



T.C.

ALTINBAŞ ÜNİVERSİTESİ

Lisansüstü Eğitim Enstitüsü

Elektrik ve Bilgisayar Mühendisliği

KRİPTO PARA MADENCİLİĞİ

Murat AYKAÇ

Yüksek Lisans Tezi

Danışman

Dr. Öğr. Üyesi Oğuz KARAN

İstanbul, 2022

KRİPTO PARA MADENCİLİĞİ

Murat AYKAÇ

Elektrik ve Bilgisayar Mühendisliği

Yüksek Lisan Tezi

ALTINBAŞ ÜNİVERSİTESİ

2022

Murat AYKAÇ tarafından hazırlanmış ve 27.02.2022 tarihinde sunulmuş KRIPTO PARA MADENCİLİĞİ başlıklı tez Elektrik ve Bilgisayar Mühendisliği Anabilim Dalında Yüksek Lisans Tezi olarak **oy birliği** ile kabul edilmiştir.

Dr. Öğr. Üyesi Oğuz KARAN

Danışman

Tez Savunma Sınavı Jüri Üyeleri:

Dr. Öğr. Üyesi Oğuz KARAN

Mühendislik ve Mimarlık
Fakültesi

Altınbaş Üniversitesi

Dr. Öğr. Üyesi Sefer KURNAZ

Mühendislik ve Mimarlık
Fakültesi,

Altınbaş Üniversitesi

Dr. Öğr. Üyesi Serdar KARGIN

Mühendislik ve Mimarlık
Fakültesi,

Beykent Üniversitesi

Bu tezin Yüksek Lisans tezi olarak bütün şartları sağladığını beyan ederim.

Tezin Lisansüstü Eğitim Enstitüsüne teslim tarihi: ____/____/____

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

Murat AYKAÇ

İmzası

İTHAF

Bu tez çalışmasını değerli fikirleri ve tecrübeleriyle yönlendiren sayın danışman hocam Dr. Öğr. Üyesi Oğuz KARAN'a ithaf ediyorum.



ÖNSÖZ

Çalışmamda desteğini her zaman hissettiğim danışman hocam Dr. Öğr. Üyesi Oğuz KARAN'a teşekkür ederim.



ÖZET

KRİPTO PARA MADENCİLİĞİ

AYKAÇ, Murat

Yüksek Lisans Tezi, Elektrik ve Bilgisayar Mühendisliği, Altınbaş Üniversitesi

Danışman: Dr. Öğr. Üyesi Oğuz KARAN

Tarih: Mart/2022

Sayfa: 112

Ekonomik hayatın temelini oluşturan takas işlemleri geçmişten günümüze değişim geçirmiştir. Nakit kullanımı her geçen gün azalırken, kredi ve banka kartı kullanımı da hızla artmıştır. Sonuç olarak, çoğu takas işlemi dijital olarak gerçekleştirilmektedir. Ödeme araçlarındaki değişiklikler devam etmekle birlikte çek vb. araçlar kredi kartlarında ve banka kartlarında yerini almıştır. Ancak dijital para olarak da bilinen elektronik para sistemlerinin kullanımı hızla artmaktadır. E-para olarak tanımlanan dijital para birimlerinin son örneği kripto para birimleridir. Kripto para birimleri, kullanıcıların herhangi bir otoriteye bağlı olmadan özgürce ticaret yapmalarını sağlamaktadır. Kripto para teknolojisindeki yenilikler, çeşitli sağlık ve bankacılık uygulamalarında kullanılmaktadır. Ödeme araçlarındaki değişimin devam edeceği ve bu değişimin finansal piyasalar ve kullanıcı alışkanlıkları üzerinde önemli bir etkisi olacağı söylenebilir. Elektronik ortama iletilen ödemelerin güvenliğinin ve devamlılığının gelecekte çok daha önemli olacağına inanılmaktadır.

Bu bağlamda çalışmanın amacı, kripto para madenciliği uygulamalarını inceleyerek özellikle günümüzde bu konuda yapılan yenilikçi çalışmaların ve mühendislik uygulamalarının değerlendirilmesidir.

Anahtar Kelimeler: Dijital Para, E-Ödeme, Kripto Para Madenciliği, Bitcoin, Madencilik Teknolojileri.

ABSTRACT

CRYPTO CURRENCY MINING

AYKAÇ, Murat

Master Thesis, Electrical and Computer Engineering, Altınbaş University,

Supervisor: Ass. Prof. Dr. Oğuz KARAN

Date: March/2022

Pages: 112

In the course of technological development, money has changed as a means of payment. The financial markets have been hardest hit by the rapid advances in technology today. As a result of these developments, the barter transactions that form the basis of economic life have shifted from the past to the present. As the use of cash is decreasing day by day, the use of credit and debit cards is increasing rapidly. As a result, most swap transactions take place digitally. Changes in payment instruments continue. check, etc. Tools have left their place in credit cards and debit cards. However, the use of electronic money systems, also known as digital money, is increasing rapidly. The final example of digital currencies defined as e-money is cryptocurrencies like bitcoin. Cryptocurrencies allow users to trade freely without being tied to any authority. It is predicted that such digital currencies will seriously affect the tax systems of states in the future. Innovations in cryptocurrency technology are used in various healthcare and banking applications. It is clear that the change in payment instruments will continue and that this change will have a significant impact on financial markets and user habits. It is believed that the security and continuity of the payments transmitted into the electronic environment will be much more important in the future.

Accordingly, the aim of the study is to examine the applications of cryptocurrency mining and to evaluate the innovative studies and engineering applications especially today.

Key Words: Digital Currency, E-Payment, Mining, Bitcoin, Mining Technologies.

İÇİNDEKİLER

Sayfa

ÖZET	vii
ABSTRACT	viii
İÇİNDEKİLER.....	ix
TABLO LİSTESİ.....	xiv
ŞEKİL LİSTESİ	xv
KISALTMALAR.....	xvii
1. GİRİŞ	1
2. PARA VE KRİPTO PARA	3
2.1. PARAYA KAVRAMSAL YAKLAŞIM	3
2.1.1. Para Kavramı	3
2.1.2. Paranın Gelişimi	3
2.1.3. Paranın Özellikleri	4
2.1.4. Paranın İşlevleri	4
2.1.5. Para Çeşitleri	5
2.1.5.1. Mal para	5
2.1.5.2. Altın ve gümüş	6
2.1.5.3. Temsili para	6
2.1.5.4. İtibari para (fiyat para)	6
2.1.5.5. Elektronik para	7
2.1.5.6. Dijital para	8
2.1.5.7. Sanal para	8
2.2. KRİPTO PARA	9
2.2.1. Kripto Para Kavramı	9
2.2.2. Kripto Paraların Tarihsel Gelişimi	9

2.2.3. Kripto Paraların Genel Özellikleri	10
2.2.4. Kripto Para İşlemleri	12
2.2.5. Kripto Paraların Muhasebeleştirilmesi	13
3. BİTCOİN ANALİZİ VE BLOKZİNCİR TEKNOLOJİSİ	14
3.1. BİTCOİN ANALİZİ	14
3.1.1. Bitcoin'in Teorik Temelleri	14
3.1.2. Peer To Peer Network Ağı (P2P)	14
3.1.3. Bitcoin'in ve Paranın Özelliklerinin Karşılaştırılması	15
3.1.4. Bitcoin'in Özellikleri	16
3.2. BLOKZİNCİR TEKNOLOJİSİ	18
3.2.1. Blokzincir Yapısının Oluşumu ve Fonksiyonları	18
3.2.2. Bitcoin Transfer İşlemlerini "Hash" Haline Getirmek	18
3.2.3. Bitcoin Transfer İşlemlerinin İmzalanması	20
3.2.4. Bitcoin İşlemlerinin Görünümü	22
3.2.5. Blokzincir Yapısının Bileşenleri	23
3.2.5.1. Sürüm	26
3.2.5.2. Önceki bloğun hash'i	26
3.2.5.3. Merkle ağacı kökü	26
3.2.5.4. Zaman damgası	27
3.2.5.5. Proof of work (İş ispatı)	27
3.2.5.6. Nonce değeri	28
3.2.6. Yetim Bloklar	29
3.2.7. Blokzincirde "Fork"lanma (Çatallanma)	29
3.2.8. Mining (Madencilik)	31
3.3. BİTCOİN CÜZDANI VE SANAL PARA TRANSFERİ	34
3.3.1. Bitcoin Temini	37

3.4. BITCOİN İLE İLGİLİ FİNANSAL VE TEKNİK ELEŞTİRİLER	38
3.4.1 .Bitcoin'in Avantajları ve Dezavantajları	39
3.4.1.1. Bitcoin'in avantajları	39
3.4.1.2. Bitcoin'in dezavantajları	39
4. ALTCOİNLERİN KRİPTO PARA PİYASASINDAKİ YERİ	41
4.1. KRİPTO PARALAR İÇERİSİNDE ALTCOİNLER	41
4.1.1. Litecoin (LTC)	43
4.1.2. Ethereum	44
4.1.2.1. Akıllı kontratlar (smart contracts)	44
4.1.2.2. Akıllı kontratların kullanım alanları	45
4.1.2.3. Ethereum ile bitcoin arasındaki benzerlikler ve farklar	46
4.1.3. EOS	49
4.1.4. Ripple (XRP)	50
5. KRİPTO PARA MADENCİLİĞİ VE UYGULAMALARI	51
5. 1. KRİPTO PARA MADENCİLERİNİN GÖREVİ	52
5. 2. MADENCİLİK ÇEŞİTLERİ	52
5. 2. 1. Ekran Kartı ile Madencilik	52
5. 2. 2. Bulut Madenciliği	53
5. 2. 3. Madencilik Havuzları	54
5. 3. MADENCİLİK ONAY İŞLEMİ	55
5. 3. 1. Emek İspatı (PoW)	55
5. 3. 2. Pay Kanıtı (PoS)	56
5. 4. MADENCİLİK ÜCRETLERİ (MINING FEES)	57
5. 5. MADENCİLİK CİHAZLARI	57
5. 5. 1. GPU Ethereum Madencilik Cihazı ve RİG	57
5. 5. 2. ASIC Bitcoin Madencilik Cihazı	58

5.6. KRİPTO PARA MADENCİLİĞİ UYGULAMALARI	59
5.6.1.Yeni Bitcoin	60
5.6.2.Bitcoin İşlemleri Doğrulama	61
5.6.3.Madencilik Analogisi	61
5.6.4.Bitcoin ve Geleneksel Currencies	62
5.6.5.Madencilğin Tarihçesi	63
5.6.6.Gelişen Evrim	64
5.6.7.Ödüllendirme Bitcoin Madencileri	64
5.6.8.Bitcoin Fiyatı	65
5.6.9.Yatırımlarla Artan Riskler	67
5.6.10.Düzenleyici Risk	68
5.6.10.1.Güvenlik riski	68
5.6.10.2.Sigorta riski	69
5.6.10.3.Dolandırıcılık riski	69
5.6.10.4.Pazarlama riski	69
5.7. KRİPTO PARA MADENCİLİĞİNDE TERMODİNAMİK SÜREÇ	70
5.7.1. İşlemciler	71
5.7.2. Veri Merkezi Boyutu	72
5.7.3. Veri Merkezi Yerleştirme Konuları	74
5.7.4. Veri Merkezi Enerji Verimliliği	76
5.7.5. Verimlilik Ölçümleri	79
5.7.5.1. PUE	79
5.7.5.2 ERE	82
5.7.5.3 ERF	83
5.7.6. Veri Merkezlerinde Verimlilik Optimizasyonu	83
5.7.7. Veri Merkezi Enerji Tasarrufu	84

5.7.7.1. Çalışma sıcaklıkları	84
5.7.7.2. Serbest soğutma	85
5.7.8. Isının Yeniden Kullanımı	87
5.7.9. Bitcoin Madenciliğinde Termodinamik Süreç	89
SONUÇ	91
REFERANSLAR	94



TABLO LİSTESİ

	<u>Sayfa</u>
Tablo 2.1: En Çok Kullanılan Kripto Paraların Piyasa Değerleri	11
Tablo 3.1: Blokzincir Yapısının Açıklaması	24
Tablo 3.2: Blok Başlığı Açıklaması	25
Tablo 4.1: Piyasa Değerine Göre Sıralanmış Kripto Para Birimleri	41
Tablo 5.1: Veri Merkezi Taksonomisi	70
Tablo 5.2: Veri Katmanı Sınıflandırılması	71
Tablo 5.3: PUE Verimliliği	77
Tablo 5.4: Verimlilik Senaryoları için PUE ve Artıklık Değerleri	77
Tablo 5.5: Sıcaklık ve Bağlı Nem Verileri ile Coğrafi İmar	81
Tablo 5.6: 2011 Veri Merkezleri için ASHRAE Termal Yönergeleri	82

ŞEKİL LİSTESİ

Sayfa

Şekil 2.1: Altın ve Gümüş Para Görselleri	6
Şekil 2.2: İtibari Para Görselleri	7
Şekil 2.3: Elektronik Paranın İşleyişi	8
Şekil 2.4: Kripto Paraların Dünya Pazarındaki Payları	11
Şekil 2.5: Blokların Gösterimi	12
Şekil 3.1: Network (İletişim Ağı) Çeşitleri	15
Şekil 3.2: Blokzincir Görseli	18
Şekil 3.3: Bloktaki işlemlerin “Hash” Uygulamasından Geçirilmesi	20
Şekil 3.4: Bitcoin İşlem Süreci	21
Şekil 3.5: Bitcoin Transfer İşlemi	22
Şekil 3.6: Bitcoin ile Ödeme Yaparak Tatlı Yemek İsteyen Müşterinin İşlemi	23
Şekil 3.7: Blokzincir Yapısı	24
Şekil 3.8: Blok Başlığı	25
Şekil 3.9: Merkle Ağacı’nın Yapısı	26
Şekil 3.10: Blokzincirde İş İspatının Gösterimi	29
Şekil 3.11: Yetim Bloklar	30
Şekil 3.12: Gönüllü Çatallanma (Soft Forking)	30
Şekil 3.13: Zorunlu Çatallanma (Hard Forking)	30
Şekil 3.14: 2009-2021 Yılları Arasında Madencilere Ödenen İşlem Ücretlerinin Toplam Değeri	31
Şekil 3.15: Toplam Bitcoin Sayısı	33
Şekil 3.16: Bitcoin Elektronik Cüzdan	34
Şekil 3.17: Bitcoin Kâğıt Cüzdan	35
Şekil 3.18: Bitcoin Cüzdanı Kullanıcı Sayısı	35

Şekil 3.19: Bitcoin ATM'si	36
Şekil 4.1: LTC/USD Fiyat Grafiği	42
Şekil 4.2: Ethereum/Bitcoin Fiyat Grafiği (Son 5 Yıl)	46
Şekil 4.3: ETH/USD Fiyat Grafiği (Son 5 Yıl)	47
Şekil 5.1: Enerji Tasarrufu Çerçevesi	75
Şekil 5.2: Sıcak Koridor/Soğuk Koridor Dolabı Konfigürasyonu	81



KISALTMALAR

ATM : Automated Teller Machine(Otomatik Para Çekme Makinesi)

PIN : Personal Identification Number(Kişisel Tanımlama Numarası, Şifre)

API : Application Programming Interface (Uygulama Programlama Arayüzü)

SDK : Software Development Kit(Yazılım Geliştirme Aracı)

POC : Proof of Concept(Kavramın İspatı)

BTC : Bitcoin Currency(Bitcoin Para Birimi)

ETH : Ethereum Currency(Ethereum Para Birimi)

EVM : Ethereum Virtual Machine(Ethereum Sanal Makinesi)

POW : Proof Of Work(İşin Kanıtı, Bir mutabakat yöntemi)

POS : Proof Of Stake(Bahisin Kanıtı, Bir mutabakat yöntemi)

PBFT : Practical Byzantine Fault Tolerance(Pratik Bizans Hata Toleransı)

NSA : National Security Agency(Ulusal Güvenlik Ajansı)

CIA : Central Intelligence Agency (Merkezi İstihbarat Teşkilatı)

Quintillion : Kentilyon(19 haneli sayı, Bin katrilyon)

GB : Gigabyte(1 Byte = 8 Bit, 1 Gigabyte = 1073741824 Bytes)

WGC : World Gold Council (Dünya Altın Konseyi)

GPS : Global Positioning System(Küresel Yer Belirleme Sistemi)

TOR : The Onion Routing(Anonim İletişim İmkânı Sağlayan Ağ ve Yazılım)

IRS : Internal Revenue Service(Gelir İdaresi, Amerika)

CFTC : Commodity Futures Trading Commission(Amerika Emtia Vadeli İşlemler Komisyonu)

1. GİRİŞ

Takas ile başlayan ticaret, paranın icadıyla daha kolay ve kabul edilebilir bir platforma yerleşmiştir. Mal ve hizmet alımı karşılığında ödeme yapmak, insanların yüz yıllardır devam ettirdikleri ticaretin vazgeçilmez kuralları arasında yer almaktadır. İnsanlar alışverişlerini kolaylaştırmak için sürekli farklı fiziki ürünleri, nesneleri takas olarak kullanmışlardır [1].

Paranın icadıyla ticaret daha hızlı bir boyuta geçmiştir. Para, geçmişten günümüze mal ve hizmetlerin satın alımında kullanılan, üzerinde değeri yazılı olan kâğıt ya da metal nesnedir. Alım satım işlemlerinin basit ya da kompleks her alanında kullanılan para, günümüze kadar değişim aracı olma özelliğini yitirmemiştir. Para, geçmişten günümüze değişik görüntülerde ve değerlerde, insanların mal ve hizmet alımında insanlara eşlik etmiştir. Kâğıt paradan önce alım satım işlemlerinde değişim aracı olarak altın, gümüş gibi kıymetli varlıklar kullanılmaya başlanmıştır. Zamanla madeni paradan daha kolay kullanım özelliklerine sahip kâğıt para piyasalarda kabul görmeye başlamıştır. Para, insanların hayatında teknolojiyle birlikte aynı amaç ve farklı kullanım biçimleri şeklinde var olmaya devam edecektir [2].

Teknolojik gelişmeler insanları her alanda yeniliklerle buluşturmaktadır. Kredi kartları, bilgisayar ya da mobil telefonlarla elektronik ödeme kolaylıklarından sonra son zamanlarda adını dijital ortamlarda kullanımıyla duyuran kripto (şifreli) paralar, alışılmış kâğıt paraların aksine fiziksel yapısı olmayan, herhangi bir merkez bankası ya da otorite tarafından basılamayan ve müdahale edilemeyen sanal paralardır.

Kripto paraların içinde kendinden en çok söz ettiren Bitcoinler, alım satım işlemlerinin dijital altyapı üzerinden gerçekleştiği internet bağlantısı ile insanlara ödeme olanağı sağlayan sanal para çeşididir. Bitcoinler ve altcoinler, blockchain (blokzincir) teknolojisiyle transfer işlemlerinde matematiksel formüller ve güvenilir yazılımı sayesinde; bireylerin, şirketlerin, yatırımcıların dikkatlerini çekmeyi başarmıştır [3]. Bitcoin'in piyasada fiyat dalgalanmaları içerisinde sürüklenmesi insanlar üzerinde güvensizlik etkisi oluştursa da Bitcoin blokzincir teknolojisiyle gelecekteki para ekonomilerinin oluşumuna ışık tutmaktadır. Bitcoin ve altcoinler paranın kullanım platformunu daha teknolojik boyutlara taşımaktadır. Çalışmamızda kripto paralar, Bitcoin ve altcoin üretimi, işlemleri, avantaj ve dezavantajları, blokzincir teknolojisi,

kripto para borsaları ve kripto paraların günümüz ve gelecek para ekonomileri üzerindeki etkileri ve kripto para madenciliği incelenecektir.



2. PARA VE KRİPTO PARA

2.1. PARAYA KAVRAMSAL YAKLAŞIM

2.1.1. Para Kavramı

Türkçe'ye “parça” anlamındaki Farsça “pâre”den geçen para kelimesi; Türk Dil Kurumu tarafından yayınlanan Türkçe sözlükte devletçe bastırılan, üzerinde değeri yazılı kâğıt veya metalden ödeme aracı anlamına gelmektedir [4].

Para kelimesine ilişkin anlamlar ile iktisatçıların paraya yükledikleri anlam arasında farklılıklar bulunmaktadır. Günlük konuşma dilinde para sözcüğü birçok anlama gelmektedir. İnsanların çoğu “para” dediğinde aslında banknot veya madeni bozukluğu kastetmektedir. İnsanların para olarak kastettiği kavramı iktisatçılar nakit olarak ifade etmektedir. İktisatçılar için para kavramı özel bir anlam taşımaktadır. Paranın iktisat literatürüne göre taşıdığı anlam “satın alınan mal ve hizmetlerin bedelinin karşı tarafa aktarılmasında ya da borçların geri ödenmesinde genel kabul gören her şey” biçimindedir. Yani para sadece nakit olarak tanımlandığında iktisatçılar için çok dar bir anlam ifade etmektedir [5].

Bir nesnenin para niteliği kazanabilmesi için o nesnenin ödeme aracı olarak görülmesi ve halk tarafından da kabul edilmesi gerekmektedir. Bir ekonomide belirli bir dönemde para olarak kullanılan nesne, zaman içerisinde para olarak kabul edilmeyebilir. Ayrıca bir toplumda para olarak kabul edilen bir ödeme aracı, başka bir toplumda aynı şekilde kabul görmeyebilir. Dolayısıyla para, zaman içerisinde farklı anlamlar kazanabilen, zamana ve mekâna göre değişim gösterebilen bir kavramdır [6].

Tarihi süreç içerisinde para, dinamik bir yapıya sahip olmuştur ve bu sebeple paranın tek ve kesin bir tanımı bulunmamaktadır. Örneğin çok önceleri para olarak kabul edilemeyen unsurlar (Bitcoin ve diğer kripto paralar gibi) günümüzde teknoloji sayesinde para olarak değerlendirilmektedir [7].

2.1.2. Paranın Gelişimi

Para icat edilmeden önce insanlar değişik nesneleri, malları değişim aracı olarak kullanmışlardır. Bazı gayrimenkuller değer saklama aracı olarak görülmüş olsa da değişim aracı olmaya çok da müsait olmadığı için insanlar işlerini kolaylaştırmaya yönelik varlıkları kullanmak istemiştir. Para, yıllar boyu farklı kalıplara girmek durumunda kalmıştır; bazen tuz, bazen fil dişi, bazen deniz kabuğu paranın fiziksel yapısını almıştır. İnsanlar güven duydukları ve işlerini kolaylaştıracak para çeşitlerini kullanmaya meyillidir. İşte bu yüzden sanal paraların alışverişlerde ve yatırım amacıyla kullanılmak üzere potansiyeli yüksek görülmektedir [7].

2.1.3. Paranın Özellikleri

Bir değişim aracına para diyebilmek için bazı özellikleri taşıması gerekmektedir.

Öztürk ve Koç [8]'un çalışmasına göre paranın özellikleri aşağıda beş madde halinde açıklanmaktadır.

- i. Taşınabilirlik: Kullanım kolaylığı açısından farklı ödeme noktalarına rahatlıkla götürülebilir olmalıdır.
- ii. Dayanıklılık: Para el değiştirerek kullanıldığı için görünüm olarak da yeterince dayanıklılığa sahip olmalıdır.
- iii. Bölünebilirlik: Para ile az ya da çok her türlü satın alma işleminin yapılabilmesi için daha küçük miktarlara bölünerek paranın dönüştürülebilmesi gerekir.
- iv. Kabul Edilebilirlik (Homojenlik): Para, aynı değeri ifade edecek şekilde, ödemelerin düzgün bir şekilde gerçekleşmesi için her yerde aynı kabulü görmelidir.
- v. Taklit Edilememe: Para, sahte para kullanımının engellenmesi açısından kolay taklit edilemeyen ve herkes tarafından tanınan güvenli bir özelliğe sahip olmalıdır.

2.1.4. Paranın İşlevleri

Paranın üç önemli işlevi bulunmaktadır. Bu işlevler sayesinde alışverişler daha kolay ve sağlıklı yürütülmektedir.

Afşar vd. [9]'nin çalışmasına göre paranın işlevleri aşağıda maddeler halinde açıklanmaktadır.

- i. Mübadele (değişim) İşlevi: Para, mal ve hizmet alımında, mal ve hizmet karşılığının ödenmesini ifade etmektedir. Para, değişim aracı olarak alım satım işlemlerinde mal ve hizmetlerin el değiştirmesini kolaylaştırarak alım satım için harcanan zamanı kısaltmaktadır. Böylece piyasadaki işlemler daha etkin hale gelmektedir.
- ii. Hesap Birimi Olma İşlevi: Paranın mal ve hizmet fiyatlamalarında bir birimi vardır. Hesap birimi olarak para, ekonomide fiyat, ücret ve refah düzeyi gibi değerleri ölçer. Ekonomide hesap birimini yerine getiren bir nesne ya da varlık olmasaydı mal ve hizmetlerin değeri yine mal ve hizmetler cinsinden belirlenecek ve ekonomide etkinsizlik oluşacaktı. Tüm malların fiyatını tek bir para birimi ile ifade ederek ekonomide oluşabilecek etkinsizlik giderilmektedir.
- iii. Değer Saklama İşlevi: Paranın ödemelerde sürdürülebilir bir şekilde kullanılabilmesi için geçmişten geleceğe alım gücünü koruması gerekir. Para kazanıldığı andan harcanıldığı zamana kadar değerini korumalıdır.

Herhangi bir şeyin para olması için, onu ödeme aracı olarak kabul edebilmek ve bu aracın da toplum tarafından kabul görmesi gerekir. Eğer kabul görmezse para olma özelliği olamaz. Para, geçmişten günümüze insanların ihtiyaçlarıyla şekillenmiştir. Örnek vermek gerekirse; para sayılan madenler (altın, gümüş vb.), değerli kâğıtlar, çek, senet, bono, bir karta elektronik ortamda yükleme yapılmış değerler de para olarak kabul edilmektedir. Dolayısıyla fiziksel özelliğinden ziyade paranın insanlar tarafından kabul görmesi önemlidir [7].

2.1.5. Para Çeşitleri

İktisat literatürüne göre para çeşitleri; mal para, altın ve gümüş para, temsili para, itibari para, elektronik para, dijital para ve sanal para başlıkları şeklinde aşağıda açıklanmaktadır.

2.1.5.1. Mal para

Uzun yıllar kullanılmış, altın, gümüş ve petrol; buğday, mısır ve arpa; balık tuz gibi gıda maddeleri, metaller ve madenler gibi alışverişe konu olan malların tamamına mal para denir. Mal para, değerini asıl olarak yapıldığı maddeden almaktadır. Mal para, mal ve hizmetlerin doğrudan değişiminden sonra kullanılmaya başlanmıştır [10].

2.1.5.2. Altın ve gümüş

Altın ve gümüş, temini ve yaygınlığı çok olmayan madenlerdir. Kimyasal olarak erime noktası fazla olmadığından bozuk para ve takı haline getirilmeleri kolaydır. Altın ve gümüş, uzun yıllar alışverişlerde mallara karşılık ödeme aracı ve hesap birimi olarak kullanılmıştır.



Şekil 2.1: Altın ve Gümüş Para Görselleri [11].

2.1.5.3. Temsili para

Merkez Bankası tarafından basılan, altın ve gümüş gibi kıymetli bir karşılığı olan, istendiğinde mal paraya dönüştürülebilen, matbaalarda bastırılan kâğıt sertifikalardır [12].

2.1.5.4. İtibari para (fiyat para)

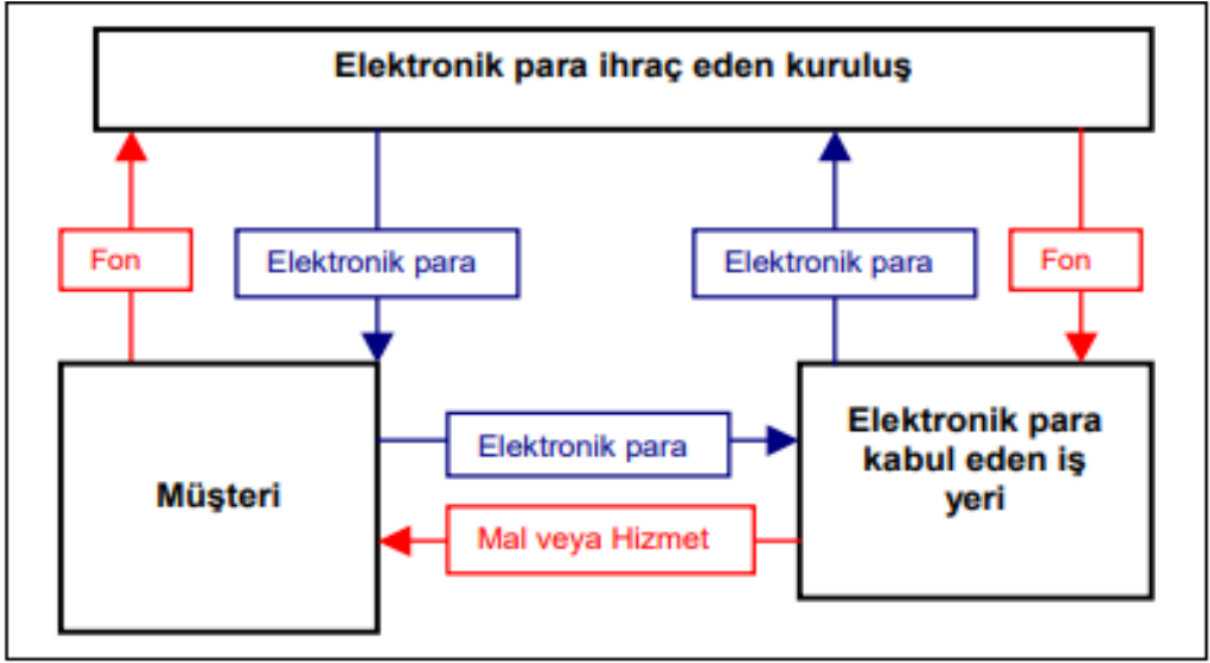
Merkez Bankası gibi resmi otoriteler tarafından çıkarılan, değerli madenler karşılığında basılmayan fakat mal ve hizmet satın alırken tamamen itibari değer ifade eden nesnelere para denilmektedir. Paraların herhangi bir mal olarak değeri olmasa da üzerinde yazan miktar kadar değeri bulunmaktadır. Günümüzde bu sistem yaygın bir şekilde kullanılmaktadır. Kâğıt paraların çalınması ve yüklü miktarının taşınamaması gibi sorunları vardır. Bu sorunları çözmek için paralar bankalarda mevduat hesaplarında saklanabilmektedir. İtibari paralar gücünü resmi otoritelerden almaktadır. Resmi otoriteler paranın taklit edilemeyeceği güvenini sağlamak için her türlü tedbiri almak zorundadır [13], [14].



Şekil 2.2: İtibari Para Görselleri [15].

2.1.5.5. Elektronik para

Elektronik para, Avrupa Birliği'nin açıklamasına göre: elektronik para ihraç eden kuruluşların, bu parayı kullanan tarafların ödediği fonlar (paralar) karşılığı çıkardıkları, elektronik olarak bilgisayarlarda ya da fiziki çipli kartlarda saklanabilen ve ödeme kolaylığı sağlayan parasal değerdir. Mesela elektronik para servisi veren bir bankadan kredi kartı ya da peşin ödemeye bir miktar e-para alındığında banka bu parayı kullanıcı bilgisayarındaki sayısal cüzdana ya da alışverişlerde kullanılabilen fiziksel çipli kartlara tanımlamaktadır. Bu tanımlama fiziken gerçekleşmemiş olup kartların üzerindeki manyetik şeritler ya da çipler aracılığıyla saklanmaktadır. Kullanıcı da bu parayı e-para olarak kabul eden internet sitelerinde, mağaza vb. alışveriş mekânlarında harcayabilmektedir. Bu işlemler kredi kartları ya da bankamatik kartlarıyla yapılan işlemlerle karıştırılmamalıdır. Elektronik kartlar banka kartlarının ikamesi değil onlara yardımcı olabilecek nitelikte kartlardır. Elektronik kartlarla yapılan işlemler de banka nezdinde kontrol altında tutulmakta ve fiziksel olarak para dolaşımı ortadan kalkmış olmaktadır. Banka kartlarında hesaptaki para kullanılırken elektronik kartlarda E-para ihraç eden kuruluşa ödeme yapıldıktan sonra yüklenen küçük tutarlı E-para kullanılmaktadır. E-kartlara en güzel örnekler Akbil ve Ego kartlardır [14].



Şekil 2.3: Elektronik Paranın İşleyişi [16].

Şekil 2.3'e göre elektronik para ihraç eden kuruluş, müşterilerinden aldığı fon karşılığında elektronik para temin etmektedir. Müşteriler E-para kabul eden kuruluşlardan mal ve hizmet satın alıp karşılığını E-para ile ödemektedir. E-para kabul eden kuruluşlar da bu parayı elektronik para ihraç eden kuruluşlara transfer ederek karşılığında fon almaktadır. E-para sonuç itibarıyla insanların bankadaki parası karşılığında bilgisayarlarına yüklenen parayı, alışverişlerde kullanarak hayatlarını kolaylaştırmalarını sağlamaktadır.

2.1.5.6. Dijital para

Elektronik ortamlarda saklanıp gönderilebilen paralardır. İstendiği zaman fiyat paraya çevrilebilir. Banka hesaplarındaki paralar dijital paralara örnektir. Saklanması kolay, taşıma sorunu olmadığı ve kullanımı rahat olduğu için dijital para günümüzde popüler hale gelmiştir. Dijital paralar merkezi otorite tarafından kontrol altındadır [12].

2.1.5.7. Sanal para

Dijital ortamlarda bulunan herhangi bir kuruluş, ulus, devlet, banka tarafından ihraç edilmediği halde bazı durumlarda paranın yerine kullanılabilen paralardır. Dijital paradan farkı, merkezi otorite tarafından basılmamasıdır. Sanal paraya örnek olarak kripto paraları verebiliriz [17].

Ülkelerdeki kıymetlerin toplam karşılığını gösteren kuruluşlar, parayı basan ve yöneten merkez bankalarıdır. Ülkemizde banknot çıkarma yetkisine sahip ilk kurum 4 Şubat 1863 tarihinde kurulmuş olan Osmanlı Bankası'dır. Cumhuriyetin ilanından sonra banknot çıkarma işlemlerini T.C. Merkez Bankası yürütmektedir. Merkez Bankası kâğıt para (banknot) basımını gerçekleştirirken madeni paraların (bozuk para) basımı Maliye Bakanlığı ile Hazine'nin yetkisindedir. Banknotlar, banknot matbaasında; madeni paralar, darphanede basılmaktadır [14].

2.2. KRİPTO PARA

2.2.1. Kripto Para Kavramı

Kripto para, blokzincir teknolojisi ve kriptografik şifreleme işlemlerinin kullanılması ile üretilen, merkezi otoritelere ya da herhangi bir aracı kurumlara bağlı olmayan, internet ortamında sanal cüzdanlar arasında transferi mümkün olan paradır. Kripto paralar organik yapıdadır; herhangi bir kuruluş, otorite ya da zümre tarafından yönetilmemektedir. En çok kullanılan kripto paralara: Bitcoin, Ethereum, Litecoin, Eos, Ripple, BitcoinCash, gibi örnekleri verebiliriz. Kripto paraların ilki Bitcoin (BTC)'dir [17].

2.2.2. Kripto Paraların Tarihsel Gelişimi

2008 yılında Satoshi Nakamoto tarafından hayat bulan Bitcoin, tamamen sıradan insanların kontrolünde; blockchain yani blokzincir altyapısı kullanılarak tarafların birbirine adapte edilmesi ile transfer edilmektedir. Kripto paraların ilki olan Bitcoin ve diğer altcoinlerin taraflar arasında akışı, hükümetlerin kontrolü dışında düşük transfer ücretleri ile gerçekleşmektedir. Kripto para işlemleri dolandırıcılıkları önleyebilecek karmaşık ve kompleks şifreleme yöntemlerine sahiptir. Para transfer işlemleri güvenli, aracısız, hızlı ve diğer ödeme yöntemlerine göre daha az masraflı olduğu için son zamanlarda adını sıkça duyurmuştur. Kripto

paralar; Bitcoin ve altcoinler, madenciler tarafından yazılım kurallarına uygun bir şekilde üretilmektedir [18].

Kripto paraların adını tüm dünyaya duyurmayı başaran Bitcoin, organik yapısı, merkezi otoritelere bağlı olmaması ve müthiş matematiksel kesinliği olan teknolojiyle insanların itimadını kazanmıştır. Kripto para akışında eşler arası transferlerin düşük maliyetlerde olması, bu paraların üzerinde herhangi bir otoritenin gölgesinin bulunmaması, insanların küreselleşmiş ekonomide yeni pazarlara yönelmesini teşvik etmektedir [10].

2.2.3. Kripto Paraların Genel Özellikleri

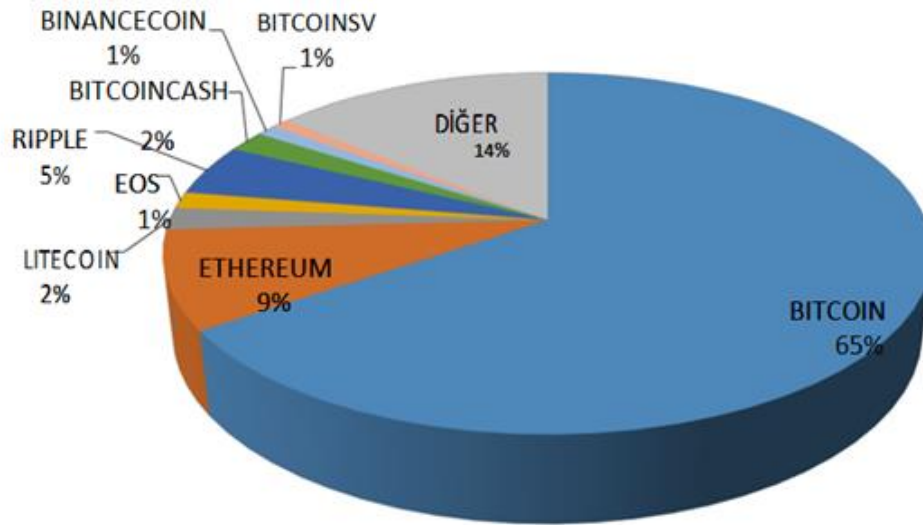
Çarkacıoğlu [18]'nin çalışmasına göre kripto paraların genel özellikleri aşağıdaki gibi sıralanmaktadır.

- i. Kripto paralar bankacılık sistemleri gibi bir merkezi tabana sahip değildir. Devletlerin ya da kuruluşların kontrolünde olmayan kripto para sistemlerinin işleyişi blokzincir (blockchain) yazılım veri tabanları ile sağlanmaktadır.
- ii. Merkezi olmayan kripto paralar, kamu tarafından erişilen ve bilinen yöntemlerle belirli oranlarda üretilir. Üretilecek kripto para arz miktarı ve zamanlaması kripto para sisteminin başlangıç aşamasında belirlenmiştir.
- iii. Kripto para işlemlerinin kaydedildiği bloklar, hesap defterleri ve kripto paraların transferleri, teknolojik olarak donanımlı madenciler tarafından güvenlik maksimum seviyelerde olacak şekilde sağlanır. Sistemin güvenliği için işlemlerin kontrolünü yapan madenciler birbirinden bağımsız bir şekilde çalışır.
- iv. Kripto paralar kendi başlarına birer para birimleridir. Hiçbir kurum ya da kuruluşun denetimi, kontrolü, etkisi altında kalmadan düzenlenip denetlenmeden işleyişini sürdürür.
- v. Kripto paraların ilki ve en çok bilineni Bitcoinler 2009 yılında tanımlanmıştır. Bitcoin'in piyasaya çıkmasıyla Bitcoin'e muadil olan ufak tefek farklılıklarıyla pek çok altcoin piyasalarda yerini almıştır.
- vi. Kripto paralar, maden ya da kâğıt gibi maddelerden üretilmemiştir. Tamamen yazılımlar sonucu dijital ortamlarda oluşan, internet yoluyla akışı sağlanan kripto paraların değeri,

kullanıcıların onu para gibi kullanmak istemelerinden ya da fiziki varlıkların yerine koyabilmelerinden gelmektedir.

- vii. 14.07.2021 tarihi itibarıyla 2267 kripto para altcoin bulunmaktadır ve kripto paraların dünya pazarındaki toplam payı yaklaşık 290 milyar dolardır. Söz konusu altcoinler piyasalarda Bitcoin'e benzer şekilde işleme tabidir. Bitcoin, yaklaşık 190 milyar dolarlık pazar payı ile kripto paralar içinde en yüksek orana sahiptir. 21.07.2021 tarihi itibarıyla 1 BTC = \$10,603,49 fiyatındadır.

Şekil 2.4'te Bitcoin ile birlikte dünya pazarında en çok pazar payına sahip olan kripto paralar gösterilmiştir.



Şekil 2.4: Kripto Paraların Dünya Pazarındaki Payları [19].

Grafik 1.1'e göre kripto paralar içinde dünya pazarındaki en çok paya %65'lik oran ile Bitcoin sahiptir. Bitcoin'den sonra ikinci sırada %8'lik oran ile Ethereum ve arkasından Ripple sanal para gelmektedir [20].

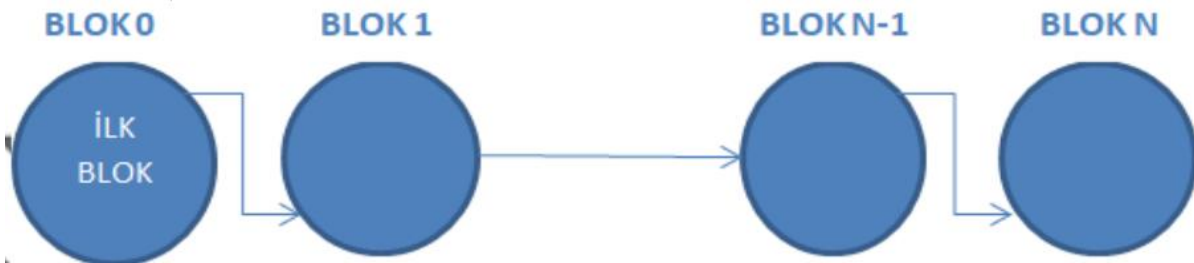
Tablo 2.1: En Çok Kullanılan Kripto Paraların Piyasa Değerleri (30.07.2021)

KRİPTO PARA	FİYAT ₺	PİYASADAKİ TOPLAM SAYISI	PİYASA DEĞERİ ₺
BITCOIN	53.522,76	17.847.325	955.238.120.401
ETHEREUM	1.176,19	107.115.748	125.988.870.268
BITCOIN CASH	1.768,96	17.920.200	31.700.054.693
LITECOIN	505,68	62.891.743	31.803.242.049
EOS	23,56	925.389.739	21.801.896.889

Tablo 2.1’de 30.07.2021 tarihi itibarıyla bazı kripto paraların fiyatları, dolaşımdaki sayıları ve piyasa değerleri sunulmuştur.

2.2.4. Kripto Para İşlemleri

Kripto para işlemleri yapılırken tüm işlemleri ihtiva eden kayıt defteri herkesle paylaşılmaktadır ve işlemler birbirinden habersiz madenciler tarafından onaylanıp doğrulanmaktadır. Güvenli bir şekilde onaylanan işlemler bloklar halinde birbirine bağlanarak kayıt defterlerinde yerini almaktadır [20].



Şekil 2.5: Blokların Gösterimi [15].

2.2.5. Kripto Paraların Muhasebeleştirilmesi

Bitcoin ve altcoinler bazı devletler tarafından göz ardı edilmektedir ancak bu, kripto paraların muhasebe kayıtlarına alınmasını engelleyemez. Kripto paralarla yapılan işlemler de muhasebenin mali konuları içine girmektedir. Muhasebenin görevi, işletmelerin görmek istedikleri finansal oluşumların takibini eksiksiz ve güvenilir bir şekilde vermektir. Eksiksiz muhasebe için kripto paraların da muhasebe kayıtlarında yer alması elzemdir [20].

Türkiye’de kripto paraların ödeme aracı olarak kullanılmasına yönelik yasal bir düzenleme bulunmamaktadır. Dolayısıyla muhasebe kayıtları ile ilgili düzenleme henüz yapılmamıştır. Ancak kripto paralar muhasebe kayıtlarında değerlendirme, rapor ve analizlerde yerini almak durumundadır. Türkiye’de kripto paralar da tüm yabancı paralar gibi, parayla ölçülme kavramı gereği Türk lirasına çevrilerek muhasebe kayıtlarına geçirilmektedir. Kripto paralar her an nakde çevrilebileceği ve tahsilat ya da ödeme aracı olarak kullanılacağı için muhasebe kayıtları içinde “Hazır Değerler” grubunda yerini bulmaktadır. Muhasebe kayıtlarında “104 Kripto Paralar Hesabı” ya da “108 Hazır Değerler Hesabı”na alt başlık olan “108.01 Kripto Paralar Hesabı” adı altında takip edilebilecektir.

Kripto paraların günden güne ilgi görmesi ve şirketlerin kullanımının artması muhasebeleştirme kavramını gündeme getirmektedir. Aşağıdaki örnekle muhasebe kayıtlarına ilişkin bilgi verilebilir.

3. BITCOIN ANALİZİ VE BLOKZİNCİR TEKNOLOJİSİ

3.1. BITCOİN ANALİZİ

3.1.1. Bitcoin'in Teorik Temelleri

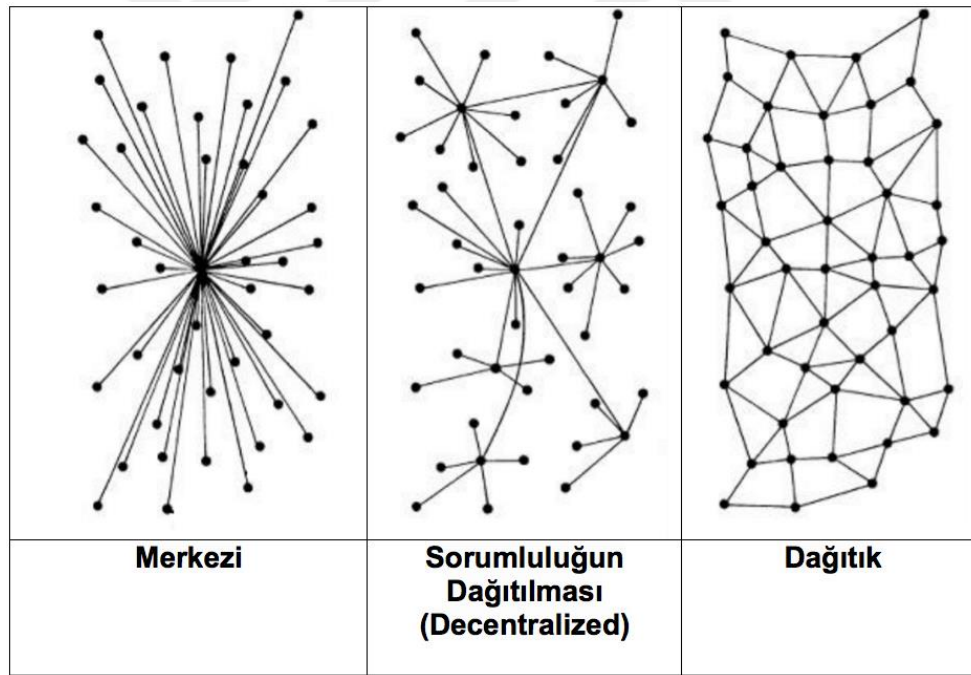
Kripto paraların ilki Bitcoin 1 Kasım 2008 tarihinde yazılımcı Satoshi Nakamoto tarafından geliştirilmiştir. Bitcoin parasal değer karşılığı basılan, fiziki bir değeri olmayan, özel donanımlı bilgisayarlarda şifreli ve güvenli bir şekilde saklanan kripto paradır. Bitcoin ile insanlar yüz yüze olmadan ve herhangi bir ödeme aracına (Kredi kartı, PayPal, Western Union) ihtiyaç duymadan düşük maliyetli transfer işlemleri yapabilmektedir. Nakamoto'nun makalesine göre Bitcoin'in işleyişi eşlerden eşlere elektronik nakit akışı şeklinde gerçekleşmektedir. Bitcoin, fiziki olarak hiçbir zaman basılmamıştır ve dijital ortamda insanların onu benimseyip kullanmasıyla faaliyete geçer. Bitcoinler eşler arası çalışan Peer to Peer (P2P) network ağı üzerinde işlem görmektedir. Bu ödemeler iki taraf arasında üçüncü bir itimat edilecek kişiyi araya sokmadan kripto (şifreli) bir şekilde yapılmaktadır. Taraflar arasında nakit transferi yapılırken işlemler tarih sırasına göre, işlemin doğruluğu kanıtlanarak çift harcamalar (mükerrer harcamalar) engellenmiş bir biçimde bloklar halinde dizilmektedir [21].

Bitcoinler elektronik ortamlarda saklanabilen, birbiriyle bağlantısını koparmamış halkaları bir araya getiren dijital imzalı dizilimlerden oluşur. Dizilimlerden oluşan Bitcoinler, blockchain (blokzincir) altyapısında birbirine halkalar halinde bağlanmış bloklardan oluşur ve güvenli karmaşık algoritmalar şeklinde işlemcilerde muhafaza edilir. Bitcoinler bilgisayarlara ya da mobil cihazlara indirilen yazılımlar (cüzdanlar) sayesinde muhafaza edilir ve bu şekilde kullanıcılara ulaşılır. Kullanıcıların açık ve gizli anahtar da denilen; açık ve gizli (kendilerine has) dijital dizilimleri vardır. Bitcoinleri ihtiva eden cüzdanların deforme olması ya da silinmesi cüzdan sahibinin Bitcoinlerine ulaşmasını imkânsız hale getirir.

3.1.2. Peer To Peer Network Ağı (P2P)

Kripto paraların en popülerleri Bitcoin'in, Peer to Peer (eşler arası) network iletişim ağı üzerinden, sadece sanal dünya için üretilmiş kripto (şifreleme) yöntemleriyle güvenliği maksimum seviyelere çıkarılmıştır. Şekil 2.1'de P2P ağının merkezi, merkezi olmayan ve dağıtık

mimarileri gösterilmektedir. Decentralization (merkezi olmayan) ve distributed (dağıtık) kavramları birbiriyle aynı değildir. Dağıtık yapı; işlemlerin birden fazla noktada gerçekleştiğini ifade etmektedir. Kripto para blokzincir yapısı da birçok noktada gerçekleştiği için dağıtık yapıdır. Decentralization (merkezi olmayan) yapı; tek bir kurum, kuruluş, zümre tarafından düzenleme yapılamayan ve kontrol edilemeyen anlamına gelir. Yani blokzincir, merkezi olmayan yapıya sahiptir. Merkezi olmayan yapıların merkezi yapılara üstünlükleri vardır; merkezi olmayan yapıda birden çok kullanıcı yapılan hata oranını düşürür yani kullanıcı hataları işlemlerin yapıldığı sistemin aksamasına neden olmaz. Güvenlik açısından merkezi olmayan sistemlere saldırı düzenlenmesi güç ve maliyetlidir çünkü saldırı için bilinen bir merkez bulunmamaktadır. Merkezi olmayan yapılarda sistemin işleyişini sağlayan katılımcılar birbirini tanımadığı için gizli anlaşma ya da hileli davranışlara yönelememektedir [21], [22].



Şekil 3.1: Network (İletişim Ağı) Çeşitleri [22].

3.1.3. Bitcoin'in ve Paranın Özelliklerinin Karşılaştırılması

İktisat teorisi parayı üç temel fonksiyonla ifade eder: değer saklama, değişim aracı ve hesap birimi. Bitcoin'in fiyatındaki dalgalanmalar, onun değer saklama aracı ve alışverişlerde

kullanılmak üzere hesap birimi olma özelliğini köreltmektedir çünkü insanlar gelecekte hızlı değişimlere uğrayan değerleri günlük işlerinde kullanmak istemez [23].

Güven ve Şahinöz [24]'ün çalışmasına göre Bitcoin'in ve paranın özellikleri karşılaştırılarak; Bitcoin'in, paranın özelliklerini ne ölçüde sağladığı aşağıda maddeler halinde açıklanmaktadır.

- i. Kabul Edilebilirlik: Bitcoin'in insanlar tarafından kanıksanması gün geçtikçe hızlı bir şekilde artmaktadır. İnsanlar Bitcoin'e zamanla daha da güven duymaktadır.
- ii. Taşınabilirlik: Bitcoin bu konuda rakip tanımamaktadır. Nakit para ya da bankadaki para, Bitcoin'in taşınabilirlik ve mobilite özelliğiyle Bitcoin'e rakip olamaz.
- iii. Tüm dünyadaki bankalar arası elektronik fon transferi standardı sağlayan Society for Worldwide Interbank Financial Telecommunication (SWIFT) sistemi ile dünyanın her yerine bankalar arasında, belli bir ücret karşılığı fon akışı sağlanabilir fakat bu süre birkaç günü bulabilir. Bitcoin işlemleri hem hızlı hem de düşük maliyetle gerçekleşmektedir.
- iv. Bölünebilirlik: 1 Bitcoin 100 milyona bölünebilir. Bitcoin gelecekte daha da yaygınlaşabilirse bölünebilirlik özelliği sayesinde, insanlar çok küçük meblağları rahatlıkla ödeyebilecektir.
- v. Dayanıklılık: Bitcoin'in ömür sınırlaması olmamaktadır. Banknotlar gibi herhangi bir yıpranmaya maruz kalmamaktadır. Merkez bankaları belirli sürelerde banknotları piyasadan toplayıp yenilerini piyasaya sürerken Bitcoin'in böyle bir maliyete katlanma sorunu bulunmamaktadır.
- vi. Taklit Edilememe: Bitcoinlerin taklitleri basılamamaktadır.

Bitcoin, paranın özelliklerini büyük ölçüde sağlasa da fiyatlardaki aşırı dalgalanmalar nedeniyle değer saklama aracı işlevini tam olarak sağlayamamaktadır. Bu da Bitcoin'in bazı çevreler tarafından eleştirilmesine neden olmaktadır.

3.1.4. Bitcoin'in Özellikleri

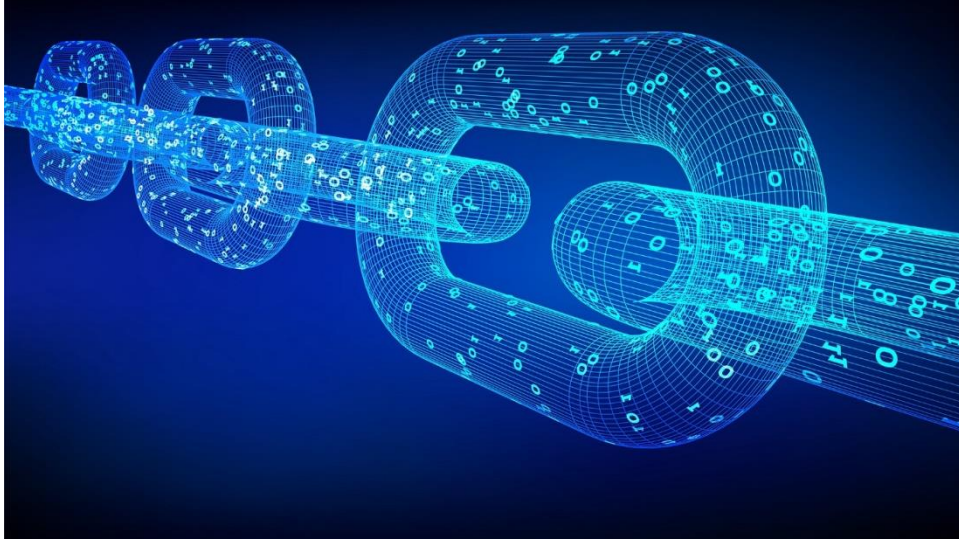
Sanal para Bitcoin'in özellikleri aşağıda sunulmaktadır.

- i. Bitcoin transferleri, özel matematiksel teknoloji kullanılarak P2P network ağı üzerinden güvenli bir şekilde sağlanmaktadır. Transfer işlemlerinde kişisel bilgiler gizlidir ve işlemler saldırılara karşı güvenlidir [25].
- ii. Bireyler arası transferler uygun ücretler karşılığında yapılır. Herhangi bir aracı kurum ya da kuruluşa fazladan ücret ödemesi yapılmaz. Taraflar arasında kredi kartı, PayPal, Western Union gibi ödeme araçlarına ihtiyaç duyulmamaktadır. Böylelikle Bitcoin'in kullanım alanı ve insanların Bitcoin'e olan talebi günden güne artış göstermektedir. Uluslararası serbest dolar transferlerinin belli bir ABD doları üst limiti bulunmakta ve bu limitin üzerinde işlem yapıldığında ABD tarafından işlemlere iptale varabilecek müdahaleler gerçekleşmektedir. Bitcoin ile transfer maliyetleri hem uygun fiyatlarda hem de kurum ya da kuruluşların, otoritelerin kontrolü olmaksızın gerçekleşmektedir. Bitcoin ile 10 dakikada tamamlanan ödeme işlemi, SWIFT ile 2-3 güne sarkabilmektedir. İşlemlerin sarkması ödeme hantallığına sebep olmaktadır [26].
- iii. Bitcoin, paranın sahip olduğu birçok özelliğe sahiptir. Bitcoin'in bölünebilir ve insanlar tarafından tanınıyor olması, kabul edilebilirliğini her geçen gün artırmaktadır. Bitcoin, 8 basamağa (0,00000001) 100.000.000 birime kadar bölünebilir. Bitcoin'in en küçük birimine "Satoshi" denir. 100 milyon Satoshi 1 BTC'dir. Bitcoin'in çok küçük birimlere bölünebilme özelliği, onu gelecekte gündelik hayatta herhangi bir alışverişte kullanıma uygun hale getirir. Bitcoin geleneksel paranın aksine, fiziksel bir görünümün yerine matematiksel ve teknik yazılımlarla desteklenmiştir. Bu sayede insanların Bitcoin'e olan güveni artmaktadır. Bitcoin'in değeri, insanlar tarafından benimsenip ödeme aracı olarak kullanılmasına, yaygınlığına, yatırımcının güvenine bağlıdır [25].
- iv. 2009'dan bu yana taraflar arasında gerçekleşen BTC gönderim işlemleri, blockchain (blokzincir) adı verilen ve herkese açık ama tarafların kimlik bilgilerinin gizli olduğu hesap defterinde muhafaza edilmektedir. Bitcoin işlem kayıtlarının tutulduğu blokzincirde bir Bitcoin'in üretiminden itibaren hangi hesaplara geçtiği şeffaf bir şekilde takip edilebilir fakat hesap sahiplerinin kimlik bilgileri gizli tutulmaktadır. Bitcoin'in maliyeti kullanıcılar tarafından belirlenir. Herhangi bir otorite, zümre ya da kuruluş bu maliyete müdahale edemez. Bitcoin kullanıcılarının hesaplarına kimse el koyamaz, hesaplar üzerinde herhangi bir işlem tesis edemez [18].

3.2. BLOKZİNCİR TEKNOLOJİSİ

3.2.1. Blokzincir Yapısının Oluşumu ve Fonksiyonları

Blockchain (blokzincir), bloklardaki verileri işleyip onaylama işlemini yapan madencilerin, bloklarla bağlantı kurduğu (zincir şeklinde bağladığı) yapıdır. Blokzincirler sayesinde Bitcoinler, şifreli bilgisayar veri tabanı ile çalışan ve sisteme katılan tüm kullanıcıların denetiminde, güvenli ve açık bir kayıt defterine kaydedilerek işlemlerden geçirilmektedir. Blokzincir yalnızca para akışını sağlamakla kalmayıp transferlerde herhangi bir aracıya gerek duyulmamasını, hızlı ve güvenilir işlem yapılabilmesini, işlem maliyetlerinin düşük olmasını da sağlamaktadır. Blokzincir sistemi yüksek teknoloji ile işlem güvenliğini maksimum seviyelere çıkarmaktadır. Blokzincir, BTC işlemlerinin kayıtlarının tutulduğu yüksek güvenli ortak ana defterdir [24].



Şekil 3.2: Blokzincir Görseli [25].

3.2.2. Bitcoin Transfer İşlemlerini “Hash” Haline Getirmek

Hash algoritması SHA (Secure Hash Algorithm) yani güvenli özetleme algoritması, bir şifreleme işlemi değildir. Hash işlemi herhangi bir verinin, belge ya da mesajın özgünlüğünü ifade etmek için kullanılan özetleme işlemidir. Hash fonksiyonları, veri tabanlarında aranan verileri hızlı bir şekilde bulmak ya da veri karşılaştırması yapmak için kullanılmaktadır. Veriler

hangi boyutta olursa olsun Hash algoritmasından geçtikten sonra sabit uzunlukta veriler ortaya çıkmaktadır [26].

Hash fonksiyonu farklı uzunluktaki verileri aloritmadan geçirip sabit uzunlukta mesaja çeviren fonksiyondur. SHA fonksiyonunun daha iyi anlaşılması için küp kök ($f(x) = 3\sqrt{x}$) fonksiyonu üzerinde örneklendirelim.

Örnek: $f(x) = 3\sqrt{x}$

Girdi sayısı (X)= 1453

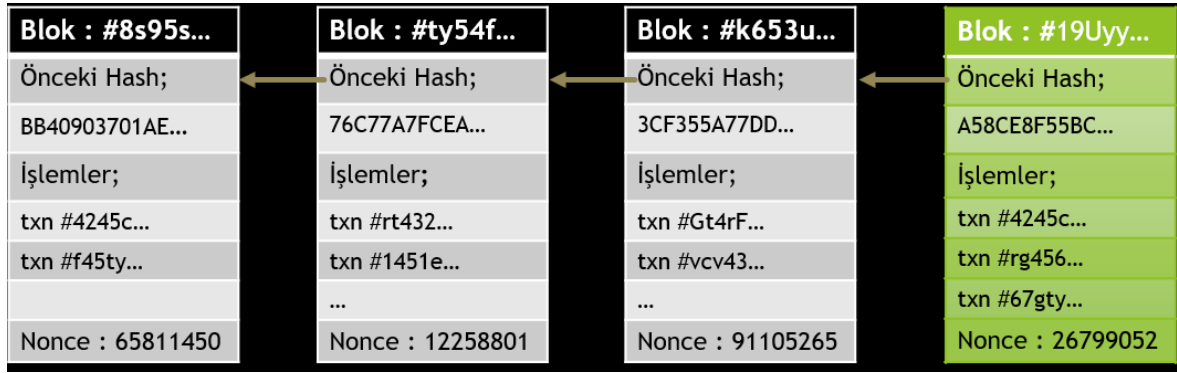
Çıktı sayısı = 11,3263124527669 olacaktır.

Çıkan sayıdan aradaki virgülü kaldırırsak;

Hash değeri = 113263124527669 olacaktır.

1453 sayısını bulmak için sayısız deneme yapmak gerektiği için SHA-256 algoritmasıyla yapılan özetlemenin güvenilir bir işlem olduğunu anlayabiliriz. Algoritma sonuçları ne kadar karmaşık, kompleks yapıda olursa işlemin güvenliği o kadar sağlam olur.

Bitcoin göndericileri tarafından bir işlem yapıldığında işlemler bloğu oluşur. Blokların her birinin içindeki bilgiler, madenciler tarafından SHA-256 Hash algoritması ile matematiksel süreçten geçirilerek görünürde harf ve sayı dizelerinden oluşan blokların özetini temsil eden Hash'e dönüştürülür. Hash, blokların en son kısmında yerini alır. Hash oluşurken hem blokların içindeki bilgiler hem de blokzincirde kendinden bir önceki bloğun Hash'i kullanılır. Böylece bloklar sağlamlaşmış, birbirine organik olarak bağlanmış olmaktadır. Bloklara karşı korsan saldırılar ve bu blokları değiştirmeye çalışanlar olursa değiştirilmeye çalışılan blok kendinden önceki ve sonraki blokları da etkilediği için yanıltıcı işlem anlaşılır hale gelecektir. Hash, blokzincirde zincirlerin can damarıdır. Zincirler arası asıl bağlantıyı sağlayan Hash'tir. Hash'in içerdiği bilgiler rastgele yapılmaz. Örneğin dizilimlerin başına belli sayıda sıfır gelmesi gerekir, belli sayıda harf ve rakamlar arka arkaya dizilir [27].



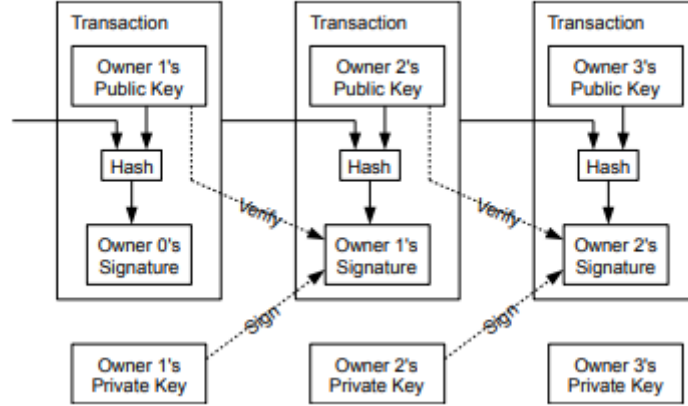
Şekil 3.3: Bloktaki işlemlerin “Hash” Uygulamasından Geçirilmesi [27].

Şekil 3.3’te blok oluşturulurken kişiler arasında aktarılan farklı uzunlukta veriler “Hash” algoritmasından geçirilmekte ve sabit uzunlukta veriler elde edilmektedir.

3.2.3. Bitcoin Transfer İşlemlerinin İmzalanması

Bitcoin gibi sanal paralar, dijital bir imza zinciri ihtiva etmektedir. Bitcoin el değiştirirken güvenlik açısından bazı işlemlerden geçmek zorundadır. İşlemler, aracı bir kuruma gereksinim duyulmadan P2P network ağı üzerinden gerçekleşmektedir. Transfer işlemleri yapılırken göndericinin e-imza ile gönderim bilgisini onaylaması, ağ üzerinde her madenciye onaylı gönderimin bildirilmesi, her bireyin bu gönderimin doğruluğunu teyit etme donanımına sahip olması gerekir. Sanal para akışı bir taraftan diğer tarafa şu şekilde iletilir: 1. taraf kendi dijital imzasıyla bir önceki işlemin özetini (Hash) ve 2. tarafın açık anahtarını imzalar, sonrasında bu imza bloğun sonuna nakledilir. Bu işlemler ödemeyi yapan kişinin daha önce bu parayı başka kişilere göndermediğini kanıtlayacak şekilde özel bir fonksiyon olan SHA-256 fonksiyonuyla sağlanır. Bu sayede blok özetleri birbirine blokzincir ile bağlanmış şekilde bulunur ve bir blok değiştiğinde kendinden sonraki tüm bloklar değişeceği için blokların güvenliği sağlanmış olur [28], [16].

Bitcoinleri aktarmak için alıcının göndericiye açık anahtarını göndermesi gerekir. Gönderici alıcının açık anahtarını imzalar ve elektronik ortamda dijital gönderim yapar. Bitcoin’i, sahibinin dışında kimse kullanamaz çünkü teknolojik kodlama yapılmaktadır. Bitcoin sahibinin kimliği de gizlidir.



Şekil 3.4: Bitcoin İşlem Süreci [28].

Şekil 3.4'te birkaç işlemin fiziki bir şekilde gösterimi yapılmıştır. Şekilde dijital imza zincirinden oluşan Bitcoin işlemi gösterilmektedir. Bitcoin'i kullanmak için bir açık anahtar bir de özel anahtar dosyalarına sahip olmak gerekir. Dosyaları güvende tutmak çok önemlidir. Çünkü dosyalar silinirse Bitcoinler de kaybolur.

Dijital imzalamaya örnek olarak taraflar arasında gönderilen veriler aşağıda örnek üzerinde anlatılmaktadır.

A kişisi ve B kişisi arasında veri iletimi gerçekleşecek olursa;

- i. A kişisi gönderisini hazırlar ve gönderi SHA-256 algoritmasında özetlenir. Buna (Özet veri A) diyelim.
- ii. A kişisi oluşturduğu özet veriyi kendi gizli anahtarıyla şifreler (imzalar) ve B kişisinin açık adresine gönderir.
- iii. B kişisi, A kişisinin adresiyle imzalanmış şifreli veriyi gizli anahtarı ile çözümler, özetlenmiş veriyi ortaya çıkarır.
- iv. B kişisi gelen şifrelenmiş veriyi özetler buna (Özet veri B) denir.
- v. B kişisi oluşturduğu özet veri ile A kişisinden gönderilen özet veriyi karşılaştırır.
- vi. Verilerin güvenli bir şekilde gelmesi için iki verinin birbirini doğrulaması şarttır.

3.2.4. Bitcoin İşlemlerinin Görünümü

Örneğin A kişisi B kişisine bir miktar Bitcoin gönderirse bu işlem şu şekilde görülür.

Girdi: Bu kayıtta A kişinin o Bitcoinlere nasıl ulaştığı görülmektedir.

Miktar: Bu kayıtta A kişinin B kişisine gönderdiği Bitcoin miktarı görülmektedir.

Çıktı: Bu kayıtta ise B kişinin Bitcoin adresi görülmektedir.

A kişisi, B kişisine Bitcoin göndermek istediği zaman girdiyi, miktarı ve çıktıyı barındıran bir mesajı imzalamak için kendi özel anahtarını kullanır ve kendi Bitcoin cüzdanından ortak Bitcoin mekanizmasına gönderir. Bitcoin madencileri işlemi onaylar ve B kişinin cüzdanına aktarım işlemi gerçekleşir [22].

Bitcoin işlemlerini analiz edecek olursak; işlemin girdi ve çıktı toplam miktarları eşit olmalıdır. Bu girdiler daha önceki işlemlerden kalan başka bir adrese aktarılmamış çıktılardır. Bitcoin gönderimi için öncelikle karşı tarafın Bitcoin adresi ya da QR kodu bilinmelidir. Bu şekilde kişi, karşı tarafa kendi Bitcoin cüzdanından transfer işlemi başlatabilir.

İŞLEMNO: *560			
GİRDİLER		ÇIKTILAR	
*500 Nolu işlem	3 BTC	Bitcoin adresi	2 BTC
*510 Nolu işlem	5 BTC	Bitcoin adresi	4 BTC
		Bitcoin adresi	2 BTC
Toplam: 8 BTC		Toplam: 8 BTC	

Şekil 3.5: Bitcoin Transfer İşlemi

Şekil 3.5'te 8 BTC sahibi bir kullanıcı, Bitcoinlerini 3 farklı adrese göndermektedir. 560 numaralı işlemin girdileri 500 ve 510 numaralı işlemlerin önceden başka işlemlerde kullanılmamış güvenli alışveriş yapılacak çıktılarıdır. 560 numaralı işlemin çıktıları ise 3 farklı Bitcoin adresinden oluşmaktadır.

İŞLEM NO: *381			
GİRDİLER		ÇIKTILAR	
*300 Nolu işlem	7 BTC	Bitcoin adresi	4 BTC
Toplam: 7 BTC		Bitcoin adresi	3 BTC
		Toplam: 7 BTC	

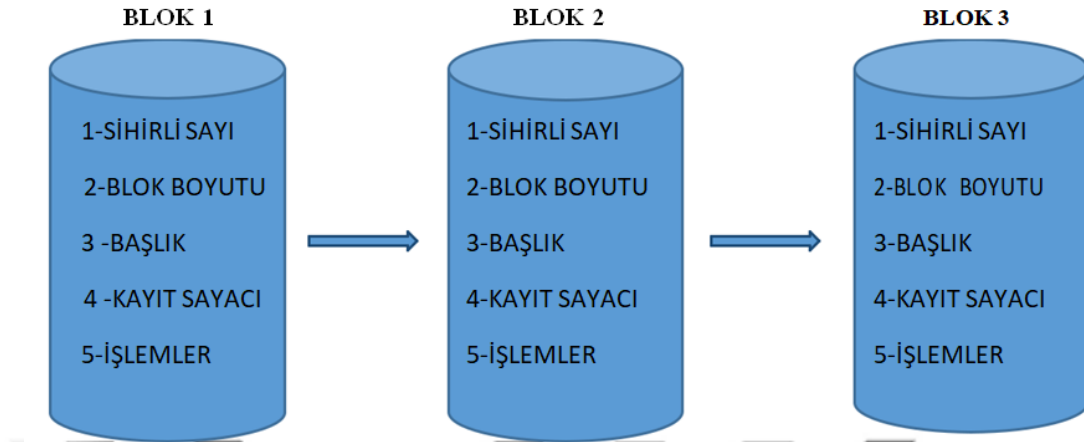
Şekil 3.6: Bitcoin ile Ödeme Yaparak Tatlı Yemek İsteyen Müşterinin İşlemi

Şekil 3.6’da ise 7 BTC sahibi bir kullanıcının, 4 Bitcoin karşılığında tatlı alması ve işlem sonucunda artan 3 Bitcoin’i yine kullanıcının kendisine ait olan Bitcoin adresine gönderilmesi gösterilmektedir [29].

3.2.5. Blokzincir Yapısının Bileşenleri

Blokzincir, donanımlı bilgisayarlar ile yapılan Bitcoin işlemlerinin madenciler tarafından güvenli bir şekilde matematiksel formüllerden geçirildikten sonra kayıt altına alınmasıyla oluşan dijital defterdir. Bu defter, merkezi bir otorite tarafından gözetlenemez ve defter üzerinde işlem tesis edilemez. Blokzincir denilen dijital defter halka açık, veri güvenliği sağlanmış, tarafların bilgileri gizli tutulacak şekilde tasarlanmıştır [21].

Blokzincir, Merkle ağacına özetlenmiş (Hash) ve matematik kodlarla eşsiz duruma getirilmiş işlemleri içinde barındıran bloklardan oluşur. Her blok önceki bloğun şifreli Hash yapısını ihtiva eder. Bir önceki bloğun Hash değerlerini barındırması blokların birbirine bağlanmasını sağlar.



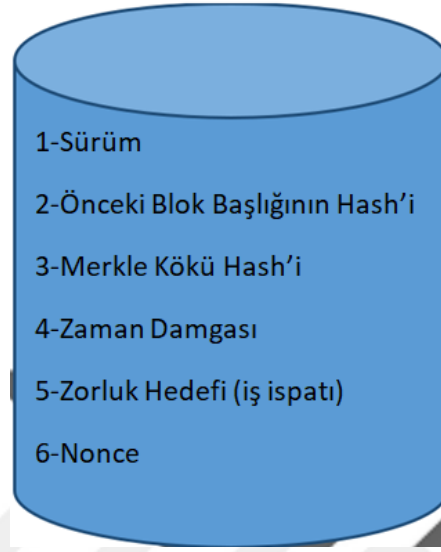
Şekil 3.7: Blokzincir Yapısı [21].

Tablo 3.1: Blokzincir Yapısının Açıklaması

ALAN ADI	BOYUT	AÇIKLAMA
Sihirli Sayı	4 Byte	“Devamındaki bilgiler bir bloktur” anlamına gelir. Bu sayı her zaman sabit bir değerdir.
Blok Boyutu	4 Byte	Bloğun sahip olduğu büyüklüğü göstermektedir.
Blok Başlığı	80 Byte	6 özel kısımdan oluşur. Çok kritik alanları barındırır.
Kayıt Sayacı	1-9 Byte	Kaç adet işlem olduğunu gösterir.
İşlemler	Değişir	Kaydedilen işlemleri gösterir.

Bir blok içerisindeki blok başlığının bileşenleri Şekil 3.8’de gösterilmektedir.

Blok Başlığı



Şekil 3.8: Blok Başlığı [23].

Şekil 3.8’de sunulan blok başlığının bileşenleri Tablo 3.2’de açıklanmaktadır.

Tablo 3.2: Blok Başlığı Açıklaması

ALAN ADI	BOYUT	AÇIKLAMA
Sürüm (versiyon)	4 Byte	Bloğun yapısal özellikleri gösterilir.
Önceki Blok Hash’i	32 Byte	Bir önceki bloğun Hash değeri gösterilir.
Merkle Kökü Hash’i	32 Byte	Bu bloktaki işlemlerin Merkle ağacı kök değeri gösterilir.
Zaman Damgası	4 Byte	Bloğun oluşma zamanı (saniye cinsinden)
Zorluk Hedefi (iş ispatı)	4 Byte	Bloğun iş ispatının zorluk derecesi
Nonce	4 Byte	PoW yapılabilmesi için bir sayaç

3.2.5.1. Sürüm

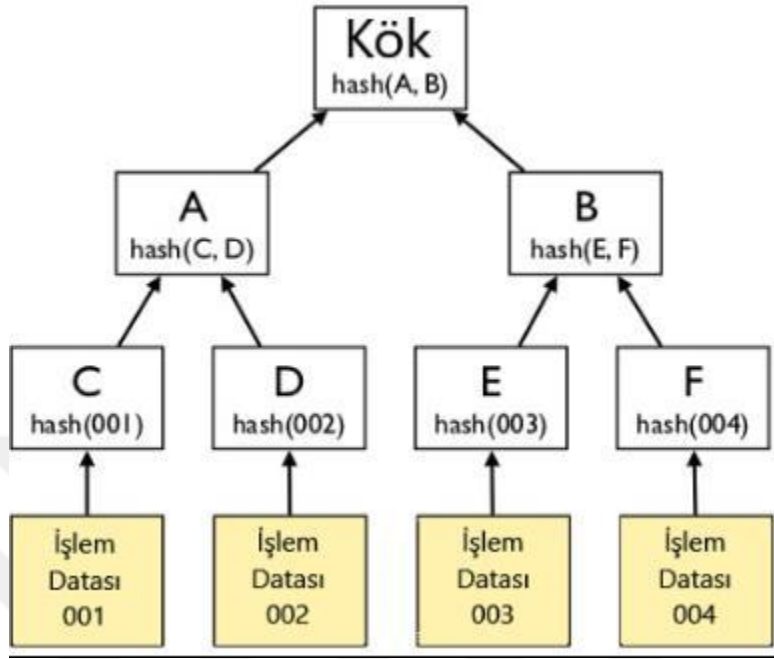
Sürüm, blokzincirde blok oluşturulurken bloğun yapısı, uzunluğu, kayıt şekli gibi standart uygulamaları gösteren kısımdır. Bu kurallar bloğu oluşturan madenciler tarafından oy çokluğu ya da oy birliği ile değiştirilebilir [19].

3.2.5.2. Önceki bloğun hash'i

Hash değeri blokzincirde blokların birbirine bağlanmasını sağlayan değerdir. Bir blok oluşunca bu bloğun tamamı yerine bloğun başlığının Hash değeri oluşturulur ve diğer bloğa da eklenerek bağlantı kurulur. Böylece blokzincire herhangi bir yanlış blok ekleme ya da blokta değiştirme işlemi yapılamaz. Blok başlığının Hash değeri o bloğun parmak izi yerine geçmektedir.

3.2.5.3. Merkle ağacı kökü

Blok içindeki işlemler ikiye bölünür ve işlemlerin Hash'i alınır. Alınan Hash değerleri tekrar ikiye bölünür ve işlemlerin yeniden Hash'i alınır ve bu şekilde Merkle köküne ulaşılır. İkiye bölünmüş hesaplanan Hash değerlerine "Merkle Ağacı" denir. Merkle ağacı yapraklarında Bitcoin işlemlerinin bilgilerini içeren veriler bulunmaktadır. Merkle ağacının kökü, bir blokta yapılan tüm işlemlerin özetini ihtiva eder. Blokzincirin her bloğunda önceki bloğun tüm işlemleri yerine sadece önceki bloğun merkle kökü bulunmaktadır. Bu şekilde işlemler bloklarda daha az yer kaplar ve daha az veri kullanılarak Bitcoin işlemlerinin doğruluğu ispatlanır. Merkle ağacı sayesinde blokların bağlantılarının tutarlı olup olmadığı anlaşılır ve Merkle kökü sayesinde veri israfı önlenmiş olur [24].



Şekil 3.9: Merkle Ağacı'nın Yapısı [28].

Uygun bir blok özetleme değeri oluşturabilmek için aşağıdaki süreçleri izlemek gerekir:

Öncelikle blok içinde yer alan işlemler seçilir. Sonrasında seçilen işlemlerle Merkle ağacı yapısı kullanılarak Merkle kök değerine ulaşılır. Merkle kök değeri + bir önceki bloğun özetleme değeri kullanılarak blok başlığı oluşur. Blok başlığı özetlenerek (Hashing) uygun değer sağlanıp sağlanmadığı kontrol edilir. Uygun değer sağlandıysa yeni blok başarılı bir şekilde sağlanmış olur. Kontrol olumsuz sonuçlandıysa doğru blok yapısı oluşturulana kadar işlem akışı tekrarlanır [29].

3.2.5.4. Zaman damgası

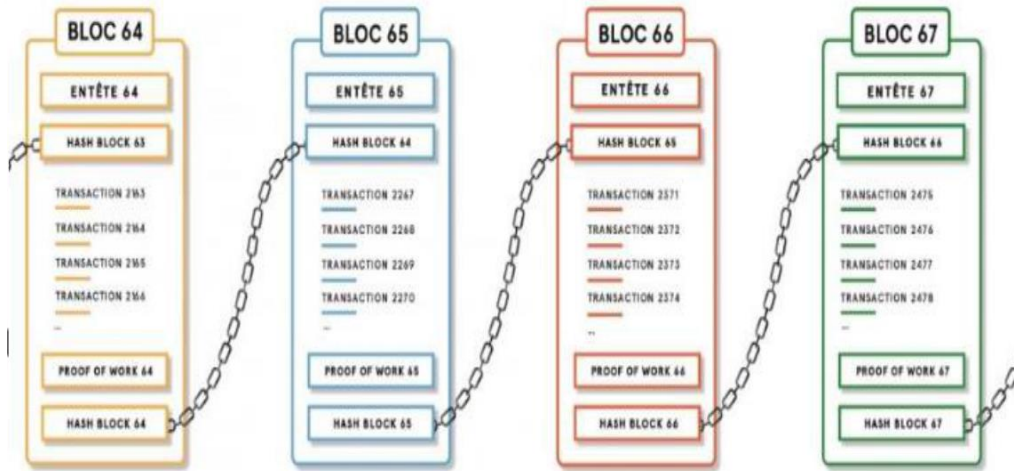
Bloğun üretildiği zamanı göstermektedir. Zaman damgası 4 Byte'a ayrılmıştır. 4 Byte 32 Bit etmektedir [29].

3.2.5.5. Proof of work

Proof of Work sistemi (PoW) blokzincire bir blok hazırlamak için kullanılır. Proof of Work sistemi ile blokların özetlerine ulaşılır. Bu sistemi kullanırken blok özeti kontrolünün kolay

olduğu bir denklem üzerinden hareket edilir. Ancak denklemi çözmek ciddi efor gerektirir. Denklemde herkesin uyması gereken kurallar vardır; Hash değeri tanımlanmış değer aralığında olmalı ve dizinler belirli bir karakter dizisi ile başlamalıdır. Bir blok oluşturulurken bloğun “Proof of Work” sistemine uygun olabilmesi için yüksek işlem gücü kullanılarak ortalama 10 dakika harcanır ama özetleme (Hash) değerinin kontrolü çok daha kısa ve kolay olmaktadır. Eğer bir blokta “Proof of Work” varsa o blok geçerli sayılan bloktur çünkü iş ispatı yapılmış demektir.

Şekil 3.10’da Proof of Work (iş ispatı) yapıp blokların sonuna eklenmiş hali gösterilmektedir.



Şekil 3.10: Blokzincirde İş İspatının Gösterimi [30], [24].

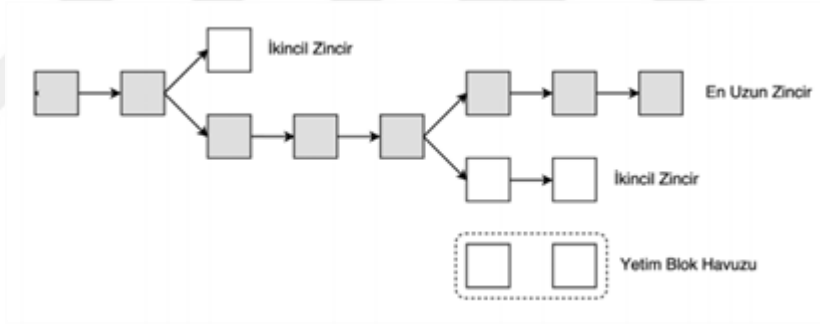
3.2.5.6. Nonce değeri

İş ispatının yapılabilmesi için bir nevi deneme yanılma yapılan alan Nonce alanıdır. Blokların Hash değerleri ispat edilirken bloğun içinde bulunan Nonce alanındaki sayılar değiştirilerek her defasında farklı Hash değeri bulunur. Denemeler yapıp doğru Hash değeri bulunana kadar Nonce sayacındaki sayılar kullanılır [30].

3.2.6. Yetim Bloklar

Blokszincirde bloklar birbirini takip eden yapıda olmak zorundadır. Bazı durumlarda işlemleri takip eden birden çok madenci iş ispatını yapar ve yaptığı ispatı bloklara bağlamaya çalışır. Bu şekilde bağlantı çatallanması meydana gelir. İşlemler tamamlandıktan sonra blokszincirdeki blokların en uzun ucu doğru bağlantı olarak kabul edilir. Diğer bloklar yetim blok olarak kalır. İş ispatı yapan madenciye hemen Bitcoin ödülü verilmez çünkü üretilen blokların eş zamanlı başka madenciler tarafından da üretilme olasılığı söz konusudur. İşlemden geçirdiği bloğu blokszincire adapte edebilen madenci Bitcoin ödülünü almaya hak kazanır [31].

Yetim blokların blokszincir yapısındaki görünümü Şekil 3.11’de sunulmaktadır. Şekle göre iki zincirli bloklar oluşmakta olup bu zincirlerin uzun olanı asıl blokszinciri temsil etmekte, kısa olan zincir ise atıl kalmaktadır.



Şekil 3.11: Yetim Bloklar [31].

3.2.7. Blokszincirde “Fork”lanma (Çatallanma)

“Fork” bir projenin kodları kullanılarak mevcut projeye teknik detaylar ekleyip farklı projeler üretme işlemidir. Forking ile blokszincir altyapısında hantallıkları ve zaman kaybını en aza indirmek için bazı teknolojik yeniliklere başvurulabilir. Fork işleminin yapılabilmesi için önerilen projenin, madenciler tarafından onaylanması şarttır çünkü blokszinciri ayakta tutan, blokszincir üzerinde düzenlemeler yapan madencilerdir. Madenciler blokszincirde yapılması planlanan değişikliklerde mutabakat sağlamak için yoğunlaşır. Örneğin bir blokszincirin sonraki bloklarının büyüklük değerini değiştirmek için öneri yapıldığında, madenci çoğunluğu bu teklifi kabul ederse blokszincirde çatallanma olmadan devam eder ve buna Soft Forking denir. Soft

Forking'in adında forking (çatallanma) geçse de zincirde sadece teknik değişiklik yaşanmaktadır [32].

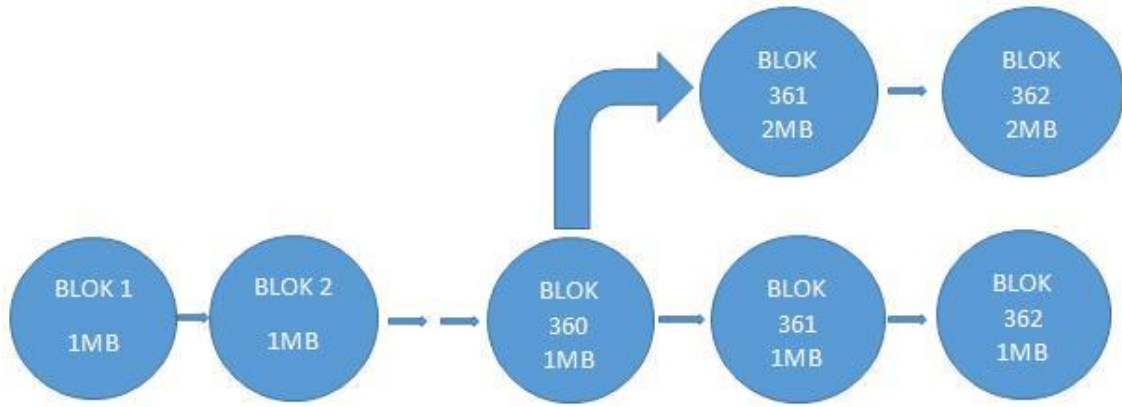
Şekil 3.12'de gönüllü çatallanmanın görseli sunulmaktadır. Şekle göre BLOK 361'den itibaren blok boyutları 2 MB'ye çıkmaktadır. Gönüllü çatallanma olduğu için zincirde herhangi bir sapma meydana gelmemiştir.



Şekil 3.12: Gönüllü Çatallanma (Soft Forking) [32].

Forking işleminde bazen madenciler arasında ihtilafa düşülen zamanlar mevcuttur. Bu gibi zamanlarda kodlama yapılan zincirden itibaren mecburi bir çatallanma meydana gelir. Bazı madenciler ilk kurala göre işlem yapmaya devam ederken bir grup madenci de yeni sisteme adapte olup yeni oluşan çatal zincir üzerinden işlem yapmaya devam eder. Bu yeni çatal zincirden devam etme işlemine Hard Forking denilmektedir.

Şekil 3.13'te zorunlu çatallanmanın görseli sunulmaktadır. Zorunlu çatallanmada 360'ıncı bloktan sonra bir çatallanma meydana gelmektedir. Yapılan yeni kodlama 360'ıncı blok ve öncesinde geçerli olmayacağından 361'inci bloktan itibaren yeni bir zincir meydana gelmektedir. Artık bir kısım madenci önceki kodlamaya göre diğerleri ise yeni zincire göre hareket edecektir. Zorunlu çatallanmaya Bitcoin'in üzerinden yapılan çatallanma sonucu oluşan Bitcoin Cash, Bitcoin Gold, SegWit, Bitcoin Diamond, Bitcoin X, Super Bitcoin, Bitcoin Platinum, Lightning Bitcoin, Bitcoin Cash Plas, Bitcoin Silver, Bitcoin Uranium, Bitcoin Top, Bitcoin Interest, Bitcoin Private, Bitcoin Atom gibi örnekler verilebilir.

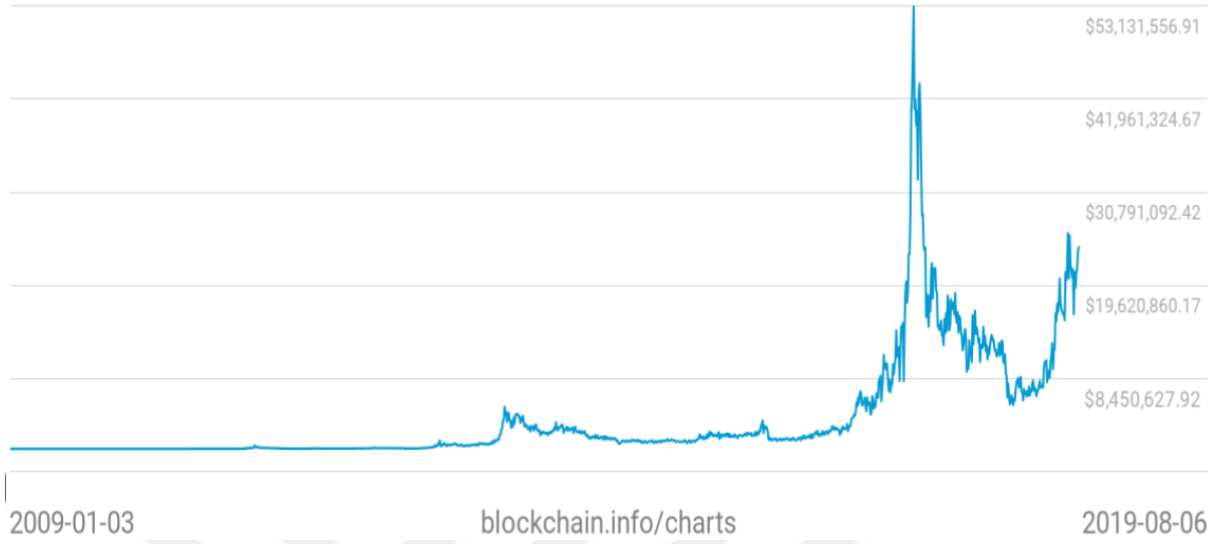


Şekil 3.13: Zorunlu Çatallanma (Hard Forking) [32].

3.2.8. Mining (Madencilik)

Madencilik, Bitcoin üretim işlemidir. Madenciler kripto para işlemlerinin güvenli yapılması için çalışan, matematiksel yazılımlarla iş ispatı yapan ve bunun karşılığında ödül olarak Bitcoin alan kimselerdir. Madenciler, tarafların birbirine gönderdiği Bitcoin işlemlerinin takibini yapar, bu takibi blok adı verilen listelerde kayıt altına alır ve onaylayıp ana deftere geçirir. Blokzincir işlemlerinin takibi, onayı, kayıt altına alınması, gizliliği madencilerin işidir. Madenciler, işlemleri süzgeçten geçirip blok oluşturabilmek için yüksek efor ve işlemsel güç sarf ederek yarışır. Madenciler blockchain işlemlerini bloğun içindeki bilgileri matematiksel formüllerden geçirip eşsiz bir yapıya (Hash) çevirir. “Hash” aslında o bloğun özetidir. Madenciler, zincirdeki diğer bloklara bu özetleri ekleyerek blokzincir yapısını oluşturur. SHA-256 gibi özel fonksiyonlar kullanılarak yapılan Bitcoin işlemleri için yüksek performans ve elektrik gücü sarf edilir [33].

Bitcoin madenciliğine örnek vermek gerekirse; insanlar altın ya da değerli madenleri bulabilmek için kazı çalışması yapar. Madenci dediğimiz kişiler de Bitcoin kazanabilmek ve bu Bitcoinleri dolaşıma sürebilmek için 16 haneli şifreyi çözmek zorundadır. Şifreyi çözebilmek, profesyonel bilgi ve teknik donanım gerektirir. Madenciler bütün bu emeklerinin karşılığında Bitcoin kazanır [33].



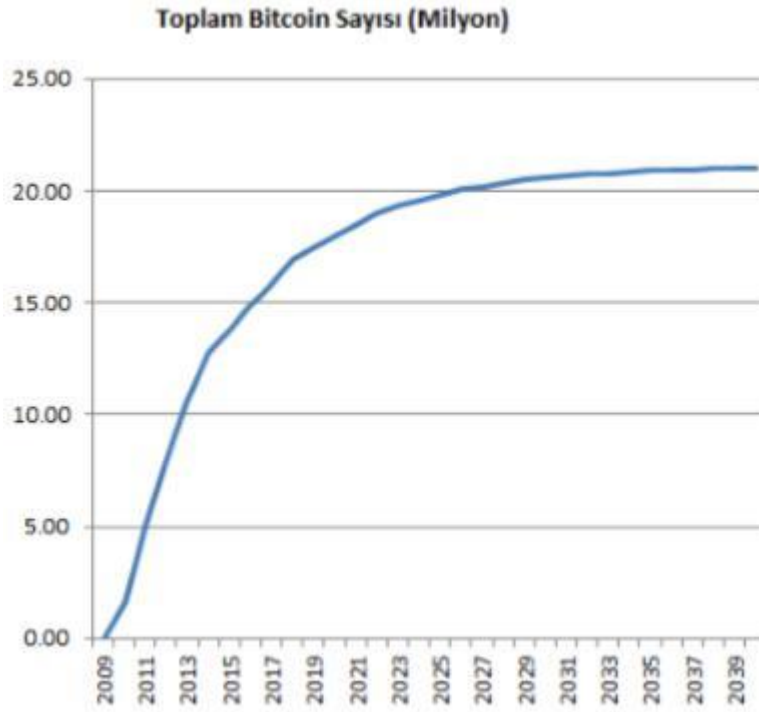
Şekil 3.14: 2009-2021 Yılları Arasında Madencilere Ödenen İşlem Ücretlerinin Toplam Değeri (Milyon Dolar) [33].

Şekil 3.14’te madencilere ödenen işlem ücreti, işlem hacminin en çok olduğu 2017 yılının son çeyreğinde 50 milyon doların üzerinde seyretmektedir. 06.08.2021 tarihinde madencilere ödenen işlem ücretlerinin toplam değeri 24 milyon dolar civarındadır.

Tamamen açık kaynaklı ve herkesin bu yazılımı bilgisayarına indirip inceleyebileceği Bitcoin yazılımı üzerinden blok oluşturup Bitcoin kazanmak, Bitcoin’in ilk piyasaya çıktığı yıllarda CPU (bilgisayar işlemcisi) tarafından yapılabiliyordu. Zamanla CPU’ların yerini daha hızlı, verimli ve CPU’lara göre daha yüksek bütçeli GPU (ekran/grafik kartı) almıştır. Daha sonra CPU ve GPU’ların da yetmediği Bitcoin üretim işlemleri, 2013 yılı itibariyle ASIC denilen Bitcoin üretimi için özel üretilen bilgisayarlar tarafından yapılmaya başlanmıştır. Bitcoin üretimi, 21 milyon ile sınırlı olması ve günden güne blok işlem sayısının artması nedeniyle daha güçlü makinelerle daha çok güç sarf edilerek yapılmaktadır. Bitcoin işlemlerinin zorluk derecesi her geçen gün artmaktadır. 2008 yılında blokzincire bir blok eklemek 50 Bitcoin ile ödüllendirilirken 2010 yılında bir blok eklemek 25 Bitcoin, 2016 yılında ise 12,5 Bitcoin kazandırmaktadır. Bu şekilde her 4 yılda bir, Bitcoin ödülü yarıya düşecektir. Bitcoin teknolojisi gelişmeler gösterse de sistem git gide daha da zorlaşacaktır [9], [21], [34].

Madencilik, yüksek teknolojik makine ve bilgisayarlar ile yapılan elektrik harcamaları çok yüksek olan maliyetli bir iştir. Günümüzde madenciler teknik donanımlara sahip olmasına rağmen makinelerini madencilik havuzuna uyarlamaktadır. Madenciler işlem ödülleri havuza yaptıkları katkı ölçüsünde almaktadır. Madencilik havuzları (mining pool) fazla sayıda Bitcoin madencisinin cihazlarıyla, belli programları kullanarak web siteleri üzerinden iletişim kurmaları sonucunda oluşur. Bu havuzlara katılmak için herhangi bir izne gerek yoktur. Dileyen herkes katılabilir. Havuza katılanlardan web sitesi üzerinden bir dosya indirilmesi istenir ve bu dosya indirildikten sonra madencilik havuzuna üyelik sağlanır. Madencilerin blokzincir üzerinden yaptıkları işlere verilen ödüller, madencilerin çalışmalarındaki yoğunluğa göre dağıtılır [34].

Maksimum üretimi Şekil 3.15'te görüldüğü üzere 21,000,000 adetle sınırlı olan Bitcoinler, karmaşık algoritmalarla teknolojiye uygun bir şekilde şifrelerden oluşan ve oluşturma işlemi yüksek işlemci performansı isteyen zincir halkalardan oluşan kripto paralardır. Maksimum üretime, her 10 dakikada 1 blok oluşturulduğu düşünülerek 2140 yılında ulaşılacağı tahmin edilmektedir [35].

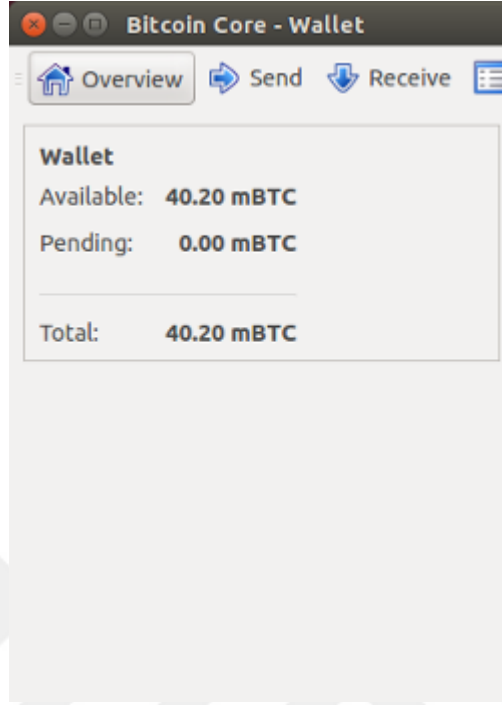


Şekil 3.15: Toplam Bitcoin Sayısı [34].

3.3. BİTCOİN CÜZDANI VE SANAL PARA TRANSFERİ

Taraflar arasında Bitcoin akışı, blokzincir üzerinden kişilerin kendilerine ait dijital imzaları ile sağlanır. Dijital imzalar tarafların kullandıkları anahtarlar sayesinde gerçekleştirilir. Bitcoin cüzdanları taraflar arasında para transferi yapmak için gerekli olan, özel anahtarları barındıran sanal ortamda hazırlanmış cüzdanlardır. Cüzdanlar bilgisayarlarda saklanmak istenilmezse kâğıt cüzdan olarak da kullanılabilir fakat kâğıt cüzdanlar dijital cüzdanlardan daha korumasızdır. Bitcoin cüzdan yazılımları masaüstü, mobil ya da çevrimiçi cüzdanlar olarak kullanılabilir. Masaüstü cüzdanlar Bitcoin'in orijinal sürümünün (Bitcoin Core) bilgisayara yüklenmesi ile masaüstünde oluşmaktadır. Bu yazılımın sağladığı güvenli anahtarlar kullanılarak sanal para akışı yapılabilir. Masaüstü cüzdanları, Bitcoinleri taşıma açısından kolay olmayabilir. Teknolojinin ilerlemesiyle akıllı telefonlara Bitcoin cüzdan yazılımı uygulama şeklinde indirilerek direkt telefonda ödeme yapma kolaylığı sağlanır. Ancak Bitcoin'in mobil cüzdan uygulamasının tam sürümünü akıllı telefonlar taşımayabilir. Bu da cüzdanları telefonda saklamayı avantaj olmaktan çıkarabilir. Mobil cüzdanları, Bitcoin sürümünün sadece bir kısmı indirilerek telefonlarda saklanmaktadır [34], [35].

Resim 2.3'teki Bitcoin elektronik cüzdan, akıllı telefonlar ya da kişisel bilgisayarlar için tasarlanmıştır. Bu cüzdanlar kullanıcılara blokzincir altyapısı kullanılarak şifreli yöntemlerle kripto paralarını saklama olanağı sunmaktadır.



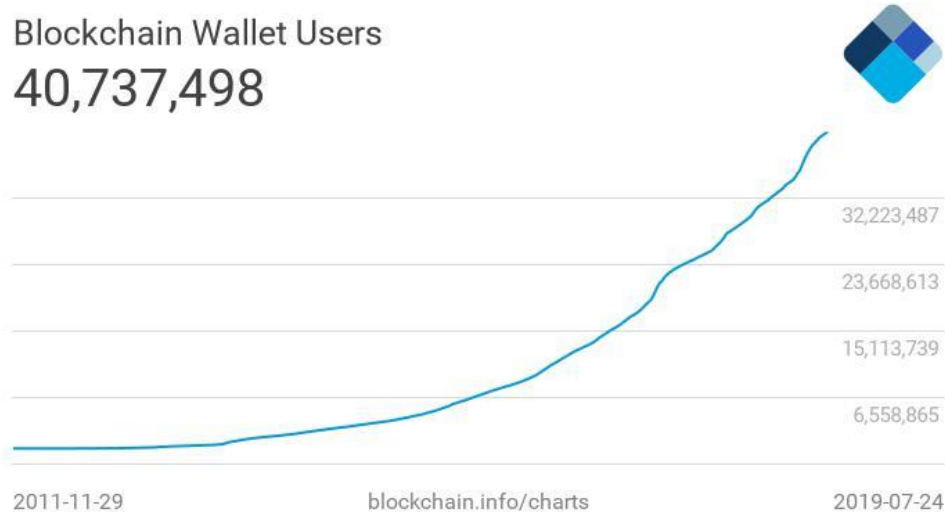
Şekil 3.16: Bitcoin Elektronik Cüzdan [35].

Şekil 3.16’da görüldüğü üzere Bitcoin kâğıt cüzdanın sol tarafı adres, sağ tarafı ise gizli anahtarı ihtiva etmektedir. Bitcoin kâğıt cüzdanlar güvenlik açısından daha korunmasızdır; üzerinde bulunan karekod, Bitcoin cüzdanı sahibinden habersiz işlem yapılmasına neden olabilmektedir.



Şekil 3.17: Bitcoin Kâğıt Cüzdan [32].

Şekil 3.18’de Bitcoin cüzdanı kullanıcı sayısının yıldan yıla arttığı görülmektedir. Bitcoin cüzdanı kullanıcı sayısı son üç yılda hızlı bir artış göstermiş ve 2021 yılında 40 milyonun üzerinde seyretmiştir.



Şekil 3.18: Bitcoin Cüzdanı Kullanıcı Sayısı [33].

3.3.1. Bitcoin Temini

Bitcoin kullanımına karşı talep ve ilgi günden güne artış göstermektedir. Bitcoin sahibi olabilmek için açık kaynak kodlu cüzdan yazılımının bilgisayara ya da mobil telefona indirilmesi gerekir. Sanal cüzdanla işlem yapabilmek yani Bitcoin alabilmek için Bitcoin borsalarına başvurulabilir, Bitcoin ATM'lerinden (Otomatik Vezne Makinesi) alışveriş yapılabilir ya da BTC madenciliği yapılarak daha uzun bir yol seçilebilir. Alınan Bitcoinler kişi veya kuruluşlardan mal veya hizmet karşılığı kullanılır [35].



Şekil 3.19: Bitcoin ATM'si [36].

Bitcoin'in ve diğer kripto paraların temini için kullanılan ATM'lerin sayısı dünyada gün geçtikçe artmaya devam etmektedir. CoinATMRadar tarafından sağlanan bilgiler ışığında dünya çapında 5.000 civarı Bitcoin ATM'si olduğu saptanmıştır. Bu ATM'lerin yüzde 75'i Amerika Birleşik Devletleri'nde, yüzde 22'si Avrupa'da bulunmaktadır. Türkiye'de 2021 yılı itibarıyla tamamı İstanbul Avrupa yakasında (Mecidiyeköy, Şişli, Nişantaşı) olmak üzere toplam 3 adet Bitcoin ATM'si bulunmaktadır. Dünyada 4,3 milyondan fazla dijital paraları desteklemeyen (geleneksel) ATM bulunuyor ve gelecekte bu ATM'lere Bitcoin'i destekleyecek yazılımlar yüklenmesi bekleniyor. Geleneksel ATM'lere kripto para birimini destekleyecek yazılımlar üzerinde çalışmalar devam ediyor [32], [36].

3.4. BITCOİN İLE İLGİLİ FİNANSAL VE TEKNİK ELEŞTİRİLER

Bitcoin'in, resmi para birimlerine alternatif olabilirliğine ilişkin, Nobel ödüllü Paul Krugman'ın The New York Times gazetesindeki yorumuna değinecek olursak; Krugman, Bitcoin başta olmak üzere kripto paralardan bazı sebeplerden dolayı kuşku duymaktadır. Örneğin altın ve değerli madenlerin, gerçek hayatla bağlarının bulunduğunu ve mücevher olarak kullanıldığını belirtmektedir. Kripto paraların ise gerçek hayata dair bir dayanağının bulunmadığını düşünmektedir. Devletlerin vergi toplama aracı olarak resmi para birimi değerlerini kabul ettiğini ancak kripto paraların herhangi bir kuruluşa bağlı olmadığını dile getirmektedir. Bunun karşılığında dünyaca ünlü soru cevap sitesi Quora'da yazar olan Ellery Davies kendi makalesinde Krugman'ın tezine karşı çıkıyor. Davies'e göre Bitcoin, toplumu geleceğe taşıyor. Değerli madenlerin alışveriş ya da yatırımlarda transferleri zor olduğu için artık kullanılmak istenmediğini düşünüyor. Ayrıca Davies, Bitcoin'in herhangi bir kurum ya da kuruluşa bağlı olmamasını, kurumlardan soyutlanmış bir şekilde kendi değerini kendisinin oluşturmasını avantaj olarak görmekte ve bu sayede insanların Bitcoin'e karşı olumlu tutumlarının arttığını belirtmektedir. Davies, Bitcoin'in devletlerin vergi toplama geleneğini bitirdiği görüşüne de karşı çıkmaktadır. Bitcoin kayıtlarının güvenli işlemlerden geçtiğini ve bu sayede suça aracılık edilmediğini söylemektedir. FinTech İstanbul ve Blockchain Türkiye Platformu Genel Yayın Yönetmeni, Blockchain 101 kitabının yazarı Ahmet Usta ise her iki yazıdan Ellery Davies'in yazısını daha haklı görüyor. Ahmet Usta; Bitcoin'in, geleceğin ekonomik modelleri için bir ışık niteliğinde olduğunu fakat Bitcoin bu sürecin içerisinde ne kadar barınabilir bunu kestirmenin zor olduğunu düşünmektedir [37], [38].

Bitcoin üzerine olan endişelerden biri de kişilerin Bitcoin alıp şifrelerini unutmalarından kaynaklanıyor. Eğer alınan Bitcoin'in şifresi unutulduysa ya da kaybedildiyse Bitcoinlere ulaşılamıyor. Bitcoin alan birey hayatını kaybederse Bitcoin atıl vaziyette kalıyor ve yine Bitcoin'e ulaşılamıyor, mirasçılara da intikal edilemiyor. Kara para aklama, silah ve uyuşturucu ticareti gibi işlemleri kolaylaştırıcı durumlar Bitcoin hakkında olumsuz tutumlara yol açmaktadır. Dolaşımdaki Bitcoinlerin hangi amaç için kullanıldığı bilinmemektedir. Tüm bu risklere rağmen Bitcoin'e olan talebin artmasıyla Bitcoin fiyatlarındaki değişimler, risk almayı seven kesimlerin dikkatini çekmeyi başarmıştır. İktisatçıların çoğunun Bitcoin'e karşı tutumu

olumsuzdur. Finansçılar ise Bitcoin'in, geleceğin ekonomisine fırsatlar sunacağını savunmaktadır [38].

3.4.1 .Bitcoin'in Avantajları ve Dezavantajları

Tüfek [39]'in. çalışmasına göre kripto para Bitcoin, avantaj ve dezavantajlarıyla birlikte günümüz küresel dünyasında yerini almaya devam etmektedir. Bu avantaj ve dezavantajlar aşağıda maddeler halinde açıklanmıştır.

3.4.1.1. Bitcoin'in avantajları

Kripto paralar içerisinde en çok kullanıma sahip olan Bitcoin, birçok avantaja sahiptir. Bu avantajların en önemlileri aşağıda sunulmaktadır.

- i. Bitcoin bir otorite tarafından kontrol edilmediği için eşler arası takas maliyetleri düşüktür.
- ii. Vergi beyanı gibi bürokrasi yaptırımlarından uzaktır.
- iii. Mahremiyet esasına dayalı sistemde sahtekârlık yapılması ihtimali yok denecek kadar düşüktür.
- iv. Bitcoin, sabit bir büyüme oranıyla programlandığından ve maksimum üretim miktarı sınırlı olduğundan enflasyona maruz kalmamaktadır. Bitcoin'in değerinde emisyon kaynaklı bir düşüş yaşanmamaktadır.
- v. Fiziksel bir para olmadığı için taşıma gibi bir zorunluluğu yoktur.
- vi. Hiçbir banka ya da kuruluş Bitcoin işlemlerini engelleyemez ya da yapılan işlem üzerinde değişiklik yapamaz.

3.4.1.2. Bitcoin'in dezavantajları

Bitcoin'in sağladığı avantajların yanı sıra dezavantajları da bulunmaktadır. Bu dezavantajlardan bazıları aşağıda belirtilmektedir.

- i. Gelişme gösteren bir alan olan blokzincir teknolojisinin herhangi bir yasal zemini bulunmamaktadır. Bu da birçok işletmeyi Bitcoin kullanımı ile ilgili şüphelere düşürmektedir.

- ii. Fiyat dalgalanmalarının yüksek olması Bitcoin'i kullanmak isteyen tarafların çekincelerine yol açmaktadır.
- iii. Bitcoin üretimi esnasında harcanan elektrik sarfıyatı her geçen gün artmaktadır. Artan elektrik sarfıyatı, Bitcoin üretim maliyetlerine olumsuz yansımaktadır.
- iv. Bitcoin cüzdanı ya da Bitcoinler kaybedildiğinde bir daha ele geçirilmesi imkânsızdır.
- v. Blokzincir teknolojisi çok yeni olduğu için siber saldırılara maruz kalmaktadır.
- vi. Bitcoin işlemleri hata kabul etmez bir yapıya sahiptir; bir işlem yapıp madencilerin onayından geçtikten sonra yapılan işlemin geri dönüşü imkânsızdır.
- vii. Yasal zemini olmayan bir otorite tarafından kontrol edilemeyen Bitcoin fiyatları spekülâtif yatırımcılar nedeniyle ani iniş ve çıkışlara maruz kalmaktadır.

4. ALTCOINLERİN KRİPTO PARA PİYASASINDAKİ YERİ

4.1. KRİPTO PARALAR İÇERİSİNDE ALTCOİNLER

Altcoinler, Bitcoin'in altyapısı olan blokzincir teknolojisi baz alınarak tasarlanmış ve iş ispatı, para arzı gibi özellikleriyle Bitcoin'den farklılık gösteren şifreli paralardır. Altcoinler, Bitcoin altyapı fikirleriyle beslenmesine rağmen Bitcoin kadar popüler olamamış, toplumsal platformda Bitcoin kadar kabullenilmemiş olsa da Bitcoinlere rakip olarak geliştirilmiştir [39].

2008'den 2011'e kadar tek kripto para olarak kalan Bitcoinlerin popüler olması yeni Bitcoin benzeri kripto paraların piyasaya girmesini sağlamıştır. Böylece şifreli para alanında yazılım uzmanları, blokzincir teknolojisinin insanlara sorunsuz ve daha verimli hizmet vermesi amacıyla çalışmalarına devam etmektedir. Bu amaçlar doğrultusunda açık kaynak kodlu yapıya sahip kripto paraların kodları ve blokzincir üzerinde bazı oynamalar yaparak farklı özelliklere sahip, Bitcoin'den esinlenerek çıkarılan şifreli paralar piyasalarda yerini almıştır. Bu paraların ilki 2011 yılında piyasaya giren Litecoin (LTC)'dir. 14.07.2021 tarihi itibarıyla 2267 kripto para altcoin bulunmaktadır ve kripto paraların dünya pazarındaki toplam payı yaklaşık 290 milyar dolardır. Söz konusu altcoinler piyasalarda Bitcoin'e benzer şekilde işleme tabidir. Bitcoin, yaklaşık 190 milyar dolarlık pazar payı ile kripto paralar içinde en yüksek orana sahiptir [40].

Tablo 4.1: Piyasa Değerine Göre Sıralanmış Kripto Para Birimleri [41].

#	İsim	Fiyat (USD)	Değ (24S)	Değ (7G)	Sembol	Fiyat (BTC)	Piy. Değ	(24S) Hac.	Toplam Hac. %
24	 OMG Network	6,5719	+16,44%	+174,26%	OMG	0,00056475	\$922,82M	\$1,59B	2,07%
17	 Cosmos	7,5362	+20,09%	+24,08%	ATOM	0,00064686	\$1,52B	\$678,24M	0,88%
19	 Neo	18,1133	-2,02%	+19,44%	NEO	0,00155387	\$1,28B	\$488,50M	0,64%
16	 Monero	91,696	-1,19%	+2,06%	XMR	0,0078894	\$1,62B	\$70,62M	0,09%
9	 Crypto.co Coin	0,1708	+1,17%	+1,71%	CRO	0,00001464	\$3,33B	\$96,29M	0,13%
18	 USD Coin	0,999652	+0,01%	-0,03%	USDC	0,00008582	\$1,35B	\$305,65M	0,40%
4	 Tether	1,0012	+0,06%	-0,05%	USDT	0,00008599	\$10,02B	\$28,85B	37,56%
20	 UNUS SED LEO	1,2655	-0,36%	-1,02%	LEO	0,00010883	\$1,27B	\$12,31M	0,02%
25	 Dash	91,81	+3,99%	-1,15%	DASH	0,00795822	\$896,35M	\$190,24M	0,25%
1	 Bitcoin	11.625,4	+0,40%	-1,49%	BTC	1	\$215,19B	\$17,63B	22,95%
7	 Litecoin	59,650	+0,08%	-2,76%	LTC	0,0051351	\$3,91B	\$2,16B	2,81%
23	 Huobi Token	4,6525	+1,10%	-3,28%	HT	0,00039913	\$993,84M	\$63,81M	0,08%
3	 XRP	0,28254	+1,13%	-4,93%	XRP	0,00002437	\$12,76B	\$1,17B	1,53%
14	 Stellar	0,10141	+0,70%	-5,29%	XLM	0,00000872	\$2,09B	\$172,64M	0,22%
5	 Bitcoin Cash	283,84	-0,11%	-5,96%	BCH	0,0244868	\$5,28B	\$1,05B	1,37%
11	 Binance Coin	21,8016	-0,99%	-6,19%	BNB	0,00187786	\$3,16B	\$204,37M	0,27%
21	 IOTA	0,38577	-3,60%	-7,05%	MIOTA	0,00003319	\$1,07B	\$21,13M	0,03%
22	 VeChain	0,018000	-0,65%	-7,14%	VET	0,00000155	\$1,00B	\$126,70M	0,16%
15	 TRON	0,024479	-1,55%	-7,87%	TRX	0,00000211	\$1,76B	\$660,33M	0,86%
2	 Ethereum	390,68	+0,19%	-8,22%	ETH	0,0336863	\$44,08B	\$8,32B	10,83%
8	 Bitcoin SV	195,35	+0,99%	-10,43%	BSV	0,0168403	\$3,63B	\$622,95M	0,81%
10	 Cardano	0,122180	-1,58%	-10,97%	ADA	0,00001051	\$3,17B	\$257,65M	0,34%
12	 EOS	3,3473	+1,98%	-11,67%	EOS	0,00028801	\$3,14B	\$1,91B	2,48%
13	 Tezos	3,46402	+0,43%	-16,16%	XTZ	0,00029978	\$2,59B	\$182,12M	0,24%
6	 Chainlink	14,92	-2,36%	-21,22%	LINK	0,00129278	\$5,27B	\$1,61B	2,10%

Tablo 3.2’de piyasa değerine göre sıralanan kripto paraların fiyatları, hacimleri ve dolaşımdaki arzları gösterilmektedir. Dolaşımdaki miktarı diğer kripto paraların dolaşım miktarına göre daha düşük olmasına rağmen fiyatının bir hayli yüksek olması sebebiyle Bitcoin, piyasa değeri bakımından birinci sırada yer almaktadır. Tabloda dikkat çeken bir diğer kripto para dördüncü sırada yer alan Bitcoin Cash’dir. Bitcoin Cash, Bitcoin’in blokzincir teknolojisi üzerinde yapılan yeni kodlama (çatallama) ile üretilmiştir.

4.1.1. Litecoin (LTC)

Charlie Lee tarafından 2011 yılında piyasaya sürülen Litecoin, Bitcoin’in açık kaynak kodlu yazılımlarından esinlenilerek Bitcoin’e rakip olarak geliştirilmiştir. Litecoin’in genel özellikleri Bitcoin ile aynıdır fakat daha hızlı işlem onaylama ve daha çok işlem depolama yeteneğine sahiptir. Litecoin, SHA 256 Hash algoritmasının aksine daha fazla hafızaya sahip SCRYPT (kriptografik şifreleme) algoritmasını kullanmaktadır ve Litecoin madenciliği güçlendirilmiş ev bilgisayarları (CPU ve GPU) ile yapılmaktadır. Bu sayede Bitcoin madenciliği için üretilen ASIC bilgisayarların piyasadaki üstünlüğü kırılmak istenmiştir. Bloklar, Litecoin yazılımında her 2,5 dakikada bir, blokzincire eklenmektedir ve 84 milyon adet Litecoin üretilebilecektir [36].

Grafik 3.1’de LTC/USD fiyatında 2017 yılının 2. çeyreğine kadar önemli bir değişiklik meydana gelmediği gözlemlenmektedir. 2017 yılı 2. çeyreğinden sonra Litecoin fiyatında Bitcoin ile paralel ani fiyat dalgalanmaları yaşanmıştır. Litecoin fiyatı 2017 yılı son çeyreğinde ise maksimum seviyelere ulaşmıştır. 16.08.2021 tarihinde Litecoin fiyatı 75,34 USD, piyasa değeri 4.750.497.399 USD, dolaşımdaki arzı 63.050.118 LTC’dir.



Şekil 4.1: LTC/USD Fiyat Grafiği [41].

4.1.2. Ethereum

Kuzey Amerika Bitcoin konferansında, kurucusu Vitalik Buterin tarafından 2015 yılında tanıtımı yapılan Ethereum, Ether (ETH) para birimini kullanan kripto işletim protokolüdür. Ethereum'un amacı blockzincir teknolojisini maksimum seviyede geliştirerek daha geniş alanlara taşımak, kullanıcıların bu sistemle birlikte yeni yazılımlar oluşturmasını sağlamak, kendi kendine yeten merkezi olmayan ve üçüncü şahıslar tarafından farklı amaçlara sürüklenemeyen, engellenemeyen ve sansürlenemeyen bir sistem oluşturmaktır. Ethereum akıllı bir finans platformu yakalama çabasıdır. Bu sistem için güçlü altyapısı olan blokzincir altyapısını kullanmaktadır. Üçüncü şahısları aradan çıkarmak için Ethereum sisteminde işlemler dağınık, anonim bir şekilde sınırsız sayıda ve farklı bilgisayarlar üzerinde korunmaktadır. Bu şekilde bilgilere tek elden ulaşmak ve hükmetmek imkânsız hale gelir. Ayrıca internet, merkezsiz bir yapıya dönüşerek herhangi bir zümre kurum ya da kuruluş tarafından yönetilemez hale gelir. Ethereum'un kullanıcılara yeni yazılım imkânı tanınması kullanıcılar tarafından birçok altcoin çıkarımını sağlamaktadır. Ethereum'un en önemli özelliği, arabulucuları ortadan kaldıran, şeffaf ve otomatik işleyiş mekanizmasını ihtiva eden akıllı sözleşmelere (kontratlar) sahip olmasıdır [41].

4.1.2.1. Akıllı kontratlar (smart contracts)

Akıllı kontrat protokolüne göre değerli varlıklar üzerinden yapılan sözleşmeler; noter, avukat gibi arabulucular olmaksızın, ihtilaflardan uzak ve şeffaf bir şekilde yapılmaktadır. Akıllı kontratlar, sözleşme ile ilgili kuralları ve cezaları belirleyip bu yükümlülükleri zamanı gelince otomatik olarak yerine getirir. Akıllı kontratlar sayesinde yapılan işlemler; herhangi bir kurum, kuruluş onayı olmadan özerk bir şekilde, yedekleme ve kayıtlarda güvenlik, hız, tasarruf ve doğruluk sağlanmış olarak blokzincire kodlanmaktadır. En akıllı sözleşme, Ethereum blok platformunda çalışmaktadır. Akıllı kontratları yazmak için “Solidity” denilen program dili kullanılmaktadır [42].

4.1.2.2. Akıllı kontratların kullanım alanları

Akıllı kontratların gelecekte kullanım alanı potansiyeli yüksek görülmektedir. Bu kullanım alanlarına yönetim, emlak, sağlık hizmetleri ve tedarik zinciri alanları gibi örnekler verilebilir. Bu örnekler İnci ve Alpen [43]'in çalışmasına göre aşağıda maddeler halinde açıklanmaktadır.

i. Yönetim Alanı

Şirketlerin iş yükü günden güne artmaktadır. Bu da şirketlerin güvenli iş kaydı yapmasını zorlaştırmaktadır. Blokzincir, yönetim ile ilgili iş operasyonlarını ve menkul kıymetleri güvenli, otomatik ve şeffaf bir şekilde depolayabilir.

ii. Emlak Alanı

Emlak alanında bir ev, arsa satılmak ya da kiraya verilmek isteniyorsa aracı kurumlara para ödmeden kripto para birimi üzerinden sözleşmeyi dijital deftere yani blokzincire kodlamak yeterlidir. Bu şekilde emlak işlemi herkes tarafından otomatik olarak görülmektedir.

iii. Sağlık Hizmetleri Alanı

Hastane üst düzey çalışanları gibi özel bireyler ile paylaşılabilen kişisel sağlık kayıtları güvenli bir şekilde blokzincir defterine kaydedilebilir ve ameliyat faturalarının ilgili kişilere otomatik bir şekilde blokzincir üzerinden gönderimi sağlanabilir. İlaç denetimleri ve hastane test sonuçları güvenli bir şekilde blokzincire kodlanabilir.

iv. Tedarik Zinciri Alanı

Tedarikçi ve alıcıların bulunduğu tedarik zinciri, kâğıt üzerinde yapılan prosedürler nedeniyle sekteye uğrayabilmektedir. Blokzincir üzerinden yapılan alışverişler ve ödemeler akıllı kontratlar sayesinde otomatik bir şekilde taraflar arasında sağlanmaktadır.

4.1.2.3. Ethereum ile bitcoin arasındaki benzerlikler ve farklar

Kripto paralar içerisinde Bitcoin'in, en yakın rakibi Ethereum ile arasında bazı benzerlikler ve farklar bulunmaktadır. Bu benzerlik ve farklar [41] ve [43] web adreslerinden derlenerek aşağıda maddeler halinde sunulmaktadır.

Ethereum ve Bitcoin arasındaki benzerliklerden bazıları aşağıda sunulmuştur.

- i. Bitcoin gibi Ethereum da blokları ihtiva eden işlem zincirine sahiptir. Bu blokzincirler madenciler tarafından önceki bloklarla bağlantı kurularak oluşturulur.

Ethereum madencileri arttıkça alacakları ödül de günden güne azalmaktadır.

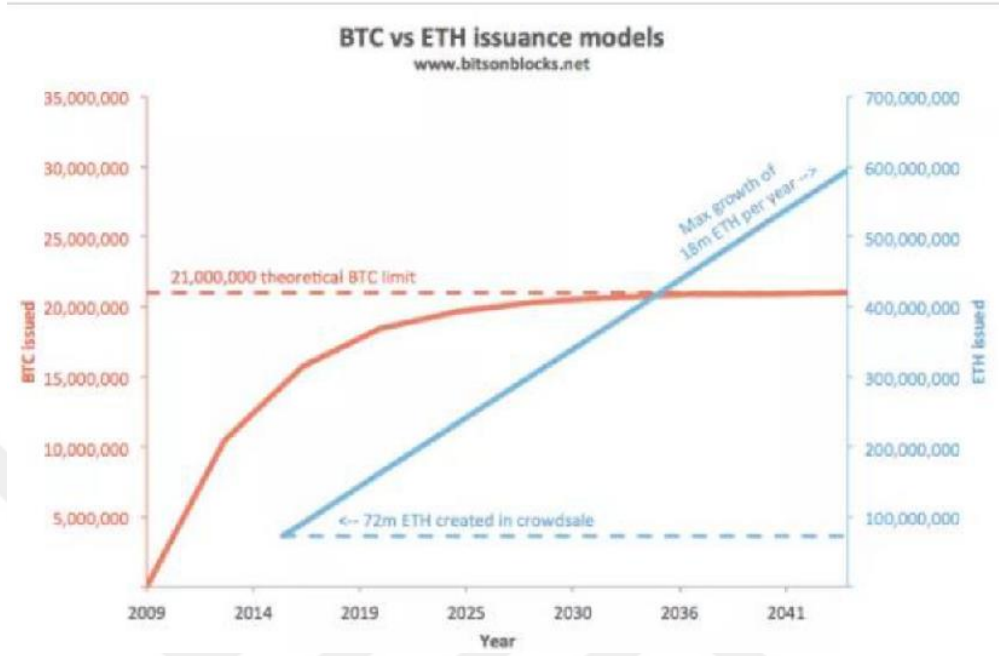
- i. Ethereum ağı Bitcoin ağı gibi herkese açık bir ağıdır.
- ii. Ethereum, iş kanıtı olarak Proof of Stake (PoS) yani hisse ispatı algoritması ile yapılan madencilğe sahiptir. PoS algoritması da PoW algoritmasına benzer yapıdadır fakat madencilikte blok ödülü değil işlem ücreti alınır. Ayrıca daha uygun maliyetle ve daha hızlı çalışır.

Bu benzerliklerle birlikte Ethereum ve Bitcoin arasındaki bazı farklar da aşağıda açıklanmıştır.

- i. Ethereum ve Bitcoin arasındaki en büyük fark, Ethereum'un bünyesinde Solidity yazılım dili ile programlanmış akıllı sözleşmeleri ihtiva etmesidir. Sözleşmelere göre taraflar vaatlerini yerine getirdiği anda otomatik olarak hazır protokol üzerinden para akışı sağlanmaktadır.
- ii. Bitcoin ile yapılan ödemelerde sistem, adres üzerinden ödeme yapıyor; kişinin adresinde 100 BTC varsa ve ödeme yapması gereken miktar 80 BTC ise 100 BTC'lik adresi kayboluyor yerine 80 BTC ödeme yapılan adres ve para üzeri olarak kişiye dönen 20 BTC'nin bulunduğu adres var oluyor. Yani bir adres kayboluyor yerine de iki adres ortaya çıkmış oluyor. Ethereum'da ise hesap üzerinden ödemeler yapılmaktadır. Kişinin hesabında 100 ETH varsa hesabı 80 ETH azalıyor ve ödeme yaptığı hesap 80 ETH artıyor [44].

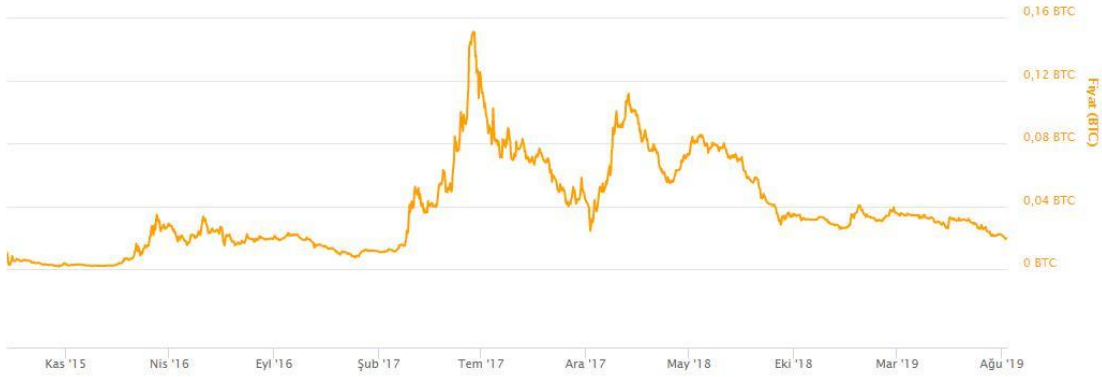
- i. Bitcoin madenciliğinde ASIC bilgisayarlarla yapılan işlemler Ethereum madenciliğinde hemen hemen her bilgisayarda kolaylıkla ekran kartı GPU (ekran/grafik kartı) ile yapılabilir.
- ii. Ethereum'un bloklar arası kurulumu daha kısadır. Bitcoin'de 10 dakikalık bir sürede bloklar bağlanırken Ethereum'da bu süre yaklaşık 15 saniyedir ve her bloktan 5 Ether çıkmaktadır. Ethereum işlemleri daha kısa sürede gerçekleşmektedir.
- iii. Ethereum'un blok boyutu 2 KB'ın altındadır oysaki Bitcoin'in blok boyutu 1 MB olmaktadır. Ethereum bir blokta daha fazla işlem barındırmaktadır.
- iv. Bitcoin'in yazılım tabanı değişen şartlara uyum sağlamak ve değişiklik yapmak için yavaştır. Ethereum ise farklılıklara uyum sağlayıp programlanabilir.
- v. Ethereum bloklarında işlem kopyaları, blok numaraları ve zorluk dereceleri bulunmaktadır.
- vi. Bitcoin madenciliğinde Bitcoin miktarı 21 milyona ulaşınca üretimi bitecektir. Ethereum'un üretim sınırı yıllık 18 milyondur.

Şekil 4.2'de BTC'nin üretimi yaklaşık her 4 yılda bir yarıya düşerek 21 milyona ulaştığında bitecektir. ETH'nin üretimi ise her yıl sabit sayıda devam edecek olup yıllık 18 milyonla sınırlandırılmıştır.



Şekil 4.2: Ethereum/Bitcoin Fiyat Grafiği (Son 5 Yıl) [44].

Şekil 4.3'te Ethereum/Bitcoin fiyatının son 5 yıl verileri incelendiğinde 2016 yılının ilk çeyreğine kadar önemli bir fiyat değişimi görülmemektedir. 2017 yılı başından 2018 yılı sonuna kadar ani fiyat dalgalanmaları yaşanmıştır. 2021 yılında ise Ethereum/Bitcoin fiyatındaki dalgalanmalar son bulmaktadır. 16.08.2021 tarihinde Ethereum/Bitcoin fiyatı 0,017 BTC'dir.



Şekil 4.3: ETH/USD Fiyat Grafiği (Son 5 Yıl) [44].

Şekil 4.3'te ETH/USD fiyatının son 5 yıl içerisinde ETH/BTC fiyat dalgalanmaları ile paralellik gösterdiği gözlemlenmektedir.

16.08.2021 tarihinde:

Ethereum fiyatı: 185,63 USD

Ethereum piyasa değeri: 19.927.311.357 USD

Ethereum dolaşımdaki toplam arz: 107.348.050 ETH'dir.

4.1.3. EOS

EOS, Dan Larimer'ın ekibi tarafından tasarlanarak 2017 Temmuz ayında piyasaya çıkmıştır. EOS'un kendi blokzinciri vardır ve madencilik yapılmaz. EOS da Ethereum gibi akıllı sözleşmeler geliştirmeye uygundur. Ayrıca Ethereum'dan daha hızlı ve esnek çözümleri olduğu için Ethereum'a güçlü bir rakip haline gelmiştir. Blokzincir teknolojisi açısından Ethereum ile aynı özelliklere sahip EOS, bazı çözümleriyle Ethereum'dan ayrılmaktadır. Yapılan işlemlerde veya yayımlanan verilerde herhangi bir hata varsa bunu tüm kullanıcılar görebilmekte olup işlem yapan kişi anında uyarılarak kişinin veriyi düzeltmesine imkân sağlanmaktadır. EOS çok fazla işlemi saniyeler içinde birbirleriyle çakıştırmadan çözebilme kapasitesine sahiptir ve kullanıcılarına belli (%5'lik) bir pay ayıracağını belirtmiştir [45].

Ethereum'un en güçlü rakibi olarak görülen EOS 2017 yılında piyasaya çıktığı andan itibaren fiyat dalgalanmalarına maruz kalmıştır.

4.1.4. Ripple (XRP)

Xripple kripto para (XRP) Ripple adında kurulmuş şirketin çıkarmış olduğu üç adet üründen birisidir. Şirket kurulmadan 100 milyar tane XRP üretmiştir ve daha fazla XRP üretilmeyeceği için madenciliği yapılmayacaktır. Ripple bloklarının üretimi iş kanıtı mutabakatında PoW kullanılmaktadır. Taraflar arasında transferler sonucu komisyon olarak Ripple kesilmekte ve bu kesilen miktar piyasadan silinmektedir. Rippleler tamamen piyasada bitince muhtemelen aynı özellikte yeni kripto paralar çıkarılacaktır. Kripto para Ripple ile para aktarımları döviz üzerinden yapılmamaktadır. XRP ile transferler hızlı ve düşük komisyonlar ile yapılmaktadır. Ripple şirketinin diğer iki ürünü XCurrent ve XVia'dır. XCurrent, bankalar tarafından tercih edilen, Swift benzeri bir sistem olarak çalışan, uluslararası ödemelerde kripto para değil de döviz kullanılan bir üründür. XVia ise XCurrent benzeri fakat bankaların yanında kurumların ve şirketlerin kullanımını da gerçekleştirebildiği bir üründür [46].

5. KRİPTO PARA MADENCİLİĞİ VE UYGULAMALARI

Blockchain sistemi aracılığıyla kripto para basma veya basma işlemi madencilik olarak bilinir. Madencilik sisteminde, bilgisayarların performansına uygun olarak matematiksel algoritmalar çözülerek işlemler bilgisayar sistemi tarafından gerçekleştirilir. Madencilik işlemlerini gerçekleştiren kişilere veya bilgisayarlara madenciler de denir. Kripto para madencileri olarak adlandırılan bu kişiler veya bilgisayarlar, alışveriş yaparken bilgileri kontrol eder ve orada bulunan bilgileri güncelleyerek güvenilir bir satın alma işlemi yapılmasına yardımcı olur. Yani, kripto para birimlerini kapsayan defterlerin herhangi bir hata içermediğinden emin olmakla ilgilenirler. Önemli olan bu notebookların tüm bilgisayarlarda aynı anda aynı şekilde var olması. Bu, kişilerin bir devir işleminden sonra yapılan işlemlere itiraz etme hakları olmadığı anlamına gelmektedir [47].

Bu bağlamda madencilik, kripto para işlemlerinin doğrulanması süreci olarak da ifade edilebilir. Bu süreç ayrıntılı olarak açıklanacak olursa, ağdaki katılımcılar her 10 dakikada bir blok adı verilen ve giderek zorlaşan matematiksel denklemleri çözerler. Her blokta bir işlem, önceki bloğa bağlı olarak işlenir. Bu nedenle herhangi bir bilgiyi değiştirmek, çok fazla bilgiyi değiştirmeyi gerektirir. Bu işlemin kolay olmaması, değiştirme işlemini neredeyse imkansız hale getirmektedir. Dolayısıyla böylesine zor bir sistemde madenciler vardır; Bilgileri doğrulama, güncelleme ve kaydetme ve yeni bir bloğu çözme gibi görevleri vardır. Bu işlemleri yapan madenciler ödüllendirilir. Bu, madencilerin bir bloğu her doğru çözdüğünde, madencilerin işlem ücreti ve küçük bir ödül alacağı anlamına gelir. Örneğin, yarattıkları her yeni bitcoin için 21 milyona ulaşana kadar az miktarda bitcoin ile ödüllendirilirler. Bu ödüller, piyasaya yeni kripto para birimlerinin girmesini sağlar [48], [49].

Madencilerin ödülü Bitcoin ile ilgili olarak değerlendirilirse, Bitcoin'deki ödül başlangıçta 50 BTC iken, ödül her 210.000 blokta bir yarıya indirilir. Her 10 dakikada bir blok kaydedildiği ve ödülün Kasım 2012'de 25 BTC'ye düştüğü bilgisine dayanarak, bu BTC ödülünün son zamanlarda daha da azalması bekleniyor [49].

Tüm bu vakalar, madenciliğin kripto para işlemlerinde vazgeçilmez bir kavram haline geldiğini gösteriyor. Bu nedenle, çalışmanın bu başlığı altında kripto para birimleri için bu kadar önemli bir yer tutan madencilik faaliyetleri ve madencilik kavramı detaylı olarak anlatılmıştır.

5. 1. KRIPTO PARA MADENCİLERİNİN GÖREVİ

Kripto para madenciliği, resmi olarak blok zinciri olarak bilinen halka açık bir defter aracılığıyla işlemlerin onaylanması ve eklenmesi süreci olarak tanımlanır. Bu nedenle madencilerin asıl işi, bilgisayarlarla bir takım matematik problemlerini çözmek ve ağdaki işlemin veya bloğun geçerliliğini kontrol etmektir. Öte yandan madencinin işlemleri kademeli; Ekli işlemleri görüntülemek, bu işlemleri onaylamak, işlemleri bloklar halinde paketlemek ve son olarak SHA-256 + (veri) + (tek seferlik rakam) gibi bir sayı tahmin etmek. Son adım olan SHA-256, bir şifreleme algoritmasıdır ve çalışmanın ilk bölümünde ayrıntılı olarak açıklanmıştır. Benzersiz bir sayı kavramı, madenciler tarafından tahmin edilen rastgele bir tam sayıyı ifade eder. Veriler ayrıca blok içindeki özeti ve önceki bloğun özetini de gösterir. Bu süreçteki zorluk, hedefe ulaşmak için karmanın kodunu çözmektir. Bu zorluklar, yalnızca belirli kişilerin madencilik yapıp yapamayacağı sorusunu gündeme getiriyor. Bu noktada uygun donanım ve internet madenciliğine sahip herkesin yapabileceği söylenmelidir. Burada önemli olan nokta iyi madencilik donanımı, madencilik yazılımı ve kripto para cüzdanıdır. Bu özelliklere sahip kişiler madenci olabilir [50].

5. 2. MADENCİLİK ÇEŞİTLERİ

Başlangıçta normal bilgisayar ekranlarından işlemler yapılabilirdi ancak zamanla blok sayısı arttıkça işlemleri gerçekleştirmek için yeni ekran kartlarına, yeni programlara ve işlemcilere ihtiyaç duyuldu. Bu, çeşitli madencilik biçimlerine yol açmıştır. Çalışmanın bu bölümünde video kartı madenciliği, bulut madenciliği ve madencilik havuzları gibi madencilik türleri isimlendirilmiştir [51].

5. 2. 1. Ekran Kartı ile Madencilik

Madenciliğin ilk günlerinde oyuncu kartlarıyla madencilik oldukça basitti ve grafik kartları artık dünya pazarında bulunmuyordu. Bu kartlar haftanın her günü ve her saati tam kapasite çalışacak

şekilde tasarlanmadıkları için birkaç ay gibi kısa bir sürede performans düşüşü görülmeye başlandı. Bu durum sadece madencilik için ekran kartları üretme fikrine yol açtı ve madencilik için ekran kartları piyasaya sürüldü. Bu sayede sadece madencilik için oyuncu kartlarından daha düşük fiyatlara ekran kartları satın almak mümkün olmuştur [52]. Dünyanın birçok yerinde sisteme katılan yeni işlemcilerin sayısı her geçen gün artmakta ve bu da bilgi işlem gücünün devasa boyutlara ulaşmasına neden olmaktadır. Bu bağlamda, grafik kartı teknolojisine dayalı GPU madenciliği, beraberinde getirdiği avantajlar nedeniyle giderek daha popüler hale geldi. Ancak son zamanlarda Bitcoin'in zorluğunun artması nedeniyle grafik kartı madenciliğinin gelir-gider bilançosunda karlı bir işlem olmadığı anlaşılmış ve madencilere özel üretilmiş işlemciler GPU'nun yerini almış ve bu işlem pek tercih edilmez hale gelmiştir. madencilik Bu konuda ASIC'ler madencilik için kar elde edilebilecek bir zorluk seviyesine ulaşmış ve GPU'ların yerini almayı başarmışlardır. Ancak bu, GPU madenciliğinin tamamen ortadan kalktığı anlamına gelmez. Grafik kartı madenciliği, başta Ethereum olmak üzere altcoin harcayan ve ticaretini yapan kişiler için halen önemli bir yere sahiptir [53].

5. 2. 2. Bulut Madenciliği

Madenciliğin maliyetinin zamanla artmasıyla bireysel olarak madencilik yapmak neredeyse imkansız hale geldi ve bu durum “bulut madenciliği” denilen bir kavramın doğmasına neden oldu. Bulut madenciliği, bir şirketten gerekli madencilik ekipmanlarının kiralanması anlamına gelir. Bu kiralama işlemi; Belirli bir süre için veya ömür boyu kullanıcılar için sabit ve sabit bir fiyatla madenciliği sağlar. Görünüşte avantajlı yapının dışında, ancak kontrol eksikliği, ev sahibinin güvenliği, ödenecek ücretlerin miktarı veya şirketin kırılganlığı gibi dezavantajlar da vardır. Yani bulut madenciliği yapmak isteyen kişilerin dolandırılma riskinin farkında olması gerekmektedir [54].

Bulut madenciliği yöntemi ile madencilik havuzlarına dahil olmak mümkündür. Ancak bu noktada bulut madenciliği ve madenci havuzları birbiriyle karıştırılmamalıdır. Çünkü madencilik için kullanılan cihazlar madenci havuzlarında bulunurken bulut madenciliği ile elde taşınabilir bir cihaz olup olmaması önemli değil, sadece belirli ve düşük bir ücret ve gelir isteniyor [54]. Bu kiralama ücretleri farklı kripto para birimleri için farklılık gösterse de

kiralama ücretlerinin genel olarak kazı başına 1,30 dolar ile 1,40 dolar arasında değiştiği biliniyor. Ancak kripto para birimlerinin öncüsü olan Bitcoin için borç verme ücreti 0,80 USD olup diğer kripto paralara göre daha düşüktür. Buradan diğer kripto para birimlerinin madenciliğinin Bitcoin madenciliğinden daha fazla kâr getirdiği sonucuna varılabilir [55].

5. 2. 3. Madencilik Havuzları

Maden havuzları olarak adlandırılan madencilik havuzları, madencilerin bir blok bulma olasılığını artırmak için kaynaklarını yani madencilik güçlerini bir araya getirme yolu olarak tanımlanmaktadır. Bu havuzlar madencilik yazılımını ve komut dosyalarını korumakla görevlendirilirken, asıl işi her madencinin hash oranını ve üretilen bloklara katkısını tahmin etmektir. Bunu yapmak için madencilik havuzu operatörü her madenci için bir PoW problemi gönderir. Bu noktada madenciler sürekli olarak havuza katılmakta ve havuzun sorununu çözmek için bilgi işlem gücünü kullanmaktadır. Bir madenci her çözüm bulduğunda, madencilik havuzunun yanındaki blok için bir hisse teklif edilir. Bazen madencilik havuzu sorununa gönderilen çözüm, daha zor ağ sorununa da çözüm olabilir [53].

Çoğu madenci, hesaplama çabalarının verimliliğini en üst düzeye çıkarmak için madencilik havuzlarını kullanır. Havuz, bir web sunucusunda veya özel bir sunucuda bulunan bir yazılımdır. Madencilerin havuz sunucusunda hesaplar oluşturduğu ve ardından havuz kimlik doğrulama bilgilerini madencilik yazılımının yapılandırma dosyalarına eklediği yer burasıdır. Kimliği doğrulandıktan sonra, donanımın daha verimli kullanılmasını sağlayan dağıtılmış bir işlem ağında kaynakları paylaşırlar. Bu işlemlerin sonucunda madencilik havuzu bir sonraki bloğu oluşturur ve madenci blok ödülünü kripto para ağından alır. Ancak burada önemli olan nokta, havuzun madenci katkısına ve ödül ödeme planına göre havuzun madencileri arasında bölünmesidir. Yani havuzlarda bloğu bulan cihaz sadece havuz sistemi tarafından bilindiği için kullanıcı hiçbir şekilde ödülün tamamına hak kazanmaz [56].

5. 3. MADENCİLİK ONAY İŞLEMİ

Çalışmanın bu bölümde de en yaygın uzlaşı protokolü olarak bilinen ve madencilerin onaylama işlemini gerçekleştirdiği Emek ispatı (Proof of Work - PoW) ve Pay kanıtı (Proof of Stake - PoS) ayrıntılı bir şekilde açıklanmıştır.

5. 3. 1. Emek İspatı (PoW)

İş kanıtı terimi ilk olarak 1992 yılında Cynthia Dwork ve Moni Naor tarafından spam ile mücadele için kullanıldı. PoW, hizmet saldırılarını önlemenin ekonomik bir yöntemi olarak ifade edilir. Burada bazı aritmetik işlemler talep eden servis veya talepte bulunan kişiler tarafından istenmektedir. Bu yöntemin en önemli özelliği asimetrik olması ve kullanıcıların sisteme erişebilecekleri bir işlevi hesaplamak için bilgi işlem gücü harcaması gerekmesidir. Bu hesaplama, talepte bulunan taraf için orta derecede güçlüklerle sahiptir. Ancak bu, hesaplamanın imkansız olduğu anlamına gelmez. Başka bir deyişle, kaynağa erişerek gereksiz kullanımdan kaçınmak için kullanıcıların orta ve zor olmayan bir işlev hesaplaması gerekir. Servis sağlayıcının işlemi kontrol etmesi çok kolaydır [52].

1992'den yaklaşık 5 yıl sonra Adam Back, Hashcash adıyla Dwork ve Naor'a benzer bir rol başlattı. Hashcash, e-postaların spam olup olmadığını tespit etmek için SHA-1 şifreleme algoritmasını kullanır. Satoshi Nakamoto, dağıtılmış bitcoin defterlerinde kullanılan madencilik işlevi için bu hashcash yönteminden de ilham aldı. Backs Dwork ve Naor'dan bu doğrultuda; Back'den esinlenerek Nakamoto tarafından oluşturulan Bitcoin konsensüs yapısı, SHA-256 şifreleme algoritmasının iki kez uygulanması yöntemine dayanmaktadır. Başka bir deyişle, bu yöntem çift işlem gerçekleştirir. Bu doğrultuda Bitcoin ortamında saniyede bir trilyon hash işleminin yapıldığı ve ortalama olarak her 10 dakikada bir blok üretildiği biliniyor. Blok içerisindeki veriler kullanılarak çalışmanın bir önceki bölümünde bahsedildiği gibi Merkle ağacı ve Merkle kök değeri, bir önceki bloğun hash değeri, zaman bilgisi ve son olarak nonce değeri alınarak blok başlığı oluşturulur. kullanılmış . Daha sonra blok başlığı SHA256 algoritma fonksiyonundan iki kez geçirildikten sonra uygun bir değer oluşup oluşmadığı kontrol edilir. Bu uyumluluk sağlandığında bilgi ağdaki tüm düğümler ile paylaşılır. Hata durumunda ise nonce değeri limitine ulaşınca kadar artırılarak işlem tekrar denenir. Bu şekilde, 2x işlem

gerçekleştirerek yapılan işin kanıtı, blok zinciri platformundaki bitcoinlerde en sık kullanılır. Ancak PoW yönteminin yüksek enerji, özel ekipman ihtiyacı ve artan blok boyutu nedeniyle blok üretim süresinin artması gibi dezavantajları da vardır [28], [52], [57].

5. 3. 2. Pay Kanıtı (PoS)

PoS yöntemi, doğrulama yoluyla ağdaki işlemleri doğrulamanın başka bir yoludur. Bu yöntemin özelliği, kullanıcıların yeni bir coin oluşturmak için herhangi bir işlem yapmalarına gerek olmamasıdır. Bu nedenle, bu yöntem aslında madencilik değil, parasal paralar olarak kabul edilir. Bu yöntem, ödül cüzdandaki para miktarıyla orantılı olarak verildiğinden, para kazanmak isteyen kullanıcıların mevcut elektronik cüzdanlarında para bulundurmalarını gerektirir. Yani elektronik cüzdanda ne kadar çok para varsa o kadar çok ödül kazanılacak ve para üretilenilecektir [58].

PoW yönteminin performansının artması için madencilik cihazlarının sayısının veya performansının artırılması, PoS yönteminde ise cüzdandaki kripto para miktarının artırılması gerekmektedir. PoS yöntemi ile öncelikle sistemdeki bir sonraki bloğu üretecek olan makinenin oranı dikkate alınır ve en yüksek orana sahip olan seçilir. Bu durumda seçilen makinenin bloğu uygun zamanda üretememe ihtimali vardır. Böyle bir durumda bir sonraki makineye aktarılır. Burada yaş kavramı, en yüksek orana sahip makinelerin her zaman birinci üretim önceliğine sahip olduğunu düzenlemek için geliştirilmiştir. Böylece blok üretiminde kullanılan oran kapsamında coinlerin yaş değerleri sıfırlanmakta ve bu kripto paralar bir süre sonra eskimeye başlamaktadır. Bu bağlamda para kazanma kavramına blok üretim süreci denilmektedir. PoS yönteminin bu operasyondaki avantajı; İşlemlerin doğrulanması, blok üretim sürecinin daha hızlı ve kolay hale getirilmesi, PoW yönteminin pahalı ve yüksek enerji tüketimi sorunlarının ortadan kaldırılması. Bu avantajlardan dolayı Bitcoin'den sonra en yaygın kullanılan kripto para birimi olan ve son zamanlarda popülerliği giderek artan Ethereum, PoW yönteminden PoS yöntemine geçiş yapmaya hazırlanıyor. Aynı şekilde mevcut kripto para birimlerinin bir kısmı da PoS yöntemine geçmekte ve yeni yayınlanan kripto para birimleri için PoS yöntemini tercih etmektedir [59].

5. 4. MADENCİLİK ÜCRETLERİ (MINING FEES)

Kripto paraların bir kişiden diğerine transferi blok zinciri sistemi üzerinden gerçekleşir ve bloklardan oluşan bu sistemde kayıt altına alınır. Kripto para madenciliği yapmak isteyen kişiler ve kuruluşlar, işlemlerini yürütmek için bu blokları kullanır. Bu bağlamda madencilerin temel görevi, belirli yazılım programlarını ve yüksek hesaplama gücüne sahip donanımları kullanarak yeni bloklar bulmaktır. Madenciler bulunan her blok için belirli bir ücret alırlar. Bitcoin örneğini incelerken sistem, fazla arzı önlemek için tamamlanan her 210.000 blok için madencilerin kazandığı ücreti yarıya indirir. Bitcoin 2008 yılında Nakamoto'nun yazısıyla gündeme geldiğinde her madenci, madencilerin bulduğu bloktan 50 BTC kazanıyordu, şu anda ise her blok için 12,5 BTC yapıyorlardı. Bu kazanılan ücret veya ücret her 4 yılda bir yarıya indirilir. Bu kademeli olarak blok bulma zorluğunu artırır ve arz miktarının belirli bir oranda azalmasını ve artmasını sağlar. Bu şekilde çalışması, toplam Bitcoin arzının 21 milyon olarak tasarlanmış olmasından kaynaklanmaktadır [60].

5. 5. MADENCİLİK CİHAZLARI

Madencilik faaliyetleri başlangıçta işlemci tabanlı iken ve hesaplama gücü ile hesaplama yoluyla kripto para üretebilirken, kripto para madenciliği daha sonra grafik kartı kullanan cihazlarla gerçekleştirilmiştir. Ancak zaman içerisinde özellikle Bitcoin madenciliğine olan ilginin giderek artması nedeniyle madencilik faaliyetlerinin verimliliği düştüğü için bu hesaplama gücünü kullanan cihazlar ve ekran kartı yetersiz kalmıştır. Buna göre Bitcoin madenciliği uygulamalarına özel entegre devreler kullanan ASIC cihazları kaldırılmış ve bu cihazdan faydalanabilecek zorluk seviyesine ulaşılmıştır. Çalışmanın bu bölümünde bozunma sürecinin uygulanması için büyük önem taşıyan bu cihazlar kısaca anlatılmaktadır [61].

5. 5. 1. GPU Ethereum Madencilik Cihazı ve RİG

Ethereum madenciliği yapmak için grafik işlemcisi olarak bilinen özel bir donanım parçası, yani GPU gereklidir. Ethereum başlangıçta ortalama bir bilgisayar işlemcisi çalıştırılarak çıkarılabilecek şekilde çalışsa da zamanla gelişmiş GPU'lar ile çalışmaya başladı. Bu bağlamda GPU, özel bir Ethereum madencilik bilgisayar olarak adlandırılır. Sistemde Ethereum Directed

Asiklik Graph (DAG) dosyası madenciler tarafından VRAM'a kaydedilir. DAG, madenciliğin artan zorluğuyla birlikte büyüyor. Bugün Ethereum madenciliği, en az 3 GB video RAM'e sahip bir GPU, yani VRAM gerektirir. Ethereum madencilik donanımı üreticileri AMD ve Nvidia'dır. İlk aşamalarda AMD, Nvidia'nın önündeydi, ancak daha sonra Nvidia'nın Titan serisi kartları, AMD ile aralarındaki boşluğu daralttı. İkisi arasındaki fark netleşmeli, AMD kartları daha ucuz ama Nvidia Microsoft Windows ile daha iyi çalışıyor. GPU'nun çalışma bağlamında sadece Ethereum olarak açıklanması, GPU madencilik cihazlarının sadece Ethereum üzerinde kullanılıp kullanılmadığı sorusunu gündeme getiriyor. Bu noktada Ethereum'a ek olarak Monero, Zcash, Vertcoin ve Ethereum Classic gibi 40 civarında farklı altcoinin madencilikte GPU'dan faydalandığını belirtmek gerekir [62].

5. 5. 2. ASIC Bitcoin Madencilik Cihazı

Bitcoin'in ilk günlerinde madenciler bilgisayarların işlem gücüne güvenebilirdi. O zamanlar normal bilgisayarların işlem gücü Bitcoin üretimi için yeterliyken, artan zorluk derecesi nedeniyle bu bilgisayarlar hem işlemi gerçekleştirmek hem de elektrik maliyetleri gibi bazı maliyetleri karşılamak için yeterli değildi. Buna göre, Bitcoin için ASICA Uygulamasına Özel Entegre Devre Cihazları geliştirildi. ASIC teknolojisinin kendine özgü doğası gereği, yalnızca Bitcoin madenciliği yapabilen özel ASIC'ler vardır. Bu ASIC cihazları sayesinde GPU madenciliğinde donanım ve güç maliyetleri gibi dezavantajlar ortadan kaldırılmış ve ASIC cihazının daha fazla işlem gücüne sahip olduğu anlaşılmıştır. ASIC madenciliği Bitcoin madencileri arasında popülaritesini artırırken, GPU'lar buna bağlı olarak arka planda kalmıştır [63].

ASIC cihazlarının ne kadar güçlü olduğunu açıklamak için bir örnek verildiğinde; 4 GPU'lu bir donanım kazısı, 3.4 MH/s'lik bir hash oranı yakalar ve 3600 kW/s tüketirken, bir ASIC cihazı 6 TH/s kazıp 2200 kW/s tüketir. Bu fark, ASIC cihazlarının GPU kazma yönteminden nasıl daha iyi performans gösterdiğini görmeyi kolaylaştırır [63]. Bununla birlikte, tek bir bilgisayarda bir ASIC cihazının bulunmasının benim için yeterli olmadığı belirtilmelidir. Çünkü "solo madencilik" olarak da bilinen tekli madencilik ile sorunu çözmek artık neredeyse imkansız. Bu imkansızlığın bir sonucu olarak kullanıcılar, tek bir bilgisayar yerine yüzlerce

hatta binlerce madencinin dahil olduđu çok daha fazla bilgi işlem gücüne sahip, birkaç kullanıcı tarafından oluşturulan madencilik havuzları olarak adlandırılan madencilik havuzlarında üretim yapmaktadır [64].

5.6. KRIPTO PARA MADENCİLİĞİ UYGULAMALARI

Bitcoin’i araştırmak, bunun en önemli nedenidir. Genel olarak, keşif, blok zincirine eklenen yeni bir blok tasarlamak için hesaplama açısından zor çözümlerin bulunmasını gerektirir. Kripto para madenciliği, muazzam bir somputing power aracılığıyla yürütülen bir kesinleştirme sürecidir. Dünyanın her yerindeki her Bitcoin, ağ ağının doğru ve güvenli olmasını sağlamak için merkezi olmayan bir eşler arası ağa katkıda bulunur. Blok zinciri defterine kesin olarak eklemek için, matematiksel sorunları çözmenin ötesine geçmeyin. Bir çözüm bulunduğunda, onaylanan işlemlerin en son bloğu blok zincirine bir sonraki bağlantı olarak eklenir. Bilinen şey, karmaşık hesaplama matematik problemlerini çözen yüksek performanslı bilgisayarlar tarafından tercih edilir; bu sorunlar, elle çözülemeyecek kadar karmaşıktır ve tamamen çözülemez [65].

Ağa bağlanmak ve katkıda bulunmak için bir teşvik olarak, sorunu çözen kişi Bitcoin’de bir blok ödüllendirilir.

Ağ üzerinde işlem kayıtları ekler ve doğrular. Bloklara blok eklemek için, madenciler birkaç parça ile ödüllendirilir; ödül her 210.000 blokta yarıya inmiştir. Blok ödülü 2009’da 50 yeniydi. 11 MAYIS 2020’de, üçüncüsü 6.25’e kadar düşmüş her blok için ödül getirdi.

Çok çeşitli donanımlar, bunları kullanmak için kullanılabilir. Ancak, bazıları diğerlerinden daha yüksek ödüller aldı. Bazı özel seçenekler, Application-Specific Tümlleşik Circuits (ASIC) ve Graphic оружия gibi daha gelişmiş birimler olarak adlandırılır. Bu laborate mining processors as “mining rigs” olarak bilinir [66].

Bir bitcoin ondalık basamağa bölünebilir (bir bitcoinin 100 milyonda biri) ve bu en küçük birim bir Satshi olarak adlandırılır. Eğer gerekliyse ve eğer birkaç kişi değişikliği kabul ederse, daha fazla ondalık sayıya kadar her şey mümkün olabilir. Bitcoin’in kaybolmasının sonucu iki yönlüdür. İlk olarak, ağdaki bu karmaşık matematik problemlerini çözdüklerinde, bunlar yeni

bir şey değil (bir öncekinden farklı olarak değil). Ve son olarak, madencilerin temel matematik problemlerini çözerek, transaction bilgilerini doğrulayarak tüm ağları güvenilir ve güvenli hale getirirler [67].

Birisi herhangi bir yerde bitcoini bitirdiğinde buna işlem denir. Transactions in-tore veya online yapılan bankalar, mevcut sistemler ve fiziksel receipts tarafından belgelenir. Daha az önce, işlemleri “blok” içinde bir araya toplayarak ve bunları halka açık bir kaynağa ekleyerek “blockchain” olarak adlandırılan aynı şeyi elde edin. Düğümler daha sonra bu blokların en önemlilerindendir, böylece gelecekte doğrulanabilirler. Bitcoin bloklara yeni bir geçiş bloğu eklediğinde, bu işin bir parçası, bu işlemlerin gerçek olduğundan emin olmaktır. Özellikle, çok az şey, “çift taraflı” bir dijital durumun olağandışı bir tuhaflığı olmadığından emin olun. Önceden belirlenmiş bir gerçekle, her zaman geçerli değildir. Ancak genel olarak, mağazada 20 doları ödediğinizde, bu fatura memurun elindedir. Ancak dijital para birimiyle, bu farklı bir hikayedir [68].

5.6.1.Yeni Bitcoin

Yeni Bitcoin keşfetme süreci, herhangi bir başka kaynak için araştırma sürecini anımsattığı için madencilik olarak tanımlanır. Altın arama ile, daha az arama yapın ve altın elde etmek için tüm dünyayı araştırın. Bitcoin ile, mevcut mathematical problems yoluyla Bitcoin bulmak için en az girişim. Blockchain, bunun üzerine inşa edilmiş bir teknolojidir. Herkese açık olarak dağıtılan ve her Bitcoin işlemini kaydeden bir defterdir. Bu, neredeyse tamamen bir bloktur. Her blok, Bitcoin bilgi aktarımı için bir grup değildir. Madenciler, karmaşık matematik sorunlarını çözmek için ortak işleme yöntemlerini kullanarak blok zincirine katkıda bulunurlar. Sorunu çözmek, bloğun listeye çok iyi bir şekilde eklenmesiyle sonuçlanacaktır. Sorunu kesin olarak çözen küçük kişi Bitcoin olarak ödüllendirilir [62].

Yukarıdakiler, Bitcoin madenciliğinin karmaşık sürecinin temelini oluşturur. Ağ ağının güvenli ve doğru olmasına yardımcı olur. Bu ağ, farklı bir ağ üzerinde inşa edilmiştir, her bir madencinin kendi ağlarının birleştirilmesine katkıda bulunduğunu, doğrulayacağını teyit eder. Bitcoin’in yaratıcısı olan Satoshi Nakamoto, ağdaki Bitcoin’i bir blokun en az 10 dakika geçmesine izin

verecek şekilde tasarladı. Bu 10 dakikalık hızın üstesinden gelmek için, matematik problemlerinin zorluğu otomatik olarak ayarlanır [64].

5.6.2.Bitcoin İşlemleri Doğrulama

Bitcoin madencilerinin genellikle geçişleri doğrulamaktan tamamen kazanmalarını sağlamak için, iki şey çok önemlidir. İlk olarak, tek bir büyük veri deposu (MB) değerinde çok sayıda veriyi doğrulamak zorundadırlar, bu da her biri tek bir büyük veri deposu kadar küçüktür.

İkinci olarak, bloklara bir geçiş bloğu eklemek için, daha önce karmaşık bir “işe karşı dayanıklı” olması gerekir. Aslında yaptıkları şey, “ha” olarak adlandırılan 64 basamaklı onaltılık bir sayı bulmaya çalışmaktır. Temel olarak, bir küçük kişi, farklı oranlarda hash’ler çıkarır. Her gün için megahashes (MH/s), mümkün olan ikinci, Bir çözüme ulaşana kadar 64 basamaklı sayılar. Ağustos 2020’deki en son bloğun zor seviyesi 16 trilyondan fazla. Bu, hedefin altında bir bilgisayar üreten bir bilgisayar değişikliğinin 16 trilyonda 1 olmasıdır. Bunu bir perspektife oturtmak gerekirse, tek bir çok sayıda biletle Powerball ikramiyesini kazanmanız, en doğru şeyi seçeceğinizden yaklaşık 44.500 daha fazla muhtemeldir. Ne yazık ki, çoğu zaman bir çok hash ortaya çıktı. Hiçbiri, bitcoin için madencilik, büyük miktarda enerji ve mükemmel bir şekilde birleştirmeyi gerektirir [68].

Zor seviye, 2016 bloğunda veya kabaca her 2 haftada bir ayarlanır, hedeflenen sabit kalma oranları sabittir. Yani, bir çözüm için daha az zaman var, sorun daha zor olacak. Bunun tersi de doğrudur. Hesaplama gücü ağdan çıkarılırsa, zorluk madenciliği daha kolay hale getirmek için aşağı doğru ayarlanır [63].

5.6.3.Madencilik Analojisi

Bitcoin madencileri sadece doğru olanı bulmak zorunda değiller, aynı zamanda bunu ilk yapanlar da olmalı. Daha önce bilgi almak aslında tahmine dayalı olduğundan, daha önce doğru ve doğru cevap vermek, bilgisayarınızın ne kadar hızlı bir şekilde sonuçlanabileceği konusunda yapılacak hemen hemen her şeye sahiptir. Sadece bir on yıl önce, az önce normal masaüstü bilgisayarlarında rekabetçi bir şekilde gerçekleştirilebilir. Bununla birlikte, zaman içinde, grafik kartlarının yalnızca video oyunları için kullanıldığının daha az etkili olduğunu ve

bu oyuna hükmedebileceklerini fark ettim. 2013'te, mümkün olduğu kadar basit, mümkün olduğu kadar basit bir şekilde kullanmak için daha önce kararlaştırılmıştır. Bunlar birkaç yüz dolardan on binlere kadar değişebilir, ancak Bitcoin'de verimliliği daha üstündür [69].

Bugün, sadece en güncel ASIC'ler ile kolayca yapılabileceği artık önemli. Masaüstü bilgisayarlar, GPU'lar veya ASIC'lerin daha eski modellerini kullanırken, enerjinin tükenme maliyeti aslında elde edilen geliri aşıyor. Elinizin altındaki en yeni birim olsa bile, bir müşteri nadiren “madencilik havuzları” olarak adlandırılan şeylerle anlaşılmaya yeter. Bir bilgi havuzu, kendi bilgi işlem becerilerini ve katılımcılar arasındaki madenciliği yapılan bitcoini birleştiren bir madenci grubudur. Beklenmedik bir şekilde çok sayıda blok, bireysel madenciler tarafından değil, havuzlar tarafından kullanılır. Madencilik projeleri ve şirketleri, bitcoin'in üretim kapasitesinin büyük yüzdelere sahiptir [69].

5.6.4.Bitcoin ve Geleneksel Currencies

Tüketici, her zaman en doğru olanı kabul etme eğilimindedir. Bunun nedeni, ABD dolarının ABD'nin merkezi bir bankası tarafından desteklenmesidir, buna Federal Rezerv denir. ABD dolarını kullanan dijital ödemeler bile merkezi bir otorite tarafından desteklenmektedir. Borç veya kredi kartınızı kullanarak çevrimiçi bir satın alma işlemi yaptığınızda, bu işlem bir parça işleme birimi (such as Mard veya V) tarafından gerçekleştirilir. Tüm geçmişinizi yeniden gözden geçirmenin yanı sıra, bu seçenekler, işlemlerin sahte olmadığını doğrular, bu da kredi kartınızdan veya kredi kartınızdan biridir [70].

Öte yandan, merkezi bir otorite tarafından düzenlenmez. Bunun yerine, bitcoin dünyanın “node” olarak adlandırdığı çok sayıda topluluk tarafından desteklenmektedir. Bu ağ, Federal Rezerv, Visa ve Mastercard ile aynı işlevi yerine getirir, ancak birkaç önemli farkla. Düğümler, prior transactions hakkında bilgi depolar ve bunların gerçekliğini doğrulamaya yardımcı olur. Bu merkezi uzmanlardan farklı olarak, ancak, bitcoin node'ları dünyanın her yerinde daha fazladır ve en son bu zamana kadar bir genel listede veriyi işlemektedir [70].

5.6.5.Madenciliğin Tarihçesi

16'da 1'i tuhaf bir şekilde, ölçekleme zor bir seviye ve kabaca 10 dakika içinde gerçekliği doğrulayan devasa ağ. Ancak 10 dakikanın bir kural değil, bir gol olduğunu unutmamak önemlidir. Bitcoin network, Ağustos 2020'den itibaren, her 10 dakikada bir blockchain logged logged ile, şu anda dört ardışık olarak işleniyor. For comparison, Visa somewhere işleyebilir etrafında 65.000 transactions per second.8 olarak the network of bitcoin users continues 10 dakika eventually 10 minutes içinde processed olmak can that işlemlerin sayısını aşması will in to büyümek, ancak, işlemlerin of sayı made. Bu durumda, yerelde bir değişiklik yapılmadığı sürece, geçişler için beklenen zamanlar başlayacak ve daha uzun sürecektir [71].

Bu, bitcoin protokolünün kalbinde yer alır ve “kayıt” olarak bilinir. Bitcoin madencileri genel olarak büyümeyi ele almak için bazı şeylerin yapılması gerektiği konusunda hemfikir olsalar da, bunun nasıl yapılacağı konusunda daha az nahoş durum var. Ölçekleme problemini ortadan kaldırmak için iki ana çözüm olmuştur. Developers, aynı sayıdaki işlemlerle blocekchar tarafından gerçekleştirilmiş olabilecek daha hızlı işlemlere izin verecek şekilde çok basit bir “zincir dışı” katman oluşturmayı önerdi. Blok başına doğrulamak için daha az veri olması nedeniyle, Solution 1, daha az kişi için geçişi daha hızlı ve daha ucuz hale getirecektir. Çözüm 2, daha fazla bilgi için her 10 dakikada bir, büyük bir boşluk bırakarak işlenmesine izin vererek çözecektir [71].

Temmuz 2017'de, madenciler ve madencilik şirketleri, ağın bilgi işlem hacminin yaklaşık %80 ila %90'ını, günlük miktarı azaltacak bir program seçmek için oy kullandı. Daha önce en çok eklenenlere oy verenler, ayrı ayrı veya SegWit olarak adlandırılır. Bu terim, “to separate” anlamına gelen Segregation ve “bitcosnt” to “tignatures” anlamına gelen Witness anlamına gelen bir terimdir. O halde, bir bloktan ayrılmak anlamına gelir - ve bunları bir extended blok olarak attach. Her ne kadar bir çözüm yoluna çok fazla benzemese de, işlenen verilerin %6'sı kadar basit olduğu tahmin edilmektedir [72].

Bir aydan kısa bir süre sonra, Ağustos 2017'de, bir grup küçük ve geliştirici, aynı bitcoin. Bu grup, ölçeklendirmeye yönelik bir çözüm ihtiyacı konusunda hemfikir olsa da, ayrılmış tanık teknolojisini önermenin, bu büyük sorunu tam olarak artırmayacağından endişe duyuyorlardı.

Bunun yerine Solution ile gittiler. Sonuç olarak, “bitcoin cash” olarak adlandırılan sonuç, yaklaşık 2 ay boyunca bir performansa izin vermek için doğrulama işlemini sırayla 8 MB’a çıkardı. 16 Ağustos 2020’de Bitcoin Cash yaklaşık 302\$ ile Bitcoin yaklaşık 11.800\$ arasında değerlendirildi [73].

5.6.6.Gelişen Evrim

2000’li yılların başlarındaki aşamalarda, gerçek şu ki, bunları kullanmanın mümkün olup olmadığıyla ilgilenmekle ilgilenmektedir. Fiyatı artınca, fark etme zorluğu da arttı. Büyüyen zorluğa uyum sağlamak için, daha fazla kapsamlı işleme seçeneği gerekiyordu. Kısa bir süre sonra, daha az zaman geçirmek için oyun bilgisayarları kullandı. Tercihler tekrarlandı ve şu anki bilgi işlem gücü ve miktarı arttı. Sonunda, bilgisayarlar ve şifreler Bitcoin madenciliğinin en iyi çözümü için yaratıldı. Bugün, güçlü bir donanım ve yüksek verimliliğe ve yüksek verimliliğe sahip, verimli bir donanım ihtiyacı duyuyor. Bloklara eklemek için Bitcoin algoritmasını çözmek ve çok büyük bir miktarda yeniden yaşamak. En düşük seviyede tutmak, Bitcoin’i en iyi ve en iyi şekilde elde etmenin anahtarıdır [73].

5.6.7.Ödüllendirme Bitcoin Madencileri

Tek bir günde 300.000’e yakın satın alma ve satışın gerçekleşmesiyle, bu işlemlerin her birinin doğrulanması, küçük işler için çok fazla iş olabilir. . Her seferinde bir blokla birlikte yayınlanan yeni bitcoin miktarına “blok ödülü” denir. Blok ödülü her 210.000 blokta (veya kabaca her 4 yılda bir) yarılanır. 2009’da 50 oldu. 2013’te 25, 2018’de 12,5 ve Mayıs 2020’de 6,25’e düştü. Blok ödülü, çözülen ve bloka eklenen her blok için Bitcoin’in ne kadar ödüllendirildiğidir. Blok ödülü, her geçen 2.016 blok için “yarıya” olarak tasarlanmıştır. “Yarılama” süreci olarak adlandırılır ve her dört yılda bir gerçekleşir [73].

En son yarılanma Mayıs 2020’de gerçekleşti. Aşağıda, 2012’ye kadar uzanan tarihi blok ödülleri bulunmaktadır:

2012: 25.00 BTC

2016: 12.50 BTC

2020: 6.25 BTC

2020’de, bir madenciyi her bloke etmek için, bu madencilerin 6,25 Bitcoins yeniden olacağı anlamına geliyor. Yarılanma, son bloğa kadar devam edecek ve sona erecek. Her bir bloğun 10 dakika içinde inmesiyle, sonuncunun 2140’ta olacağı tahmin ediliyor. Blok ile, ağ madencilerin tüm küresel toplulukları tarafından hizmet verilir. Her biri, her bir işlemin meşruiyetini teyit etmeye katkıda bulunur. Müdahale etmeye teşvik olarak, madenciler hizmetleri için bir blokla ödüllendirilirler. Bu sistem 2140’a kadar devam edecek. Bu durumda, madenciler ağ kullanıcıları arasında geçiş yapma karşılığında ödüllendirilecekler. Bu ücretler, daha az zaman kaybetmemenizi ve ağın devam etmesini sağlar. Fikir, bu bayram için bir şeylerin bitmesinden sonra bunların kısa süre içinde kalmalarına neden olacağıdır [74].

Bitcoin, blok zincirinde farklı bir teknoloji sunar. Mevcut durumun kendisi desantralize edilmiştir, bu da hükümet yeniden yapılandırması ve sona ermesi olmaksızın tüm dünyada geçiş yapılmasına izin verir. Madenciler cryptocurrency’nin azalmasında değerlidir. En son madencilik teknolojisiyle, Bitcoin madenciliği, temel donanımların (bilgisayarların) çıkışına dayalı bir gelir akışını belirlemek için bozulabilir [74]:

Daha az şey, başarılı bir oyun deneyimi için inanılmaz sonuçlarla anlaşmak için en son donanıma sahip olmak zorunda. Ekipman, birkaç yıl içinde eskimiş olabilir. Maliyetli olabilecek en önemli donanıma ihtiyaçları var. En son ASIC mining donanımları bilgisayar başına 1500 doların üzerinde. Güç ana işletme gideri olacaktır. Electricity, kilovat-saat (kWh) başına ücretlendirilir. Mining için profitability, kWh başına 0,03 - 0,08 ABD doları arasında seyredebilir. Birkaç saniyelik bir değişiklik, daha iyi bir deneyim için tüm farkı yaratabilir. Bir kişinin mümkün olan en düşük fiyattan yararlanabilmesi önemlidir [75].

5.6.8.Bitcoin Fiyatı

Bitcoin’in fiyatı, matematik problemlerini doğru bir şekilde çözdüklerinde belirli bir Bitcoin miktarına sahip olmamaları nedeniyle önemlidir. eğer akım Bitcoin block ödülü 6,25 jeton; Bunun çok değerli olmasını isteyeceksiniz. 6,25 saniyeye geri kalırsanız ve Bi’nin fiyatı 5.000

\$ ise, madencilik operasyonunuz büyük olasılıkla uygunsuz olacaktır. Fiyat başına 12.000\$ ise, madencilik operasyonunuz sağlıklı ve kolay bir şekilde çalışabilir.

Yukarıdaki öğelerin doğru karışımı, macerayı çekici bir girişim haline getirir. Değişkenlerin tümü uygunsa, daha az artabilir ve benimki daha iyi olur. Bitirmek için diğer bir çekici neden ise bir yatırım potansiyelidir. En son 100.000 ABD Doları (2020’de 10.000 ABD Doları civarındadır).

Bitmemiş bir Bitcoin miktarı benim için mümkün olduğu için, talep her zaman olduğu gibi daha da artacaktır. Bitcoin, mevcut kullanım için daha fazla tercih edilir hale gelirse, talebe eklenecektir [75].

Bitcoin madenciliğine başlamak için aşağıdakiler gereklidir:

- i. Rekabetçi bilgisayarlar (teçhizatlar)
- ii. Düşük maliyetli güç
- iii. Madencilik yazılımı
- iv. Madencilik pool membership
- v. Deneyim Pools

Bitcoin’in ortaya çıkan fikri, zor geçen sorunların üstesinden gelmek için yükseldi. Küçük bir grup, toplu olarak Bitcoin madenciliği yapmak için bir araya gelen bilgi işlem gücü. Havuz bir bloğu başarılı bir şekilde çözerse, projedeki tüm madenciler, ne kadar güç kullandıklarına bağlı olarak tahsis edilecektir. Bir blok ödülü almanın tek olasılığı düşüktür, ancak binlerce oyun bir araya geldiğinde bu garip bir ihtimaldir. Kısa bir süre önce, şu anda Bitcoin’e tam olarak ulaşmak için herhangi bir fotoğraf çekmenin önemli olduğu kabul ediliyor. Kendini beğenmiş olanlar, bitcoin ile ilgili bir iş için ödeme alabilirler. Bunu başarmanın bir çok yolu vardır, herhangi bir internet hizmetini oluşturmak ve bitcoin cüzdanınızı her şeye eklemek gibi. Ayrıca dijital para birimlerine ayrılmış birkaç web sitesi ve iş panosu vardır [75].

Cryptogrind, iş arayanlar ve potansiyel iş arayanlar için özel web siteleri aracılığıyla (serbest, tam zamanlı ve tam zamanlı) kripto para birimlerinde diğer kripto para birimlerinde kripto para birimleri için bir araya getiriyor. Jobs4Bitcoins, reddit.com’un bir parçasıdır. Bitwage, iş

maaşınızın bir bölümünü seçmenin bir yolunu sunar; bu, yalnızca en iyi ve en önemli şey için dönüştürülür [75].

Geleceğin gerçek olduğuna inanan pek çok şey var. Bunun dünya çapında çok daha hızlı, düşük maliyetli çözüm sağladığına inanan birçok kişi. Herhangi bir hükümet veya merkez bankası tarafından desteklenmese de, bunlar geleneksel para birimleri için değiştirilebilir; Aslında, dolar karşısındaki döviz kuru, potansiyel yatırımcıları ve sürekli oyunlarla ilgilenen tüccarları cezbetmektedir. Gerçekten de, benzersiz bir büyüme için en önemli nedenlerden biri, her şey için tek başına bir şey yapabilmeleridir [76].

Mart 2014'te, IRS, her şey dahil olmak üzere tüm sanal para birimlerinin, sürekli olarak değil, mülk olarak vergilendirileceğini açıkladı. Temel olarak tutulanlardan elde edilen kazançlar veya kayıplar, temel kazançlar veya kaybolmalar kadar gerçek olacaktır, oysa bitcoin'ler olağan bir şey değildir. Çıkardığınız veya başka bir parçadan satın aldığınız bitcoinlerin satışı veya mallar veya ürünler için kullanılmasıdır [76].

Diğer herhangi bir şey gibi, düşük fiyattan satın almanın ve bitcoin'e yüksek satış yapmanın ana nedeni. Sürekliliği sağlamanın en iyi yolu, borsada satın almaktır, ancak bunları satın almanın ve satın almanın başka yolları da vardır.

5.6.9.Yatırımlarla Artan Riskler

Bitcoin olmamasına rağmen düşük tasarlanmış normal sermaye yatırımı (hisse senedi ihraç edilmedi). Bununla birlikte, garantili değer ve dijital doğasının olmaması, satın alma ve kullanmanın bazı önemli riskleri olmadığı anlamına gelir. Sanal bir para biriminin seçeneği henüz yenidir ve geleneksel yatırımlara bağlı olarak, bitcoin uzun vadeli bir geçmişe veya güvenilirlik geçmişine sahip değildir. Artan popularity ile, neredeyse her gün daha az deneysel; yine de, yalnızca bir on yıl sonra, tüm dijital para birimleri hala geliştirme aşamasında kalır. Digital Para Birimi Grubunun CEO'su, "Bitcoin'de iyi durumda olan şirketlerin CEO'su Barry Silbert, "Bu, en yüksek riskli, en yüksek geri dönüşlü, satın alma şansınızdır" diyor [76].

5.6.10.Düzenleyici Risk

Pek çok farklı şekilde para yatırımı yapmak, riskten kaçınma amaçlı değildir. Bitcoins hükümete sürekli rakiptir ve kara market işlemleri, para aklama, yasadışı faaliyetler veya vergi kaçakçılığı için kullanılabilir. Sonuç olarak, hükümet bitcoin kullanımını ve bazılarını (ve bazılarında zaten var) düzenlemeye, kısıtlamaya veya yasaklamaya çalışabilir. Diğerleri farklı kurallarla ortaya çıkıyor.

Örneğin, 2015 yılında, nihai düzenlemeler, New York Dışişleri Bakanlığı finansal hizmetlerine ait olan bitcoinlerin satın alınması, satılması, aktarılması veya depolanması ile, kimlikle uğraşan şirketlerin müşterilerine ait kayıtları bir uyum görevlisi ile kaydetmek ve sermaye rezervlerini korumak. 10.000 ABD Doları veya daha fazla değerindeki işlemlerin yeniden değerlendirilmesi ve raporlanması gerekir. Bitcoin (ve diğer sanal) hakkında tek tip düzenlemelerin olmaması, bunların uzun ömürlülüğü, basitliği ve benzersizliği hakkında soruları artırmaktadır [77].

5.6.10.1.Güvenlik riski

Bitcoin'e sahip olan ve onu kullanan çoğu kişi, bunu bir kez daha gözden geçirerek çözemedi. Bunun yerine, bitcoin olarak bilinen bir dizi popüler çevrimiçi pazarın herhangi birinde, her yerde ve diğer dijital pazarlarda satın alır ve satarlar.

Bitcoin değişimi tamamen dijitaldir ve tüm sanal sistemlerde olduğu gibi, bilgisayar korsanları, kötü amaçlı yazılımlar ve operasyonel hatalara karşı risk altındadır. Eğer bir hırsız, sahibinin sabit diskindeki bir sürücüye ulaşmayı başarsa ve bunu en iyi şekilde seçerse, başka bir hesaptan başka bir şey yapamazlar. Bilgisayar korsanları, aynı zamanda, bitcoinlerin en çok kullanıldığı binlerce cüzdana ve dijital cüzdanlara erişim sağlayarak, iki borsayı da hedefleyebilir. Japonya'da büyük bir borsa olan Gox Dağı'nın, milyonlarca değer birden fazla değer kaybettiği 2014'te beklenmedik bir şey değil [77].

Tüm Bitcoin işlemlerinin kalıcı ve kalıcı olduğu göz önüne alındığında, bu özellikle önemlidir. Bu, nakitle işlem yapmak gibidir: Yalnızca, geri alan kişi iade ederse geri alınabilir. Bir borç veya kredi kartı durumunda olduğu gibi, üçüncü bir parça veya büyük bir işlemci yoktur; bu nedenle, herhangi bir soruna itiraz edilmez.

5.6.10.2. Sigorta riski

Bazı yatırımlar, Securities Investor Protection Corporation aracılığıyla sigortalanır. Normal banka hesapları, yargı yetkisine bağlı olarak belirli bir miktara kadar Federal Deposit Insurance Corporation (FDIC) aracılığıyla sigortalanır.

Genel olarak, bu tür federal veya hükümet programları yoktur, bitcoin borsaları ve bitcoin hesapları vardır. 2019 yılında ana satıcı ve ticaret platformu SFOX, FDIC sigortası ile bitcoin yatırımı yapabileceklerini ancak sadece olaylarla ilgili işlemler için yapabileceklerini açıkladı.

5.6.10.3. Dolandırıcılık riski

Sahipleri doğrulamak ve işlemleri kaydetmek için özel anahtar kullanırken, sahtekarlık ve yanlışlık Kısa süre önce, Temmuz 2013'te SEC, konuyla ilgili bir Ponzi oyununun operatörüne karşı yasal işlem başlattı. Ayrıca, sahtekarlığın başka bir yaygın biçimiyle ilgili bazı kanıtlar da vardır.

5.6.10.4. Pazarlama riski

Herhangi bir yatırımda olduğu gibi, değer dalgalanma gösterebilir. Gerçekten de, mevcut zamanın değeri, kısa süre içinde her zamankinden daha fazla artacağını gördü. Yüksek hacimli satın alma ve değiş-tokuş etme konusuna bağlı olarak, haber değeri taşıyan herhangi bir olaya yüksek derecede düşük bir değere sahiptir. CFPB'ye göre, 2013'te tek günlük fiyat %61 düşerken, 2014'teki bir günlük fiyat %80 kadar büyüktü.

Eğer bir süre önce bunu kabul etmeye daha az tercih edilirse, bunlar tek başına değer kaybedebilir ve daha kötü hale gelebilir. Aslında, 2017'de tüm zamanların en yüksek fiyatı düştüğünde "bitcoin balonu"nun patlamış olması muhtemeldi. Halihazırda çok sayıda seçenek var ve bitcoin yüzlerce diğer özel para biriminde büyük bir yol katetmesine rağmen, marka tanınırlığının önemli ölçüde artması ve daha iyi bir teknolojik atılıma sahip olması bir tehdit unsurudur [78]. Bu süreç "çatlama" olarak bilinir ve genellikle yeni bir isimle yeni bir bitcoin türünün yaratılmasıyla sonuçlanır. Bu bölünme, en başından beri, en başından beri yeni bir "sert çatal" olabilir. (Ağustos 2017'de yaratılmıştır), dünyanın her yerinde (2017'de yaratılmıştır) zor

bir çalışmanın bir sonucu olarak yaratılmış olduğuna dair bir örnek. Bir “yumuşak çatal”, eski sistem kuralıyla hala uyumlu olmayan bir değişikliktir. Örneğin, yumuşak çatallar bloğun toplam boyutunu artırdı.

5.7. KRIPTO PARA MADENCİLİĞİNDE TERMODİNAMİK SÜREÇ

Geçtiğimiz on yıllar boyunca, küresel hesaplama ortamı, yoğun işlem gücünde anıtsal artışlarla sonuçlanan devrim niteliğinde bir değişime uğramıştır. Verilerin depolanması, işlenmesi ve yönetilmesinin ağır kaldırılması, kuruluşların kritik teknolojik uygulamalarını ve verilerini barındıran veri merkezleri olarak bilinen yüksek yoğunluklu bilgi işlem tesislerine kaymıştır. Teknoloji altyapısı ve donanımıyla donatılmış merkezi veri tesisleri, tüm önemli iş süreçlerinin, finansal işlemlerin, iletişimin, üniversite, belediye ve hükümet sistemlerinin temel işlevlerini desteklemektedir [78].

Neredeyse tüm kurumlar elektronik veri alışverişine bağımlıdır ve veri merkezi gereksinimleri dereceye göre değişir. Büyük kuruluşlar operasyonlarını desteklemek için onlarca veya yüzlerce veri merkezine ihtiyaç duyarlar [78]. Veri merkezi etkinliği bu tür e-posta, dosya paylaşımı, haberleşme, streaming, internet ve barındırma olanaklarının yanı sıra veri konsolidasyonu ve analizi, depolama, kripto para işlem ve yüksek performanslı işlem gibi geleneksel kurumsal hizmetleri kapsar. Yapay zeka, makine öğrenimi ve derin öğrenmenin dönüştürücü disiplinleri veri merkezlerine bağlıdır. Küresel toplam veri merkezi sayısı son yıllarda azalırken, kritik hesaplama uygulamalarının bulut servis sağlayıcıları tarafından geliştirilen hiper ölçekli tesislere dış kaynak kullanımı, öngörülebilir gelecekte toplam veri merkezi alanında genel bir artışa katkıda bulunacaktır [78].

Tipik veri merkezi tasarımı, yönlendiriciler, anahtarlar, güvenlik duvarları, depolama sistemleri, sunucular ve uygulama dağıtım denetleyicileri gibi standart fiziksel bilgi teknolojisi (BT) bileşenlerini içerir. Veri merkezi boyutu amaçlanan amaca bağlıdır, bu nedenle veri merkezleri farklı konfigürasyonlara sahiptir. Ağ topolojisi ve destekleyici ekipman sağlanan hizmete göre özelleştirildiğinden düzen işleve göre değişebilir [79]. Gerekli hesaplama destek düzeyine bağlı olarak, veri merkezleri depo sunucuların az sayıda sunucuları onbinlerce tarzı tesislerinden menzilli ve bazı yapı standartları var ise, tüm veri merkezleri önerilen bina kodları izleyin. Veri

merkezi altyapısının fiziksel tasarımı ve lojistik düzeni kapasite, güç ve sıcaklık kontrol gereksinimleri için optimize edilmiştir, ancak talep dalgalanmalarına uyum sağlamak için genellikle esnek olmalıdır. Özel hizmet sağlayıcılar, hizmet kesintilerinin kuruluşta veya işletmede felaketle sonuçlanabilecek aksaklıklara neden olabileceği ‘görev açısından kritik’ tesisler olarak sınıflandırılabilir. Sonuç olarak, kapsamlı dc’lerdeki kritik bina sistemleri arasında güç kaynağı yedekliliği, yedek güç üretim ekipmanı, ısıtma, havalandırma ve iklimlendirme (HVAC) sistemlerinin yanı sıra kapsamlı yangından korunma ve güvenlik sistemleri bulunmaktadır. BT ekipmanlarını korumak için nem ve sıcaklık gibi çevresel faktörler dikkatle kontrol edilir [80].

5.7.1. İşlemciler

Bilgi işlem endüstrisinin ilk günlerinden itibaren, Moore yasası, mikroçip üzerindeki transistörlerin iki yılda bir ikiye katlanmasıyla ilişkili olarak bilgi işlem gücündeki artışı öngördü. Moore’un öngörülerine uygun olarak, hesaplama gücü zaman içinde istikrarlı ve hızlı bir şekilde büyüdü ve BT devriminin başarısını artırdı. Yakın zamana kadar, bilgi işlem çip cihazlarının işlem verimliliği ve kapasitesi arttıkça, ilgili maliyet, boyut ve güç tüketimi azaldı [80].

Bir bilgi işlem cihazının ‘beyni’ olarak, genel program işlevlerini yerine getirmek için hesaplamalı işlem birimleri (CPU’lar) geliştirilmiştir. Esnek ve çok işlevli CPU işlemcileri çok çeşitli karmaşık hesaplama görevleri yapabilir. Dual ve multi-core İşlemciler tandem çalıştırmak olabilir işlem sayısı arttı. Modern çok çekirdekli CPU’lar 1-12 çekirdeğe sahiptir, ancak temel tasarım büyük ölçüde erken Cpu’lara benzemektedir (Baltazar, 2018). Grafik işlem biriminin (GPU) yükselişi, paralel olarak basit görevleri yerine getirebilecek işlem birimlerine duyulan ihtiyaçla çakıştı. Günümüzde GPU’lar binlerce işleme çekirdeğine sahiptir ve daha düşük genel işleme kapasitesine rağmen GPU verimliliği, göreve özgü işlevsellikte CPU’ları hızla geride bırakmıştır. Büyük veri süreçlerinde her saniye binlerce gigabayt veri üretilir, bu nedenle anlık ve verimli işleme kritik öneme sahiptir [81]. Mikroçip geliştirmedeki daha ileri gelişmeler, Alan Programlanabilir Kapı Dizilerinin (Fpga’lar) ve Uygulamaya Özel Entegre Devrelerin (ASIC’LER) özel tek amaçlı çip tasarımına yol açtı. Asic’ler belirli işlevleri yerine getirmek

üzere geliştirilmiş ve üretilmiştir; Bitcoin madenciliğinde kullanılan asic'ler, göreve özgü yoğun blockchain karma hesaplamalarını gerçekleştirir ve başka bir amaç için kullanılamaz. ASIC yongalarının verimliliği, çipin tekil işleyişinden kaynaklanmaktadır, sonuç olarak ASIC'LER, karmaları Cpu'lardan 100.000 kat daha hızlı hesaplayabilir [81].

İleri teknoloji mikroişlemcilerle olan talep, yoğun karma işlemlerinin üst düzey Gpu'lardan ve ASIC'lerden sağlanan işlem gücünü gerektirdiği veri madenciliği, makine öğrenimi ve derin öğrenmenin ortaya çıkmasıyla önemli ölçüde artmıştır. 2018 yılı sonuna kadar makine öğrenimi veri merkezlerinde kullanılan yongaların %25'inin FPGA ve ASIC olacağı ve işlemlerin mikroçip ısı çıkışı dikkate alınarak watt başına performans metriği ile ölçüleceği tahmin edilmektedir [82].

Artık Moore yasasının sınırlarına ulaşıldığı iyi anlaşılmıştır. Mikroskobik transistör boyutlarında, giderek daha küçük altyapı yoluyla elektron transfer hızının neden olduğu ısı üretimi, transistörlerde aşınmaya neden olur ve ısı dağılımı zorlukları yaratan sıcaklık eşiklerini aşar [76]. Bilgi işlem performansındaki artan talebe uyum sağlamak için, kurumsal uygulamalardaki sunucu yoğunluğu da son on yılda önemli ölçüde artmış ve ısı ve güç sorunlarını hızlandırmıştır [83]. Gelişmiş işleme yongaları için en büyük tek istemci olan sunucu işletmeleri, daha sonra birçok BT kuruluşu için güç ve soğutma zorlukları yaratan büyük miktarda ısı döktü. Sonuç olarak, veri merkezi yöneticileri sistemlere nasıl büyük miktarda güç sağlanacağını ve üretilen aşırı ısı miktarlarıyla nasıl mücadele edileceğini belirlemelidir.

5.7.2. Veri Merkezi Boyutu

Veri merkezleri hem boyut hem de performansa göre sınıflandırılır. International Data Corporation (IDC), veri merkezlerini büyüklüklerine göre beş türe ayırır, ancak [81] en gelişmiş veri merkezi türlerini hesaba katmak için altıncı bir türü benimser.

En küçük sınıflandırma türü olan sunucu dolapları, küçük işletmeleri veya bireysel projeleri destekler ve genellikle uzman olmayanlar tarafından yönetilir. Biraz daha büyük sunucu odaları (5-25 sunucu) daha büyük şirketlerde benzer süreçleri destekler ve genellikle özel BT personeli tarafından yönetilir. Yerelleştirilmiş veri merkezleri (26-100 sunucu), güç ve soğutma

sistemlerinde bir dereceye kadar fazlalık gerektiren iş açısından kritik uygulamalarda kullanılır, ancak bu boyut sınıflandırmasında kesinti süresi felaket değildir. Orta seviye veri merkezleri (101-499 sunucu), İK, e-posta, dahili veri depolama gibi işletim sistemlerini barındıran büyük ve orta ölçekli kuruluşlar tarafından kullanılmaktadır. Bu büyüklükteki tesislerde, kesinti süreleri işletmenin işleyişini etkileyebilir. bu nedenle, orta seviye veri merkezleri bir dereceye kadar güç kaynağı yedekliliği gerektirir. Kurumsal veri merkezleri (500'den fazla sunucu), bankalar, finans ve sağlık şirketleri gibi kuruluşlar için temel iş operasyonlarını desteklemek için kullanılan bağımsız saha dışı tesislerdir. Hizmet kesintilerine neden olan hizmet kesintileri felaket olabilir ve kurumsal veri merkezlerinin tasarımlarında yüksek derecede fazlalık vardır. Son olarak, sunucu çiftlikleri veya depo ölçekli bilgisayarlar (WSCS) olarak da adlandırılan hiper ölçekli veri merkezleri 5000 veya daha fazla sunucuya sahip olarak sınıflandırılır. Hiperscale veri merkezleri genellikle bilgi ve iletişim teknolojisi şirketleri (BT'LER) ve ana bilgisayar veri ve bulut hizmetleri tarafından oluşturulur. Hiper ölçekli tesislerin mimarisi, verimliliği vurgulayan yüksek derecede homojenlik sağlar [82].

Tablo 5.1: Veri Merkezi Taksonomisi [82].

<i>Classification</i>	<i>Taxonomy</i>	<i>Servers</i>	<i>Dimensions (ft²)</i>
<i>Small Data Centers</i>	Server Closet	1-4	≥100
	Server Rooms	5-25	101-1000
<i>Mid-size Data Centers</i>	Localized Data Center	26-100	1001-2000
	Mid-tier Data Center	101-499	2001-20000
<i>Large Data Centers</i>	Enterprise Data Center	500+	20000+
	Hyperscale Data center	5000+	20000+

Uptime Institute'un Katman Sınıflandırma Sistemi, veri merkezi performansını ve yedekliliğini sınıflandırır. Kritik öneme sahip tesisler için hizmet kesintisi, gelir kaybından can kaybına kadar ciddi iş sonuçları doğurabilir, bu nedenle tesis performansını iş talebine göre sağlamak için bir sertifikasyon süreci ile kademe sınıflandırması geliştirilir [83]. Katman 4 sınıflandırması, veri merkezleri için en yüksek yedeklilik düzeyini ve en düşük kesinti derecesini temsil eder ve tamamen yedek olarak belirlenir.

Tablo 5.2: Veri Katmanı Sınıflandırılması [83].

<i>Tier</i>	<i>Uptime</i>	<i>Redundancy</i>	<i>Downtime (h/y)</i>
1	99.671%	No redundancy	28.8
2	99.741%	Partial redundancy	22
3	99.982%	Fault tolerant	1.6
4	99.99%	Fully redundant	0.43

5.7.3. Veri Merkezi Yerleştirme Konuları

Veri merkezi saha seçimi, sıkı güvenilirlik gereklilikleriyle sınırlandırılmıştır [83]. Yer seçimi için sanayi kriter iş yapıyor, vergilendirme, siyasi istikrar, sürdürülebilirlik, doğal afetler, enerji güvenliği, temel konularla ilgili bir dizi; enerji, bant genişliği, kullanım kolaylığı, kişi ve tehlikeler [84], [85] yanı sıra iklim ve insan-kişi başına düşen su miktarı başına GSYİH vardır. Veri merkezleri nihai kullanıcılardan daha uzak mesafelere yerleştirilebildiğinden, istemci mesafesi faktörleri daha az önemlidir.

Kritik güç altyapısının güvenilirliği, veri merkezi saha seçiminde operatörler için en önemli husustur. Kritik bir enerji tüketicisi olarak, güç kullanılabilirliği ve maliyet, veri merkezi operatörlerinin temel itici güçleridir. Veri merkezi operasyonları için temel yük üretiminin karakteristiği olan istikrarlı oranlarla ekonomik, güvenilir enerjiye erişim esastır. Veri merkezlerini yerleştirirken, operatörler tedarikte fazlalığı korumaya çalışırlar. Elektrğin türü veya kaynağı, yenilenebilir kaynaklardan gelen ‘yeşil’ güç kaynağına doğru giderek artan sayıda DC ile saha seçimini etkileyebilir. Üretim kaynağına yakınlık, dağıtım kayıplarının azalmasına ve daha az gerekli altyapıya yol açarak tesis maliyetini / MW’I düşürür [85].

Fiberoptik ve iletişim altyapısının kullanılabilirliği ve güvenilirliği, veri merkezi saha seçimi için bir başka üst düzey husustur. Pazar bağlantısı, yüksek hızlı ve yüksek hacimli veri iletimi gereksinimi göz önüne alındığında tesis konumunun önemli bir sürücüsüdür. Güç kaynağı gibi, altyapı güvenilirliği de sürekli operasyonlar için kritik öneme sahiptir ve ağ trafiği altyapı kalitesiyle sınırlıdır. Yeterli kapasiteye ek olarak, veri merkezi talebi zaman içinde büyüdükçe altyapının genişlemesine izin verecek şekilde esnek olması gerekir.

Hem iklim hem de doğal tehlikeler dahil olmak üzere çevresel koşullar veri merkezi güvenilirliğini ve maliyetini etkileyebilir. Yüksek sunucu ısı çıkışı nedeniyle, serin iklimler sıcaklık kontrol taleplerini azaltmak için kullanılabilecek bir varlıktır. İklim, veri merkezi verimliliğini etkiler ve tesis tasarımını ve yapımını da etkileyebilir. Yoğun soğutma, hem başlangıç sermayesi harcamalarını hem de ömür boyu işletme harcamalarını artırarak daha fazla altyapı gerektirir [86]. Uygun iklimlerde, dış ortam havasının yeterince düşük sıcaklıkta kullanılması olan ‘serbest soğutma’, enerji maliyetlerini önemli ölçüde azaltmak için bir yöntem olarak kullanılabilir. Soğuk ve kuru iklimler, veri merkezi verimliliği için en uygun koşulları sağlar. Veri merkezleri için uygun konumlar sismik olarak kararludur ve seller, kasırgalar, kasırgalar ve volkanlar gibi doğal tehlikelere karşı düşük bir eğilime sahiptir. Yüksek rüzgarlar, soğutma için harici hava kullanan dc’ler ve toz fırtınalarından, ağır polenlerden, aşındırıcılardan kaynaklanan düşük hava kalitesi için sorunlu olabilir (örn. okyanus havasından gelen tuz), dumanlar, kimyasal kirleticiler ve diğer ince partikül maddeler maliyetli filtreleme ekipmanı ve filtre bakımı gerektirebilir [87].

Yer seçimi sırasında dikkate alınan ek faktörler arasında siyasi istikrar ve ekonomik teşvikler yer almaktadır. Bir veri merkezi sitesi seçiminde siyasi istikrarın ikinci en önemli risk faktörü olduğunu tespit etmiştir. Siyasi huzursuzluk, çatışma birincil enerji kaynaklarının arzını bozabileceğinden veri merkezi güvenilirliğini engelleyebilir. Vergilendirme ve düzenleme yer seçimini teşvik edebilir ve sosyoekonomik faktörler sürdürülebilir bir işgücünün kullanılabilirliğini belirler. Esnek bir risk değerlendirme metodolojisi kullanan [88] bir Veri Merkezi Risk Endeksi geliştirdi. Otuz yedi ülke, başarılı veri merkezi operasyonunu etkileyen en önemli on risk faktörüne göre sıralandı. En yüksek beş ülke; İzlanda, Norveç, İsviçre, Finlandiya ve İsveç Kuzey Avrupa’da yer almaktadır. Bu ülkeler, güçlü enerji güvenliği ve önemli oranda yenilenebilir enerji üretimi olan işletmeler için hem politik hem de jeolojik açıdan istikrarlı ortamlar sunmaktadır [89] Endeks sıralaması, veri merkezi ayak izini düşürmek için sürdürülebilir düşük maliyetli enerji kaynakları arama eğiliminin temsilcisidir. İsveç, Norveç ve Finlandiya gibi veri merkezi merkezleri güvenilir, düşük maliyetli enerji, vergilendirme avantajları, güçlü bağlantı, düşük doğal tehlike riski ve siyasi istikrardan yararlanmaktadır.

Yakından takip eden Kanada, endekste altıncı sırada yer alıyor ve Kuzey Avrupa ülkelerini veri merkezi genişlemesi için çok değerli hedefler haline getiren özelliklerin çoğuna sahip. Kanada, hidroelektrik ve doğal gazdan üretilen elektrik için rekabetçi düşük enerji fiyatları ile enerji güvenlidir. Kanada, serbest soğutma için gerekli serin iklime sahiptir ve düşük doğal tehlike riski ile jeolojik olarak kararlıdır. Politik ve ekonomik istikrarda üst sıralarda yer alır ve Kanada veri merkezlerindeki sunucularda depolanan verilerin gizliliğini sağlayarak güçlü yasal gizlilik korumasına sahiptir. Kanada'nın çalışma izni ve göçmenlik süreçleri, işgücünün % 37,6'sının göçmen statüsüne sahip olduğu Kanada teknoloji sektörüne fayda sağlayan yabancı teknoloji çalışanlarına dosttur [89].

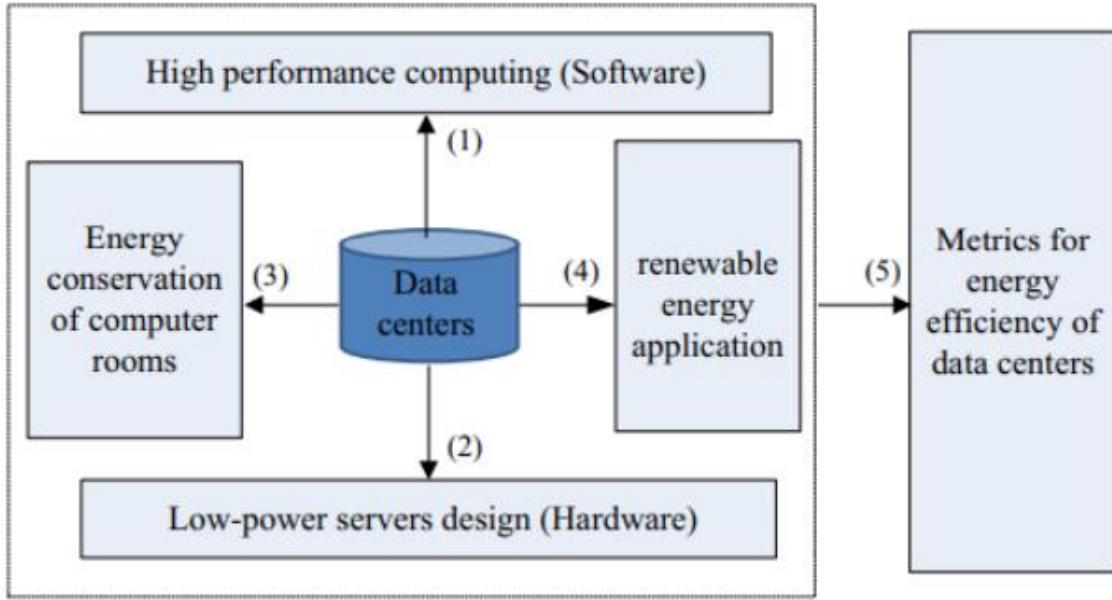
Alberta eyaleti, Kuzey Amerika'daki veri merkezi yatırımları için en uygun maliyetli yerlerden biridir. Alberta Enerji Piyasası Kanada'da sadece serbest pazar, bölgenin en düşük elektrik fiyatları bazı sonuçlanan. Bol miktarda doğal gaz kaynağı, temel yük gücünün önemli bir bölümünü sağlar. Sınırlı ihracat talebi ve tartışmalı boru hattı kısıtlamalarından kaynaklanan son arz fazlası, rekabetçi uzun vadeli oran müzakerelerine izin veren düşük fiyatlara neden olmuştur. Uygun bir döviz kuru ve düşük nispi inşaat maliyetleri daha fazla teşvik sağlar. Ek olarak, satış, sermaye, bordro veya ekipman vergisi ve düşük ticari emlak vergisi oranı olmadan Alberta'daki işletmeler ve çalışanlar Kanada'daki en düşük genel vergilendirme oranından yararlanır [90]. Alberta ayrıca istikrarlı, yükseltilmiş bir elektrik şebekesine ve yüksek hızlı, düşük gecikmeli bir ağa sahip geniş bir telekomünikasyon ağına sahiptir (Invest Alberta, N.d.). İl ayrıca son derece yetkin bir işgücüne sahiptir; Calgary şehri, Alberta'nın kaynak sektöründe istihdam edilen teknik profesyonellerin bir yansıması olan Kanada'daki en yüksek teknoloji işçilerinin konsantrasyonunu koruyor [91]. Son olarak, Alberta'nın serin ve kuru iklimi, sıcaklık kontrol maliyetini en aza indirir ve yılın% 10'undan daha azı klima kullanımını gerektirir.

5.7.4. Veri Merkezi Enerji Verimliliği

Kesintisiz güç kaynağı gerektiren veri kullanılabilirliği, güvenlik ve bant genişliği gereksinimleri ile veri merkezleri enerji yoğun işlemlerdir. Bilgi işlem altyapısı ve donanımının ürettiği konsantre ısının kullanılması ciddi güç ihtiyacına katkıda bulunur [87]. Tipik veri merkezi güç yoğunlukları 538-2153 W / m² arasında değişir ve 10.000 W / m²'ye ulaşır. Buna

karşılık, modern yüksek teknolojili ofis güç yoğunlukları 108-161 W / m² arasında oldukça düşüktür [90]. Veri merkezi sıcaklık kontrol sistemleri, tesise verilen enerjinin ortalama% 40'ını tüketirken; en verimli soğutma sistemleri toplam tesis enerjisinin% 24'ünü ve en az %61'ini verimli tüketmektedir. Smart 2020 Raporunda, BİT sektörüne yönelik emisyonların 2000-2020 yılları arasındaki 20 yıllık dönemde%180 artacağı, veri merkezi emisyonlarının ise aynı dönemde%240 artacağı tahmin edilmektedir. Veri merkezlerinin hızla genişlemesi, hiper ölçekli tesislerin geliştirilmesi ve bileşen ve tesis tasarımının evrimi, veri merkezleri için önemli sermaye ve işletme maliyeti artışına neden olmuştur [91]. Birincil enerji üretimi kaynağı olan fosil yakıtlar, küresel olarak üretilen elektriğin çoğunluğunu oluşturur, bu nedenle veri merkezleri için verimlilik optimizasyonu, hem ekonomik hem de çevresel ayak izlerini azaltmada hayati öneme sahiptir.

İşlenen yüksek hacimli hassas veriler göz önüne alındığında, veri merkezi operasyonunda güvenlik her şeyden önemlidir. Yöneticiler, veri güvenliği ve rekabet amacıyla veri merkezi konumlarının anonimliğini koruma konusunda ihtiyatlıdır. Veri merkezi gizliliği genellikle enerji kullanımına kadar uzanır, bu da gözetimin yetersiz olduğu ve enerji kullanımının izlenmesinin zor olduğu anlamına gelir. Bölgeye özgü bazı mevzuat göz önünde bulundurulmasına rağmen, veri merkezi enerji tüketimini ve emisyonlarını izleyen veya sınırlayan uygun bir yasal çerçeve veya politika bulunmamaktadır [92].



Şekil 5.1: Enerji Tasarrufu Çerçevesi [92].

Ekonomik ve çevresel yükleri iyileştirmek için veri merkezi platformları verimlilik optimizasyonuna odaklanır. Şekil 2’de gösterildiği gibi, veri merkezleri dört ana yöntemle ‘yeşillendirilebilir’; yüksek performanslı bilgi işlem, düşük güçlü sunucu tasarımı, enerji tasarrufu ve yenilenebilir enerji uygulamasının dahil edilmesi. Yüksek performanslı bilgi işlem, süper bilgisayar mimarisi ve yapay zeka yazılımının benimsenmesiyle tesis verimliliğini optimize eder. Düşük güçlü sunucu tasarımı, enerji tüketimini azaltmak için donanım iyileştirmelerini kolaylaştırır. Bilgisayar odalarının enerji tasarrufu, serbest soğutma ve sıvı soğutma gibi yenilikçi ve verimli soğutma yöntemlerinin dahil edilmesini içerir. Ve son olarak, yenilenebilir enerji uygulaması hem yenilenebilir enerji kaynağının dahil edilmesini hem de tesis tarafından üretilen termal enerjinin doğrudan uygulanmasını ifade eder. Bu proje, son iki verimlilik iyileştirme biçimine, enerji tasarrufu ve yenilenebilir enerji uygulamasına odaklanmaktadır.

5.7.5. Verimlilik Ölçümleri

5.7.5.1. PUE

Güç kullanım etkinliği (PUE), bir veri merkezinin enerji performansını ölçmek için kullanılan endüstri standardı bir metriktir. PUE, bir veri merkezinin toplam güç tüketiminin ve BT ekipmanı tarafından tüketilen gücün verimlilik oranıdır [92].

PUE, güç ve soğutmanın BT ekipmanına ne kadar etkili bir şekilde gönderildiğini karakterize eder. BT ekipmanı enerjisi, bilgi işlem, depolama ve ağ ekipmanlarının yanı sıra veri merkezi gözetimi ve kontrolünde kullanılan monitörler, iş istasyonları ve anahtarlar tarafından da karşılanır. Tesis enerjisi, tarif edilen BT ekipmanını ve güç dağıtım bileşenleri, soğutma sistemi bileşenleri ve aydınlatma gibi çeşitli bileşen yükleri dahil ancak bunlarla sınırlı olmamak üzere diğer bileşen yüklerini içerir. PUE ölçümünün kapsadığı üç ana süreç, BT ekipmanına verilen enerji, bu güç dağıtımı sırasında kaybedilen enerji ve soğutma ve altyapının gerektirdiği enerjidir [93].

PUE bir verimlilik metriği değildir ve kapsamlı bir verimlilik metriği değildir ve PUE tesisin veya BT ekipmanının tüm çevresel yükünü ifade etmemektedir. PUE değerleri, operasyonel verimlilik iyileştirme fırsatlarını belirlemek ve operasyonel tasarım ve süreçlerin zaman içinde gelişip gelişmediğini göstermek için kullanılabilir. Ayrıca, PUE ölçümleri benzer veri merkezlerini karşılaştırmak için kullanılabilir ve yeni veri merkezleri için bir tasarım hedefi görevi görebilir. Sürekli PUE izleme, işletme verimliliğini izlemek için genellikle bina yönetim sistemlerine entegre edilir [93].

Hesaplanan PUE değerleri 1.0 ile sonsuzluk arasında değişebilir. PUE, veri merkezine verilen gücün% 100'ünün yalnızca bilgi işlem ekipmanı tarafından kullanıldığı ideal 1.0 değerine sahiptir. Tüm tesisler aydınlatma ve güç dağıtımı nedeniyle bazı verimlilik kayıpları yaşadığından 1.0 değeri teorik bir minimumdur. Şu anda, küresel veri merkezi PUE değerleri için kapsamlı bir veri kümesi eksiktir ve veri merkezleri arasında pue'deki gerçek varyans bilinmemektedir. Endüstri çapında PUE ölçümleri değişmekle birlikte, 61 Dcs'den oluşan bir EPA araştırması, PUE'LERİN ortalama 1.92 ile 1.25 ila 3.75 arasında değiştiğini göstermiştir

[86]. 2013 Kendi kendini raporlayan Çalışma Süresi Enstitüsü anketi ortalama 1.65 PUE gösterdi. 1.92’de veri merkezi altyapı değeri (DCiE), tesise ulaşan enerjinin yarısından biraz daha azının (% 48) BT ekipmanı tarafından hesaplama işlemlerinde kullanıldığını, 1.65’te bu değerin% 40 olduğunu göstermektedir. Ultra düşük PUE ölçütlerine, optimize edilmiş tesisler tasarlamak için gereken kaynak ve uzmanlığa sahip Google, Facebook ve Amazon gibi büyük teknoloji kuruluşları tarafından ulaşılır.

2015 yılında Google, 12 aylık filo ortalaması PUE’NİN 1.12 (Google, N.D.) olduğunu ve Facebook’un en büyük iki veri merkezinin TTM değerlerinin 1.08 ve 1.09 olduğunu bildirdi. Verimlilik düzeyleri Tablo 3’te gösterilmiştir. Eğilimler, tüm veri merkezi boyutlarında pue’de genel bir düşüş öngörmektedir (Shehabi vd., 2016), ancak gözetim eksikliği, PUE değerlerinin büyük ölçüde kendi kendine bildirildiği için güvenilir enerji verilerinin tespit edilmesinin zor olduğu anlamına gelir [93].

Tablo 5.3: PUE Verimliliği

<i>PUE</i>	<i>Infrastructure Efficiency (DCiE)</i>	<i>Level of Efficiency</i>
3.0	33%	Very inefficient
2.5	40%	Inefficient
2	50%	Average
1.5	67%	Efficient
1.2	83%	Very Efficient

Tablo 5.4: Verimlilik Senaryoları için PUE ve Artıklık Değerleri [77].

2020 PUE					
DC Type	2014 PUE	Current Trends	Improved Management	Best Practices	Redundancy
Room	2.5	2.35	2.00	2.00	N+0.5N
Closet	2.0	2.00	1.70	1.50	N+1
Localized	2.0	1.88	1.70	1.50	N+1
Midtier	1.9	1.79	1.70	1.40	N+0.2N
High-end	1.7	1.60	1.51	1.30	N+0.5N
Hyperscale	1.2	1.13	1.13	1.10	N

PUE değerleri veri merkezi konumundan önemli ölçüde etkilenebilir. Mekanik ve hesaplamalı sistemlerin verimliliği iklime göre değişir ve sıcaklığın işletme sınırlarını aşmamasını sağlamak için gereken sıcaklık kontrol miktarını bildirir. Yerel iklim, yenilikçi soğutma işlemlerinde kullanılan dış sıcaklıklardan yararlanma yeteneğini belirler. Hava durumu, ortam sıcaklığı ve bağıl nem gibi iklim parametreleri enerji tüketimini ve işlemci performansını etkileyebilir. Tablo 5.5'te gösterildiği gibi, İskandinav ve Kıta Avrupası ülkeleri ile Kanada ve kuzey Amerika Birleşik Devletleri gibi daha soğuk iklime sahip ülkeler daha düşük ortalama PUE değerleri yaşamaktadır.

Tablo 5.5: Sıcaklık ve Bağıl Nem Verileri ile Coğrafi İmar [94].

Geographical Zones	Countries	Temperature Range (°C)	RH Range (%)	Average PUE	Number of Data Centres
Nordic countries	Denmark, Finland, Norway, Sweden	18–26	20–80	1.71	13
UK and Republic of Ireland	England, Scotland, Wales, Northern Ireland, Republic of Ireland.	17–30	8–80	1.83	116
Northern/Central Europe	Austria, Belgium, France, Germany, Hungary, Luxembourg, The Netherlands, Portugal, Poland, Switzerland	14–28	16–75	1.72	122
Southern Europe/Mediterranean	Gibraltar, Greece, Italy, Malta, Spain, Turkey, Monaco, Romania, Bulgaria	16–26	20–80	2.00	30
Non EU	Republic of Mauritius, US	-	-	-	5

PUE, birkaç önemli nedenden dolayı ilgili bir metriktir. PUE, operasyonel harcamalardan etkilenir; PUE değerindeki düşüş, kamu hizmeti maliyetlerindeki düşüşe karşılık gelir. PUE, pik PUE, tesis pik yükünü karşılamak için gerekli tasarım gereksinimlerini yansıttığı için sermaye harcamalarını da etkileyebilir. PUE sürdürülebilirliği etkiler, bilgi işlem işleme için küresel enerji tüketimi arttıkça, veri merkezleri için enerji yönetimi ve verimliliği kritik öneme sahiptir. Son olarak, PUE elektrik şebekesi talebinin temsilcisidir. Kullanışlılığına rağmen, PUE çevresel performans veya 'yeşillik' için bir vekil değildir [91]. Karşılaştırılabilir iki veri merkezi için BT yükü aynı olabilir, ancak BT donanımından ve ilişkili veri merkezi altyapısından gelen enerji tüketimi değişir ve farklı PUE değerlerine çevrilir. PUE enerji tüketimini veya emisyonları ölçmez ve ısının yeniden kullanılması gibi verimlilik önlemleri pue'yi artırabilir. [94], ısı yeniden kullanımı uygulamasının, referans duruma göre (ısı yeniden kullanımı yok) enerji tüketimini artırdığını ve bazı durumlarda PUE değerlerine ulaştığını tespit etmiştir. Veri merkezi sürdürülebilirliğini ve enerji verimliliğini daha iyi tanımlamak için operatörlerin daha fazla sürdürülebilirlik ölçümüne bakmaları gerekir.

5.7.5.2 ERE

Enerji Yeniden Kullanım Etkinliği (ERE), veri merkezi mühendisliği analiz amaçları tarafından enerji geri kazanımını karakterize etmek için kullanılan bir orandır. ERE, enerji yeniden kullanımını PUE denklemine dahil eder ve veri merkezi tesisini çalıştırmak için gereken toplam enerjinin yeniden kullanım enerjisinden daha azının BT ekipmanı tarafından tüketilen enerjiye oranının ölçülmesidir. Aşağıdaki denklemler kullanılarak hesaplanır.

ERE, yalnızca kontrol hacminin (veri merkezinin etrafındaki sınır) dışında yeniden kullanılan enerjiyi dikkate alır. Kontrol hacmi içindeki enerjinin yeniden kullanımı (yani, bir soğutucuyu çalıştırmak için ısı) PUE değeri tarafından yakalanır, ancak harici bir kullanım (yani, bir bölgesel ısıtma sistemine ısı) ERE ile ölçülebilir. ERE, tesise verilen enerjinin %100'ünün harici uygulamalarda tekrar kullanıldığı 0,0'lık bir alt sınıra sahiptir [94].

Veri merkezlerini 'yeşil' hale getirme çabasında yenilenebilir kaynaklardan güç elde etme yönünde bir itici güç var, ancak güç kaynağı veri merkezi verimliliğini etkilemiyor. Verimlilik optimizasyonu ve ısının yeniden kullanımı yoluyla atıkların en aza indirilmesi, çevre koruma ve

maliyet tasarrufu alanıdır ve hem PUE hem de ERE, atık ısıнын yeniden kullanımı ve güç tüketimindeki azalmalar için bağlam sağlamaktadır.

5.7.5.3 ERF

PUE ve ERE arasındaki ilişki, Enerji Yeniden Kullanım Faktörü (ERF) ile tanımlanır. ERF, enerji yeniden kullanımının veri merkezinin toplam enerjisine oranıdır. Ere'ye benzer şekilde, ERF, kontrol hacmi dışında kullanılan enerji olarak enerjinin yeniden kullanımını ve kontrol hacmi içinde kullanılan enerji olarak toplam enerjiyi ifade eder. ERF değerleri 0.0 ile 1.0 arasında değişir; 0'lık bir ERF, enerjinin yeniden kullanılmadığını ve 1.0'ın tüm enerjinin veri merkezi dışında yeniden kullanıldığını gösterir.

Düşük PUE değerleri veri merkezi performansının göstergesidir ve genellikle daha verimli işlemleri temsil eder. Bununla birlikte, en verimli şekilde, veri merkezleri hala çoğu ısıya dönüştürülen muazzam miktarda güç tüketmektedir. Daha fazla sürdürülebilirlik kazancı elde etmek için, atık ısıнын yeniden kullanımının uygulanması için tesis içi verimliliğin ötesine bakmak gerekir.

5.7.6. Veri Merkezlerinde Verimlilik Optimizasyonu

Bu proje, enerji tasarrufu ve ısıнын yeniden kullanımı yoluyla veri merkezinin 'yeşillendirilmesini' araştırıyor. Sunucu odalarının enerji tüketiminin azaltılması doğrudan sıcaklık kontrol gereksinimi ile ilgilidir. Soğutma sistemlerinde yapılan iyileştirmeler, veri merkezi tasarımında gelişmekte olan bir odak noktası olmuştur. Geleneksel bilgisayar odası klimalarının (CRAC'LER) yerine dış ortam havasının kullanıldığı 'serbest soğutma' uygulamasının veri merkezi yerleşimi üzerinde önemli bir etkisi olmuştur.

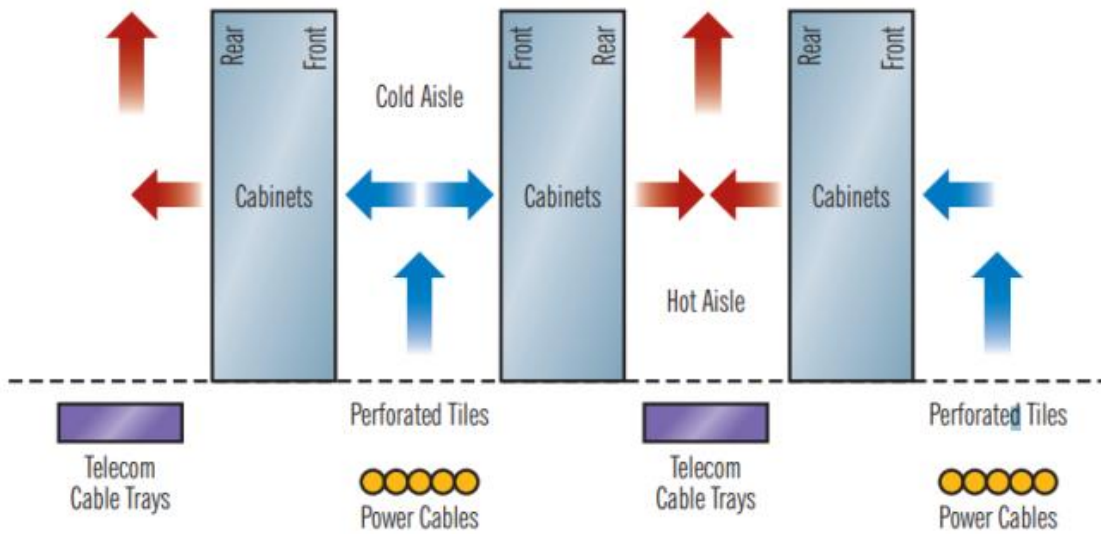
Veri merkezi düzeni, ısı dağılımını yönetmek ve veri merkezi ekipmanı için işlevsel çalışma sıcaklıklarını korumak ve ekipmanın aşırı ısınmasını önlemek için tasarlanmıştır. Veriye dayalı ısı üretimi sunucuları olumsuz etkiler, kullanım ömrünü kısaltır ve dahili sunucu soğutma fanlarını aşırı yükler. Sıcaklık, elektronik bileşenler için ana tehdittir ve DC'LERDE (% 55) bileşen arızasının başlıca nedenini titreşim (% 20), nem (% 19) ve toz (% 6) izlemektedir [94]. Geleneksel olarak, veri merkezi sıcaklığı, pompa veya fan gerektiren hava soğutma sistemleri

kullanılarak kontrol edilmiştir. Veri merkezi tasarımcıları ve mühendisleri için verimliliği gözetirken ekipman için ideal koşulları sağlamak zor bir iştir.

5.7.7. Veri Merkezi Enerji Tasarrufu

5.7.7.1. Çalışma sıcaklıkları

Tipik veri merkezlerindeki hava soğutma sistemleri, en çok ‘sıcak’ ve ‘soğuk koridorlar’ olarak düzenlenmiş sunucu rafı düzenine bağlıdır [95]. Soğuk koridorlarda, sunucu raflarının ön tarafları öne bakar ve bilgisayar odası kliması (CRAC) ünitesi tarafından sağlanan soğutulmuş hava, zemindeki veya tavandaki delikli karolardan dağıtılır. Isıtılmış sunucu havası, havanın yakalandığı ve CRAC girişine geri döndüğü sıcak koridora boşaltılır. Sıcak ve soğuk koridor havasını izole etmek için kullanılan muhafaza stratejileri, genel sıcaklık ve soğutma talebinin artmasını önlemek için hayati öneme sahiptir. CRAC içindeki ısı, çevreye maksimum dağılım için bir soğutucu veya soğutma kulesi döngüsüne emilir.



Şekil 5.2: Sıcak Koridor/Soğuk Koridor Dolabı Konfigürasyonu [92].

Termal rehberi-Klima Mühendisleri (18-27 ° 9,9 Mühendisleri TC, 2016 Isıtma, Soğutma ve Hava %60'ı (Amerikan Toplum) bağıl nem arasında ideal besleme hava sıcaklığı ASHRAE) Isıtma ve Soğutma ve Hava American Society tarafından veri işleme ortamları için ayarlanır.

Ekipmanın çalışmasıyla ilgili önceki endişeler, operatörlerin maksimum çalışma sıcaklıklarını 22°C olarak ayarlamasına ve bazı veri merkezlerinin 13°C kadar düşük sıcaklıklarda çalışmasına neden olmuştur [75]. Yüksek güç maliyeti, operatörlerin de'leri daha yüksek sıcaklıklarda çalıştırmaya başlamasına neden oldu ve veri merkezi ekipmanının varsayıldığından daha fazla sıcaklık direncine sahip olduğu bulundu. ASHRAE yönergeleri daha geniş sıcaklık aralıklarını kapsayacak şekilde revize edildi [95]. Daha yüksek çalışma sıcaklıkları CRAC / CRAH soğutmaya olan bağımlılığı azaltır. Bugüne kadar, bazı büyük ölçekli veri merkezi operatörleri ASHRAE yönergelerinin üst ucunda, 35 ° C'de çalışan bir dizi yüksek verimli veri merkezi ile çalışmaktadır [96]. Araştırmalar, modern, iyi tasarlanmış sunucular için arıza oranlarının ASHRAE yönergelerinin üst aralığında çalıştırıldığında artmadığını, ancak eski ekipman sınıflarının değiştirilmiş sıcaklık aralığıyla uyumlu olmadığını ve bu nedenle daha yüksek sıcaklıklarda çalıştırıldığında güvenilirlikte bir düşüş yaşadığını göstermektedir. Ashrae'nin Çevresel Sınıf Tanımları veri merkezlerini operasyonel işleyişe göre sınıflandırır Tablo 5'te özetlenmiştir.

Tablo 5.6: 2011 Veri Merkezleri için ASHRAE Termal Yönergeleri [87].

Class	IT Equipment Type	Rec. operating range	Allowable operating range	Max dew point	Environmental control
A1	Enterprise servers, storage products	18-27°C	15-32°C	17°C	Tightly controlled
A2	Volume servers, storage products, personal computers, workstations	18-27°C	10-35°C	21°C	Some control
A3	Same as above	18-27°C	5-40°C	24°C	Some control
A4	Same as above	18-27°C	5-45°C	24°C	Some control

(American Society of Heating, Refrigerating and Air-Conditioning Engineers TC 9.9, 2016)

5.7.7.2. Serbest soğutma

Soğutma sistemleri, herhangi bir veri merkezi tesisi için kritik altyapıdır. Veri merkezleri için geleneksel hava soğutma yöntemleri enerji yoğunudur ve veri merkezi enerji tüketiminin% 30-50'sini gerektirir [97]. Belirlenen soğutma ekipmanı sistemleri, bilgisayar odası klimaları

(CRAC'LER) ve bilgisayar odası hava işleyicileri (CRAH'LAR) ile gerekli soğutucular, pompalar ve fanlardan oluşur. Bu sistemler, aynı havayı sunucular üzerinden soğutarak ve döngüsel hale getirerek, ısıyı hareket eden havaya ısı transferi yoluyla dağıtarak çalışır.

Sunucudan çıktıktan sonra, sistem havası tipik olarak sunucu giriş havası sıcaklıklarından 10-15 derece daha sıcaktır. Bu sıcaklık farkına hava tarafı sıcaklık farkı denir ve gereken soğutma derecesini belirler. Önerilen düşük çalışma sıcaklıkları daha önce serbest soğutma ekonomizer çevrimlerinin uygulanabilirliğini kısıtlamıştı, ancak çalışma sıcaklıkları için ASHRAE değerleri daha yüksek sunucu giriş sıcaklıklarına uyum sağlayacak şekilde ayarlandığından, serbest soğutma olanakları arttı [95].

Isıtılmış sunucu çıkış havası toplanır ve sıkıştırma soğutması yoluyla belirlenen giriş sıcaklığına soğutulduğu CRAC / CRAH değerine geri döndürülür. Hava ve sıvı bazlı soğutma sistemlerini kullanan yenilikçi pasif soğutma teknikleri, güç tüketen kompresör çevrimlerini büyük ölçüde atlayarak tesis güç tüketimini önemli ölçüde azaltır. Bu proje, enerji tüketen soğutucular ve iklimlendirme gereksinimini atlamak için doğal hava sıcaklıklarını kullanan pasif hava bazlı bir soğutma tekniği olan 'serbest soğutma' üzerine odaklanmaktadır.

'Serbest soğutma' veya 'ekonomizer döngüsü', veri merkezi içinde soğutma için ortamdaki dış havayı ve doğal hava akışlarını kullanır [96]. Serbest soğutma iklime bağlıdır ve iki ana tipe ayrılır: dış havanın doğrudan tesis içinde uygulandığı doğrudan serbest soğutma ve dış havadan soğutmanın ısı eşanjörü üzerinden aktarıldığı dolaylı serbest soğutma [97]. Bu sistem, bir CRAC soğutma sistemine olan ihtiyacı büyük ölçüde azalttığı veya ortadan kaldırdığı için doğrudan hava kenarı ekonomizasyonu uygulama yeteneği, veri merkezi geliştiricileri için bir avantajdır. Doğrudan serbest soğutma, tüm serbest soğutma sistemlerinin en yüksek teorik verimliliğine sahiptir, ancak doğrudan hava ekonomizer döngüleri hava kalitesini ve nem kontrolünü içermelidir. Hava kalitesi sorunları sunucunun çalışmasını engelleyebilir ve BT ekipmanının partikül maddeden zarar görmesini önlemek için dış hava filtrelenmelidir. Dış sıcaklıklar çok soğuksa, kabul edilebilir sunucu giriş sıcaklıklarını korumak için veri merkezinden gelen sıcak hava birleştirilir. Sunucunun çalışması aşırı kuruluk veya rutubetten olumsuz etkilendiğinden, nem serbest soğutma kullanımında ek bir husustur. Yüksek nem, elektronik ekipmanlarda ve

aşırı kuru havadaki iletken arızaların veya korozyonun elektrostatik deşarj yoluyla ekipmana zarar verme olasılığını artırabilir [98].

Serbest soğutma birçok yerde uygulanabilir, ancak daha soğuk kuzey iklimleri daha fazla sayıda serbest soğutma saatine izin verir. Daha soğuk iklimlerdeki veri merkezlerinin soğuk dış ortam sıcaklıklarından yararlanabileceği ve doğrudan hava ekonomizer modlarının pue'yi önemli ölçüde azalttığı ve %49'a varan enerji tasarrufu sağladığı gösterilmiştir [99]. Intel, ekonomizer modu kullanıldığında güç tüketiminde yıllık %91 oranında %67'lik bir düşüş tespit etti. Chicago, Atlanta ve Phoenix için çoklu modları modelleyen ekonomizer modlarının analizi, serbest soğutmanın geleneksel soğutma sistemlerine göre daha fazla tasarruf sağladığını gösterdi. Hava ekonomizörü modunda toplam soğutma enerjisi %51,7-54,7 oranında azaltılmıştır (Sujatha & Abimannan, 2011). Makul yer seçimi, toplam enerji tüketiminde %12-15'lik bir düşüşe neden olabilir ve buna bağlı finansal etkiler, yeni veri merkezlerinin yerleştirilmesinde geliştiriciler için önemli bir husustur [92].

Yahoo gibi BİT şirketleri tarafından geliştirilenler gibi Hiperscale veri merkezleri!. Facebook ve Google, 1.1 civarında ultra düşük PUE değerleriyle serbest soğutmaya büyük ölçüde güveniyor. Serbest soğutma teknolojisi hızla gelişiyor ve veri merkezi enerji verimliliğini artırmak için en uygun teknoloji olarak gösteriliyor. Soğuk ve kuru iklimler serbest soğutma için en avantajlı olanlardır, ancak çoğu veri merkezi konumu belirlenen tesis sıcaklıklarının altında günlük sıcaklıklara sahiptir ve kısmi serbest soğutmadan yararlanabilir. Gelecekteki ASHRAE standartlarında ekonomizer çevrimlerinin kullanılması önerilecek ve bazı Amerikan planlama ve geliştirme otoriteleri ekonomizer modu gerekliliklerini uygulamaya başlamıştır [100].

5.7.8. Isının Yeniden Kullanımı

Birçok endüstriyel sürecin bir yan ürünü olan atık ısı, dünyanın en büyük enerji kaynaklarından biri ve büyük ölçüde değer düşüklüğüne uğramış bir kaynak olarak tanımlanmıştır. Veri merkezlerinde, verimsiz sunucu işlemleri, çoğu atmosfere kaybedilen önemli miktarda atık ısı yayar. Atık ısının hem iç hem de dış yeniden kullanımı, ilave yakıtların (genellikle karbon bazlı) dengelenmesi yoluyla enerji gereksinimini ve karbondioksit emisyonlarını doğrudan azaltır. Bu

nedenle atık ısı'nın yeniden kullanımı yoluyla emisyonlardan kaçınılması, tüketicilere, müşterilere ve yeşil endüstriyel uygulamalara odaklanan düzenleyicilere hitap eden ekonomik, çevresel ve teknik olarak sürdürülebilir bir uygulamadır. Elektrik ve ısı'nın birlikte üretilmesi yeni bir kavram değildir ve BİT sektöründe ısı'nın yeniden kullanımı giderek yaygınlaşmıştır. Fiziksel mikroçip tabanlı iyileştirmeler için kalan fırsatlar azaldıkça ve. Tesis verimliliğindeki gelecekteki gelişmelerin, enerji yeniden kullanımı şeklinde veri merkezi sınırları dışından gelmesi muhtemeldir.

İskandinav ülkeleri, tanımlanabilir çeşitli nedenlerden dolayı atık ısı'nın yeniden kullanılmasına öncülük etmektedir. Serin ılıman iklim, serbest soğutma için idealdir ve hem konut hem de ticari sektörlerde yüksek ısı talebine neden olur. 1970'lerin petrol krizlerinden sonra, İskandinav ülkelerindeki hükümetler, daha sonra büyük miktarlarda atık ısı üreten endüstrilere ısı şebekeleri açarak, bölgesel ısıtma ağlarının geliştirilmesini zorunlu kıldı. Bölgesel ısıtmada endüstriyel atık ısı, 2018'de Finlandiya'nın şebekesinin% 10'unu ve 2017'de İsveç'in şebekesinin %8'ini oluşturuyordu. Finlandiya'daki bölgesel ısıtma tesisleri, dcs'yi ısı için en büyük ikinci potansiyel kaynak olarak tahmin etmiştir [100]. Bu nedenle, bu bölgelerdeki veri merkezleri kasıtlı olarak bölgesel ısıtma şebekelerine proksimal olarak yerleştirilmiştir. Bölgesel ısıtmanın dışında, uygulamadaki engeller nedeniyle atık ısı'nın yeniden kullanımı daha karmaşıktır.

Atık ısı'nın yeniden kullanılmasını engelleyen iki önemli engel vardır; ısı talebi ve kalitesi. Uzun mesafelerde ısı iletiminin mümkün olmadığı göz önüne alındığında, atık ısı yeniden kullanımının uygulanmasını içeren herhangi bir veri merkezi tasarımı, bir ısı alım kaynağının yakınında bulunmalıdır. [101] atık ısı için çeşitli özel kullanımları özetledi; alan ısıtma, yerden ısıtma, evsel sıcak su ısıtma, kar eritme, enerji santrallerinde ve endüstriyel proseslerde besleme suyunun ön ısıtılması, biyokütlenin kurutulması, suyun tuzdan arındırılması ve enerji üretimi. Bölgesel ısıtma şebekelerinden alan ısıtmasına olan talep mevsimseldir, bu nedenle atık ısı'nın talebi ve karlılığı yıl boyunca dalgalanmaktadır. Bölgesel ısıtma sistemleri için ısı yeniden kullanımının uygulanması için gerekli olan ilave enerji ve altyapı, toplam elektrik tüketimini ve sermaye harcamalarını artırarak PUE değerini artırmaktadır. Yeniden enerji ERE değer ve (yüzme havuzu, sera, yakındaki binalar ve endüstriyel işlemler) küçük ölçekli, yere özgü

özmler genellikle [102] merkezi ısıtma sistemleri ile karşılaştırıldığında önemli ağır yatırım gerektiren açıklanmıştır.

Isının yeniden kullanımı için ikinci husus ısı kalitesidir. Veri merkezlerinden gelen ısı, hava soğutmalı Dc’lerden 25-35 °C arasında ve sıvı soğutmalı veri merkezlerinden 50-60 °C arasında yakalanan atık ısı ile düşük dereceli ısı olarak kategorize edilir [103] Isıyı yeniden kullanmak için, düşük dereceli bir ısı uygulaması mevcut olmalıdır, aksi takdirde kullanılabilirliği artırmak için ısı pompalarıyla düşük kaliteli ısı yükseltilmelidir. Yatırım ve altyapı maliyeti ile birlikte ısı talebi ve kalitesi, ısı yeniden kullanımının uygulanmasındaki en büyük engellerdir, ancak diğer faktörler ısı yeniden kullanımının benimsenmesini etkileyebilir. İki ayrı kuruluş olarak, veri merkezi ve bölge operatörlerinin karşılıklı öncelikleri olabilir işbirliği içinde çalışmalıdır [103] Daha önce de tartışıldığı gibi, veri merkezi güvenliği, atık ısı yeniden kullanımının uygulanmasında göz önünde bulundurulması gereken birincil operasyonel bir husustur. Gizlilik ve güvenlik nedenleriyle veri merkezleri, enerji kullanımı ve ısının yeniden kullanımı ile ilgili sınırlı verileri ortaya koymaktadır ve şeffaflık eksikliği, ticari atık ısının yeniden kullanımının yavaş benimsenmesinde önemli bir faktör olarak kabul edilmektedir [97]. Şu anda, kaynağın ekonomik potansiyeli göz önüne alındığında atık ısı yeniden kullanım ölçeği sınırlıdır.

5.7.9. Bitcoin Madenciliğinde Termodinamik Süreç

Bugüne kadar Alberta’daki en büyük veri merkezi tesisleri, bu modelde yerel veri merkezini temsil edecek analog olarak seçilen kripto para birimi madenciliği operasyonlarıdır. Bitcoin madenciliği operasyonları, serin iklim ve düşük, öngörülebilir güç oranları arayışı içinde Alberta’ya çekildi. Kanada’nın en büyük kripto para madenciliği şirketi Toronto merkezli Hut 8 mining, Drumheller ve Medicine Hat’ta iki bitcoin madenciliği veri merkezi işletiyor [102].

Bitcoin, ‘blockchain’ adı verilen değişmez bir genel muhasebe defterinde tutulan bir şifreleme protokolü üzerinde çalışan eşler arası bir dijital para birimidir. Merkezi olmayan bir para birimi olarak, bitcoin merkezi bir otorite tarafından verilmez, bunun yerine bitcoin ‘madencilik’ adı verilen bir süreçle işlem görür ve güvence altına alınır. İşlemsel verilerin ‘bloklarını’ eklemek için, uzman bilgisayarlar karmaşık hesaplama problemlerini, sorunun çözümü veya ‘karma’ ile

sonuçlanan ‘iş kanıtı’ şemasını çözer. Bitcoin madenciliği, muazzam miktarda güç ve soğutma gerektiren yüksek performanslı ASIC yongaları kullanılarak gerçekleştirilir.

Bitcoin madenciliğinde enerji maliyeti sınırlayıcı bir faktördür. Tüm para birimlerinde olduğu gibi, bitcoin’in değeri zaman içinde dalgalanarak aktif bitcoin madencilerinin genel işlem gücünü etkiler. Bitcoin proof of work algoritması, zorluk ayarı olarak bilinen kalan bitcoin miktarı azaldıkça zamanla zorluk artar. Çözüm oranı, mevcut ağ madenciliği gücünden bağımsız olarak yaklaşık olarak sabit kalır, bu nedenle değerdeki bir artış, karşılaştırılabilir bir başarı oranını korumak için daha güçlü donanım ihtiyacına karşılık gelir. Rekabetçi kalabilmek için bitcoin donanımının yüksek hash oranına ve düşük enerji ayak izine sahip olması gerekir. 2018’te, bir bitcoin üretiminin, 2500 USD (\$ 3,318 CAD) gücüne kadar olan maliyetlere eşit olduğu tahmin edildi [103].

Diğer veri merkezleri türlerine benzer şekilde, Bitcoin madenciliği tesisleri de operasyonları hakkında çok az şey anlatıyor. Madencilik operasyonlarının etkinliği büyük ölçüde açıklanmamıştır ve PUE iddiaları bağımsız olarak doğrulanmamıştır. Bitcoin’in küresel güç tüketimi 2018’de en az 4,2 Gw’dı ve yılda en az 37 TWh ile tahmini gerçek 69 TWh veya küresel enerji tüketiminin% 0,31’i arasında tüketiyordu. Bitcoin madenciliği Alberta’nın ucuz ve bol doğal gazının karlı bir kullanımı olsa da, Bitcoin’in güvenli ve açık kaynaklı sanal defteri olan blockchain’in değeri gelecekteki diğer pratik uygulamalar için potansiyele sahip. Blockchain kimlik doğrulama, lojistik ve finansal işlemleri barındırmak için kullanılabilir [104].

SONUÇ

Bitcoin olarak bilinen sanal nakit biçiminde yeni bir dijital para birimi, 2009 yılında Satoshi tarafından dünya ile tanışmıştır. Bitcoin, en dikkate değer dijital paradır. Merkezi bir otoritenin kontrol etmediği eşler arası dağıtılmış sisteme dayanır. Tüm işlemlerin kaydını içeren bir tür eşler arası defter sistemi olan Blockchain olarak bilinen tekniğe dayanmaktadır. Tüm işlem seti bloklara kaydedilir. Kullanıcılar tarafından oluşturulan yeni işlemler, Bitcoin ağı üzerinden doğrulamak için imzalı bloklar kullanılarak yayınlanır. İşlem, madencilik süreci ile doğrulanır ve Blockchain'e eklenir. İşlemi bloğa eklemek için madenci kriptografik bulmacayı çözer. Çözülen bulmaca sonucunda madenciler, Bitcoin ile ödüllendirilir.

Blokchain ağını ve kripto paralardan bahsetmiştik. Madencilik Blockchain ağında kripto para üretimine denilmektedir. Madenciliği adından da anlaşılacağı üzere bildiğimiz anlamda madenciliğe benzetebiliriz. Dijital dünyada madencilik işlemi, bir takım matematiksel şifreli işlemleri özel yazılım bilgileri ve kodları ile çözmek anlamını taşır. Madenciliğe “mining”, kripto para üreten madencilere de “madenci” denilmektedir. Blok zincir ağında çözülen her denklem, her yeni blok oluşturulduğunda kripto para ortaya çıkmaktadır. Madenciler blok zincir ağında bekleyen işlemlerden bloklar oluşturarak bunları blok zincir ağında yayınlarak, blok zincirin devam etmesini sağlarlar. Teknik olarak bilgisayar kullanarak bir matematik sorusunu çözmek gibidir. Madenciliğin bir başka tanımı ise, blok zincir ağında bulunan işlemleri incelemek, doğrulamak, onaylamak ve yenilerini üretmek anlamına gelmektedir. Blockzincir ağında bulunan madenler, tıpkı gerçek hayattaki gibi sınırlı sayıda kaynak barındırırlar. Bitcoin örneğinden hareket edecek olursak, Sathosi Nakamoto 21 milyon adet Bitcoin üretmiştir. Tıpkı altın madenleri gibi, kripto para madeninde bulunan kaynakta bir gün bitecektir. Bir kişinin madencilik yapabilmesi için; iyi donanımlı bir bilgisayara, iyi bir madencilik yazılımına, bilgisayarların sürekli işlem yapmasından dolayı ısınmayı önlemek adına soğuk bir mekâna ve enerji harcamaları için yeterli bütçeye sahip olması gerekmektedir. Madencilik işleminde işlem yapan bilgisayarlar yoğun bir şekilde çalıştığından dolayı yüksek enerji tüketmektedirler. Haliyle işlem yapan bilgisayarlar ısınmaktadır ve soğutulmaz ise kullanılmaz hale gelmektedir. Bu konunun önemini şu şekilde açıklayabiliriz; Çin'de Himalayalara yakın yerlerdeki uçak hangarlı, İsviçre'nin alp dağları gibi yerler madencilerin tercih ettiği yerler arasındadır.

Bitcoin yazılımı, düğüm adı verilen güçlü bir bilgisayarda çalışır. Ayrıca, bilgilerin dağıtılmış ağ üzerinden iletilmesine de yardımcı olur. Bilgisayara ve internete erişimi olan herkes ücretsiz yazılımı indirip çalıştırabilir. İletişim için belirli bağlantı noktası açık bırakılmalıdır. Düğüm, çok fazla enerji ve bellek alanı tüketir. İşlemler, kendisi tarafından bilinen düğümler aracılığıyla ağ üzerinden çok hızlı bir şekilde yayılır. Bazı düğümler madencilik düğümleri olarak hareket edebilir ve bu düğümlerde çalışanlar madenciler olarak adlandırılır. Madencilerin işi, tüm çözülmemiş ve sonlanmamış işlemleri bir 36 blok olarak gruplamaktır. Oluşturulan blok daha sonra blok zincirine eklenecektir.

Madenciler, Bitcoin programının bir parçası olan “Proof of Work (POW)” olarak bilinen karmaşık matematiksel bulmacayı çözmektedir. Bulmacalarda madenci, nonce (kriptografik iletişimde sadece bir kere kullanılabilen rasgele bir sayı) olarak bilinen bir sayıyı bulmaya çalışır. Bu numara bloktaki verilerle birleştirilecek ve daha sonra hash fonksiyonundan geçirilecektir.

Asıl soru, madencilerin nonce’yi nasıl bulacağıdır? Çıktıyı tahmin etmek neredeyse imkansızdır. Önceden tanımlanmış sıfır sayısıyla başlayan hash veren sayıyı tahmin etmenin bir yolu yoktur. Dahası, iki ardışık sayı tamamen farklı hash değerlerine sahip olabilir. Doğru nonce’yi bulmanın tek yolu, istenen çıktıyı elde edene kadar denemeye devam etmektir. Madencilik sürecinde aşağıdaki adımlardan geçilir:

- i. Madenci, dağıtılmış ağ üzerinden yayınlanan tüm işlemleri toplar.
- ii. İşlemler kontrol edilir ve doğrulanır. Daha önceden işlemlerin yapılıp yapılmadığı da kontrol edilir.
- iii. En uzun yoldaki en son blok, blok zincirinde seçilir. Maksimum hesaplama gücü elde eden yol, en uzun yoldur.
- iv. Madenci tarafından Proof of Work (İş Kanıtı) çözülür ve çözüm ağdaki tüm düğümlere yayınlanır. Yukarıdaki adımlar tekrar edilir. Bloğa dahil olmayan herhangi bir işlem ise, bir sonraki döngü için kaydedilir.

Madenci bir kez istenen çıktıyı bulur ve bunu ağdaki diğer tüm düğümlere iletir. Madencilerin geri kalanı, çözümün bulunduğu blokta çalışmayı bırakır. İstenilen çıktıyı bulan madenci, ödülünü belirli Bitcoin cinsinden alır. Bir blok madenciliği için başlangıçta 50 Bitcoin verilirken bu değer zaman içerisinde düşmüştür. Ödül değeri her dört yılda bir yarıya düşürülmektedir. Ödül için Bitcoin sayısındaki bu azalma, değerindeki artışla telafi edilmektedir. Ancak piyasaların durumuna göre değer değişebileceği için, değer artışı olacak şeklinde bir garanti yoktur. Bilinen bir gerçek ise zamanla bulmacaların çözümünün zorlaştığı, Bitcoin madenciliği yapmak için gerekli donanım maliyetlerinin ve harcanacak elektrik tüketiminin artacağıdır. Özet olarak kripto para madenciliği, geçerli bloğu bulma sürecidir. İnternete erişimi olan herkes madenci olabilir. Merkezi olmayan dağıtılmış ağ kullandığından, bu görev için yetkiyi devretmek gibi bir durum söz konusu değildir. Sahte işlemlerin yapıldığının tespit edilmesi durumunda dağıtılmış sistem hemen çalışmayı durdurur. Bitcoin geliştiricileri, madencilerin hesaplama işleri yaparken uymaları gereken kuralları tasarlamışlardır. Çok kesin olmak gerekirse, madencilerin yeni bloğu bir öncekine bağlayan, iş kanıtı olarak bilinen bir hash işlevi bulmaları gerekir.

Madencilerin kriptografik bilmeceye dayanan istenen çözümü bulmak için birbirleriyle rekabet ettikleri belirlenmiştir. İstenilen çözüm bulunduğu madenci, ürettiği bloğu blok zincirine ekler ve belirli sayıda Bitcoin ödülü alır. Bitcoin, yalnızca madencinin kriptografik bulmacayı çözmesi durumunda üretilebilir. Her çözümünden sonra bulmacanın zorluğu artmakta ve ödül de düşmektedir. Dönemsel olarak üretilebilecek Bitcoin sayısı, belirli bir miktarı aşamaz. Bulmacayı çözmek için ne kadar donanım yeteneği olursa, madencilik maliyeti o kadar fazla olacaktır.

REFERANSLAR

- [1] Lehman, P., & Johnstone, P. (2010). The Climate-Killers Inside-Measuring the astoundingly high environmental costs of grow houses. Retrieved from North Coast.
- [2] The Climate Group. (2008). SMART 2020: Enabling the low carbon economy in the information age. Brussels, BE: Global eSustainability Initiative.
- [3] Government of Alberta. (2018). Fiscal Plan - Budget 2018. Edmonton: President of Treasury Board and Minister of Finance and its licensors.
- [4] Kırıcı, H. (2016). 2008 Küresel Krizinin Kökeninde Yatan Hatalar ve Dodd-Frank Kanunu Düzenlemeleri(The Origin Mistakes of the 2008 Global Crisis and Dodd-Frank Act Regulations). Celal Bayar Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 468.
- [5] Black, H.C.(1968).Black's Law Dictionary. St. Paul Minnesota, West Publishing Corporation.
- [6] Fama, E.F. (1980).Banking the theory of finance. Journal of Monetary Economics, 6, 39-57.
- [7] Bernanke, B.S. (1983). Nonmonetary Effects of the Financial Crisis in the Propagation of the Great Depression. The American Economic Review,73(3).
- [8] Arestis, P. and Demetriades, P (1997). Financial development and economic growth: Assesing the evidence. Economic Journal, 107,783-799.
- [9] Akgiray, V. (1998). Finansal Yeniliklerin ve Risk Yönetiminin Ekonomik Kalkınmaya Katkıları. İMKB Dergisi,2(5),1-97.
- [10] Beck ,T., Levine, R.,and Loayza, N. (2000). Finance and the Sources of Growth. Journal of Financial Economics, 58(1-2), 261–300.
- [11] Akbulut, R. (2002). Türkiye’de Sermaye Piyasasında Devletin Rolü. Yönetim Dergisi,13(41), 47-65.
- [12] Al-Yousif, Y.K. (2002). Financial Development and Economic Growth: Another Look at the Evidence from Developing Countries. Review of Financial Economics, 11(2),131-150.
- [13] Chang, T.Y.(2002).Financial Development and Economic Growth in Mainland China: A Note on Testing Demand-Following or SupplyLeading Hypothesis. Applied Economics Letters, 9(13),869-873.

- [14] Bostancı, F. (2003). Davranişçi Finans. Davranişçi Finans. İstanbul: Sermaye Piyasası Kurulu Denetleme Dairesi.
- [15] Obstfeld, M., & Taylor, A. M. (2003). Globalization and Capital Markets.
- [16] Tuncer, P. N. (2004). Elektronik Paranın Banknot Kullanımına Etkisi. Ankara.
- [17] Brindle, M. and Cox, R. (2004). Law of Bank Payment. London, Sweet&Maxvell
- [18] Bell, M. A. (2005). Use Best Practices to Design Data Center Facilities. Stamford, CT: Gartner.
- [19] Akay, H. K., & Nargeleçekenler, M. (2006). Finansal Piyasa Volatilitesi Ve Ekonomi. Ankara Üniversitesi SBF Dergisi, (s. 6).
- [20] Alper, Y. D., & Ertan, A. G. (2006). Yatırım Fonu Seçim Kararlarında Çerçeveleme Etkisi. Uludağ Üniversitesi, İİBF, (s. 175-176).
- [21] Ateş, A. (2007). Finansal Yatırımların Davranişsal Finans Açısından Değerlendirilmesi Üzerine Bir Araştırma. Finansal Yatırımların Davranişsal Finans Açısından Değerlendirilmesi Üzerine Bir Araştırma. Konya, Konya: Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü.
- [22] Afşar, A. (2007). Finansal gelişme ile ekonomik büyüme arasındaki ilişki. Muhasebe ve Finansman Dergisi, 36, 188-198.
- [23] Aksoy, A. ve Tanrıöven, C. (2007). Sermaye Piyasası Yatırım Araçları ve Analizi. Ankara: Gazi Kitabevi.
- [24] Anandan, S., & Ramalingam, V. (2008). Thermal management of electronics: A review of literature. Thermal Science Vol. 12, 5-26.
- [25] Chandra, S., Lata, H., Khan, I. A., & Elsohly, M. A. (2008). Photosynthetic response of Cannabis sativa L. to variations in photosynthetic photon flux densities, temperature and CO2 conditions. Phisiology of Molecular Biology Plants, 299-306.
- [26] Turner, W. P., Seader, J. H., Renaud, V., & Brill, K. G. (2008). Tier Classifications Define Site Infrastructure Performance. Santa Fe, NM: [White Paper]. Uptime Institute.
- [27] Afşar, M. (2009). Türkiye’de Eğitim Yatırımları ve Ekonomi ve Büyüme İlişkisi. Anadolu Üniversitesi Sosyal Bilimler Dergisi, 9(1), 85-98.
- [28] Alger, D. (2010). Grow a Greener Data Center. Indianapolis: Cisco.

- [29] An, L and Brown, D. (2010).Equity Market Integration Between The Us and Bric Countries: Evidence From Unit Root and Cointegration Test. *Research Journal Of International Studies*,16,15-24.
- [30] Zhou, T., Lu, Y.,and Wang, B. (2010). Integrating TTF and UTAUT to Explain Mobile Banking User Adoption. *Computers in Human Behavior*, 26, 760– 767.
- [31] Anderson, R., & Pearce, J. M. (2011). Environmental and economic assessment of a greenhouse waste heat exchange. *Journal of Cleaner Production* Vol. 19, 1446-1454.
- [32] National Renewable Energy Laboratory. (2011). Federal Energy Management Program Best Practices Guide for Energy - Efficient Data Center Design. U.S. Department of Energy - Energy Efficiency & Renewable Energy.
- [33] Rasmussen, N. (2011). Electrical Efficiency Measurement for Data Centers. Rueil-Malmaison, FR: APC/Schneider Electric.
- [34] Sujatha, C., & Abimannan, S. (2011). Energy Efficient Free Cooling System for Data Centers. *Proc. 2011 IEEE Third International Conference on Cloud Computing Technology and Science*, 646-651.
- [35] Mills, E. (2012). The carbon footprint of indoor Cannabis production. *Energy Policy* Vol. 46, 58-67.
- [36] Ensor, B., Montez, T., and Wannemacher, P. (2012). The state of mobile banking 2012. Amerika: Forrester Research.
- [37] Fazekas, A.(2012). Silver in Space: Metal Found to Form in Distinct Star Explosions. *National Geographic*. September, 9.
- [38] Covas, M., Silva, C., & Dias, L. (2013). Multicriteria decision analysis for sustainable data centers location. *International Transactions in Operational Reasearch* Vol. 20, 269-299.
- [39] Alp, İ. A. (2013). Terörün Ekonomik Etkileri. *Uluslararası Güvenlik ve Terörizm Dergisi*,, 13.
- [40] Whitehead, B., Andrews, D., Shah, A., & Maidment, G. (2014). Assessing the environmental impact of data centers part 1: Background, energy use and metrics. *Building and Environment*, 151-159.
- [41] Woodruff, J., Brenner, P., Buccellato, A., & Go, D. (2014). Environmentally opportunistic computing: A distributed waste heat. *Energy and Buildings*, 41-50.

- [42] Baker, H., & Ricciardi, V. (2014). How Biases Affect Investor Behaviour. *Insight*, (s. 7-10).
- [43] Kristoufek, L. (2014). What Are the Main Drivers of the Bitcoin Price? Evidence from Wavelet Coherence. *Public Library of Science*, (s. 5).
- [44] Robleh, A., Barrdear, J., Clews, R., & Soutgate, J. (2014). The economics of digital currencies.
- [45] Ali, R., Barrdear, J., Clews, and R., Southgate, J. (2014). The Economics of Digital Currencies. *Bank of England Quarterly Bulletin*, 54(3), 276-286.
- [46] Antonopoulos, A. M. (2014). *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*, O'Reilly Media.
- [47] B ker S., A ıko lu, R. ve G ven, S. (2014). *Finansal Y netim*. Ankara: S zkesen Matbaacılık.
- [48] Alberta Environment and Sustainable Resource Development. (2015). *Carbon Offset Emission Factors Handbook*. Edmonton, AB: Government of Alberta.
- [49] Government of Alberta. (2015). *Carbon Offset Emission Factors Handbook - Specified Gas Emitters Regulation*. Edmonton: Government of Alberta.
- [50] Atik, M., K se, -Y., Yılmaz, B., & Sa lam, F. (2015). Kripto Para: Bitcoin ve D viz Kurları  zerine Etkileri. *Bartın  niversitesi İ.İ.B.F. Dergisi*, (s. 259-260).
- [51] Cheung, A., Roca, E., & Su, J.-J. (2015). Crypto-Currency Bubbles: An application of the Phillips-Shi-Yu (2013) methodology on. *Applied*, (s. 15).
- [52] Edwards, C. (2015). Bitcoin Price Crash Finds New Victims. *Engineering & Technology*, (s. 19).
- [53] Vigna, P., & J. Casey, M. (2015). *Kriptopara  a ı*. Buzda ı Yayınevi. (s. 88).
- [54] Block, W.E. and Davidson, L. (2015). Bitcoin, the regression theorem, and the emergence of a new medium of Exchange. *Quarterly Journal of Austrian Economics*, 18(3), 311-338.
- [55] Chuen, D., Lee, K., and Teo, E.G.S. (2015). Emergence of FinTech and the LASIC principles, *EY Global Financial Services Institute*, 3(3), 1-29.
- [56] Farrell, R. (2015). An Analysis of the Cryptocurrency Industry. *Wharton Research Scholars*, 130, 1-23.

- [57] Rong, H., Zhang, H., Xiao, S., Li, C., & Hu, C. (2016). Optimizing energy consumption for data centers. *Renewable and Sustainable Energy Reviews*, 674-691.
- [58] Dyhrberg, A. H. (2016). Bitcoin, gold and the dollar – A GARCH volatility. *Finance Research Letters*, 92.
- [59] Ateş, B.(2016).Kripto para birimleri, Bitcoin ve muhasebesi. Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,7(1),349-366.
- [60] Bilir, H. ve Çay, Ş. (2016). Elektronik Para ve Finansal Piyasalar Arasındaki İlişki. Niğde Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi. 9(2), 21-30.
- [61] Ganeshalingam, M., Shehabi, A., & Desroches, L. (2017). Shining a Light on Small Data Centers in the U.S. Berkeley, CA: Energy Analysis and Environmental Impacts Division Lawrence Berkeley National Library.
- [62] Johannesson, A. (2017). Swedish district heating: Reducing the nation’s CO2 emissions. Retrieved from Euroheat & Power.
- [63] Moore, S. (2017). Southeast Alberta Energy Diversification Report: Our region, our jobs, our communities. Medicine Hat, AB: Economic Development Alliance of Southeast Alberta.
- [64] Ni, J., & Xuelian, B. (2017). A review of air conditioning energy performance in data centers. *Renewable and Sustainable Energy Reviews*, 625-640.
- [65] Balcilar, M., Bouri, E., Gupta, R., & Roubaud, D. (2017). Can Volume Predict Bitcoin Returns and Volatility? A Quantiles-Based Approach. *Economic Modelling*, (s. 18-19).
- [66] Gültekin, Y., & Bulut, Y. (2017). Bitcoin Ekonomisi: Bitcoin EkoSisteminden Doğan Yeni Sektörler ve Analizi. Adnan Menderes Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi, (s. 83).
- [67] Sahoo, P. K. (2017). Bitcoin as digital money: Its growth and future sustainability. *Theoretical and Applied Economics*, (s. 60-63).
- [68] Andrianto, Y. and Diputra, Y. (2017). The Effect of Cryptocurrency on Investment Portfolio Effectiveness. *Journal of Finance and Accounting*, 5(6), 229-238.
- [69] Baur, D. G., Hong,K and Lee,A. (2017).Bitcoin: Medium Of Exchange Or Speculative Assets? *Journal Of International Financial Markets, Institutions and Money*, 54, 177-189.

- [70] Bouri, E., Molnár, P., Azzi, G., Roubaud, D. and Hagfors, L. (2017). On The Hedge and Safe Haven Properties Of Bitcoin: Is It Really More Than A Diversifier. *Finance Research Letters*, 20, 192-198.
- [71] Dumitrescu, G. C. (2017). Bitcoin – A Brief Analysis of the Advantages and Disadvantages. 13(5).
- [72] Zhu, Yechen, David, D. A. and Jianjun, L. (2017). Analysis On The Influence Factors Of Bitcoin's Price Based On Vec Model. *Financial Innovation*, 3(3), 1-13.
- [73] Laate, E. (2018). Economics of Production and Marketing Greenhouse Crops in Alberta. Edmonton: Alberta Agriculture and Forestry, Economics and Competitiveness Branch, Economics Section.
- [74] Altınırnak, Karaağaç. (2018). En Yüksek Piyasa Değerine Sahip On Kripto Paranın. *Muhasebe ve Finansman Dergisi*, (s. 124,125).
- [75] Exton, J. (2018). Cracking the code on cryptocurrency Bitcoin buy-in across Europe, the USA and Australia. *ING International Survey*.
- [76] Gümüş, U. T., & Evlimoğlu, U. (2018). İtibari Paranın Kullanımdan Kaldırılmasına Yönelik Teorik Bir Değerlendirme. *İzmir Adnan Menderes Üniversitesi Sosyal Bilimler Dergisi*, (s. 168).
- [77] Twentify. (2018). Türkiye'nin Yeni Sanal Cüzdanı. Twentify Araştırma Grubu.
- [78] Alpago, H. (2018). Bitcoin'den Selfcoin'e Kripto Para. *Uluslararası Bilimsel Araştırmalar Dergisi*, 3(2), 411-428.
- [79] Atabaş, A. (2018). Blokzincir Teknolojisi ve Kripto Paraların Hayatımızdaki Yeni Yeri (1.Baskı). İstanbul: Ceres Yayınları.
- [80] Avunduk, H. ve Aşan, H. (2018). Blok Zinciri (Blockchain) Teknolojisi Ve İşletme Uygulamaları: Genel Bir Değerlendirme. *Dokuz Eylül Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi*, 33(1), 369-384.
- [81] Azman, F. (2018). Kripto Para, Kripto Para Ekonomisi. Konya: Eğitim Yayınevi.
- Alptekin, V., Metin, İ. ve Akcan, A. T. (2018). Kripto Para Ekonomisi. Konya: Eğitim Yayınevi.
- [82] Çağlar, Ü. ve Dışkaya, S. (2018). Küreselleşme, Uluslararası Para Sistemi ve Kriz. *İktisat Politikası Araştırmaları Dergisi*, 5(2), 1-24.

- [83] Çetiner, M. (2018). Bitcoin (Kripto Para) ve Blok Zincirin Yeni Dünyaya Getirdikleri. İstanbul Sosyal Bilimler Dergisi, 20, 1-16.
- [84] Alberta Agriculture and Forestry. (2019). Current and Historical Alberta Weather Station Data Viewer. Retrieved from Alberta Agriculture and Forestry.
- [85] Nadjahi, C., Louahlia, H., & Lemasson, S. (2019). A review of thermal management and innovative cooling strategies for data center. Sustainable Computing: Informatics and Systems, 14-28.
- [86] National Energy Board. (2019). Provincial and Territorial Energy Profiles - Alberta. Retrieved from National Energy Board, Government of Canada.
- [87] Büyüklgaz, U. (2019).İçsel para teorisi ve Joan Robinson. Akademik Araştırmalar ve Çalışmalar Dergisi,11(20),219-230.
- [88] Ersan, İ.(2019).Bitcoin: Gelecek mi, Balon mu? Muhasebe Enstitüsü Dergisi,17(60),5
- [89] American Society of Heating, Refrigerating and Air-Conditioning Engineers TC 9.9. (2016). Data Center Power Equipment Thermal Guidelines and Best Practices [White paper]. Atlanta, GA: American Society of Heating, Refrigerating and Air-Conditioning Engineers.
- [90] Asaad, S., Bellofatto, R., Brezzo, B., Haymes, C., Kapur, M., Parker, B., . . . Tierno, J. (2012). A Cycle-accurate, Cycle-reproducible multi-FPGA System for Accelerating Multi-core Processor Simulation. Proceedings of the Association for Computing Machinery Special Interest Group on Design Automation International Symposium on Field Programmable Gate Arrays (FGPA '12), (pp. 153-162.).
- [91] Blom, T. J., Straver, W. A., Ingratta, F. J., Khosla, S., & Brown, W. (2012). Carbon Dioxide in Greenhouses. Guelph, ON: Ontario Ministry of Agriculture Food and Rural Affairs.
- [92] Boulder County. (2014). Resolution 2014-41 A Resolution Creating The Boulder County Energy Impact Offset Fund. Boulder, Colorado.
- [93]Koinedge Farms.(2019). Koinedge Farms. Retrieved From. Erişim adresi : <https://www.koinedgefarms.ca/> Erişim : 24 Mart 2022
- [94] Akdiş, M. (2006). Para teorisi ve politikası (2.Baskı).Ankara: Gazi Kitabevi.
- [95] Akman, C.(2001). Bireysel Yatırımcının Rehberi (1.Baskı).İstanbul: İletişim Yayınları.

- [96] Aksoy, E.(2018). Bitcoin paradan sonraki en büyük icat (1.Baskı).İstanbul: Abaküs Kitap Yayın Dağıtım Hizmetleri.
- [97] Driffill, J. (2003). Growth and Finance. The Manchester School.71(4), 363-380.
- [98] Durmuş,S., ve Polat, M.Ş.(2018).Sanal Para Bitcoin. Kafkas Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,9(18),659-673.
- [99] Erdem, E.(2010).Para banka ve finansal sistem (3.Baskı).Ankara: Detay Yayıncılık.
- [100] Zheng., Zibin., Shaon Xie, Hong.D., Xiangping C and Huaimin W. (2018). Blockchain Challenges and Opportunities: A Survey. International Journal Web and Grid Services, 14(4),352-375.
- [101] Andresen, G.: March 2013 chain fork postmortem. BIP 50,
Erişim Adresi : https://en.bitcoin.it/wiki/BIP_50 , Erişim : 24 Mart 2022
- [102] Kroll, J.A., Davey, I.C., Felten, E.W.: The economics of Bitcoin mining or, Bitcoin in the presence of adversaries.
- [103] CoinDesk, “CoinDesk State of Bitcoin Q2 2014,” Technical Report, CoinDesk July 2014. Erişim Adresi : <http://www.coindesk.com/state-ofbitcoin-q2-2014-report-expanding-bitcoineconomy/> , Erişim : 24 Mart 2022
- [104] Barber, S., Boyen, X., Shi, E., Uzun, E.: Bitter to better, how to make Bitcoin a better currency. In: Financial Cryptography and Data Security.