi: 16 Nisan 2019.

[17] "First cryptocurrency freight deal takes Russian wheat to Turkey". Bloomberg.com. 23 January 2018. Erişim tarihi: 16 Nisan 2019.

"Commodities Shipper Seeks $150 Million to Start Digital Coin". Bloomberg.com. 20 February 2018. Erişim tarihi: 16 Nisan 2019.

ICO Market Quarterly Analysis (2019- Q1)- https://icobench.com/ico/prime-shipping-foundation. Erişim tarihi: 16 Nisan 2019.

[18] "Tech Tent: Social giants get grilled". BBC. 3 November 2017. Erişim tarihi: 17 Nisan 2019.

"Using blockchain to fight fake news is the most 2017 thing ever". The Next Web. 23 October 2017. Erişim tarihi: 17 Nisan 2019.

[19] "Level One Project". Bill & Melinda Gates Foundation. 30 April 2017. Erişim tarihi: 17 Nisan 2019.

Woyke, Elizabeth (18 April 2017). "How Blockchain Can Bring Financial Services to the Poor". MIT Technology Review. Erişim tarihi: 17 Nisan 2019.

[20] Chavez-Dreyfuss, Gertrude (16 June 2016). "Sweden tests blockchain technology for land registry". Reuters. Erişim tarihi: 17 Nisan 2019.

[21] Shin, Laura (21 April 2016). "Republic Of Georgia To Pilot Land Titling On Blockchain With Economist Hernando De Soto, BitFury". Forbes. Erişim tarihi: 17 Nisan 2019.

[22] "Indian State Uses Blockchain Technology to Stop Land Ownership Fraud". Erişim tarihi: 17 Nisan 2019.

[23] Snow, Matt(19 October 2017). "How I sold 5 acres of land using BitBay's blockchain based smart-contracts" Erişim tarihi: 17 Nisan 2019.

[24] Meyer, David (20 October 2017). "Russia experiments with using blockchain tech for land registry: Pilot project uses blockchain in Moscow". ZDNet. Erişim tarihi: 17 Nisan 2019.

[25] Friedman, Sara (21 September 2017). "GSA looks to blockchain for speeding procurement processes". Government Computer News. Erişim tarihi: 17 Nisan 2019.

[26] "Tunisia To Replace eDinar With Blockchain-Based Currency". EconoTimes. 11 January 2016. Erişim tarihi: 17 Nisan 2019.

[27] "Senegal To Introduce A New Blockchain-Based National Digital Currency, The Second Such Currency In The World". iAfrikan News. 24 November 2016. Erişim tarihi: 17 Nisan 2019.

[28] "Akbank, Ripple ağı üzerinden para transferlerine başladı". Uzmancoin Haber Sitesi. 14 Aralık 2018. Erişim tarihi: 18 Nisan 2019.

"Ripple bugün resmen Akbank Direkt'e geldi". Uzmancoin Haber Sitesi. 22 Aralık 2018. Erişim tarihi: 18 Nisan 2019.

[29] Demirel, Fırat (18 Ekim 2017). "Webrazzi Arena 2017'nin kazananı blockchain tabanlı dijital kimlik girişimi Kimlic oldu!". webrazzi.com. Erişim tarihi: 18 Nisan 2019.

[30] "Türkiye'nin ilk Blockchain projesi BBN... BKM Genel Müdürü Dr. Soner Canko anlatıyor". TurkishTime Dergisi. 27 Aralık 2017. Erişim tarihi: 18 Nisan 2019.

[31] Demirel, Fırat (21 Kasım 2017). "TÜBİTAK'tan blok zincirine özel araştırma laboratuvarı". webrazzi.com. Erişim tarihi: 18 Nisan 2019.

[32] Wikipedi

https://tr.wikipedia.org/wiki/Blok_zinciri

[33] Binance Academy

https://www.binance.vision/tr/blockchain/

[34] Ünsal E., Kocaoğlu Ö. (Ağustos 2018). "Blok Zinciri Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri". Avrupa Bilim ve Teknoloji Dergisi.

[35] "Blokzincir potansiyelinin keşfi". 2018 Yılı Türkiye Blokzincir Araştırması. Deloitte.com

[36] Bankalararası Kart Merkezi

https://bkm.com.tr/blok-zinciri-blockchain-nedir/

[37] Blockgeeks

https://blockgeeks.com

[38] Blockchain

https://www.blockchain.com

ÖZGEÇMİŞ

14 Haziran 1980 Almanya doğumluyum. İlk ve Orta öğrenimimi Balıkesir'in Erdek ilçesinde tamamladım. 1998 yılında Bandırma Şehit Mehmet Gönenç Süper lisesinden, 2003 yılında Ege Üniversitesi Tekstil Mühendisliğinden mezun oldum. Bilişim ve Teknoloji merakımdan dolayı bu sektöre girip ERP Danışmanlığı, İş Analistliği, Veri tabanı Yönetimi, Yazılım Geliştirme alanlarında 16 yıldır çalışmaktayım.

2015 yılında Beykent Üniversitesi Bilgisayar Mühendisliği Anabilim Dalında yüksek lisans eğitimine başladım.

Özel ilgi alanlarım; su sporları, tarih, farklı dil ve kültürler öğrenmektir.

Ali Osman TİKVEŞLİ