TEMEL BLOKZİNCİR TEKNOLOJİLERİ

2023
YÜKSEK LİSANS TEZİ
FİNANS VE KATILIM BANKACILIĞI

Nurlan HUSEYNLİ

Tez Danışmanı
Dr. Öğr. Üyesi Hakim AZİZ

TEMEL BLOKZİNCİR TEKNOLOJİLERİ

Nurlan HUSEYNLİ

Tez Danışmanı
Dr. Öğr. Üyesi Hakim AZİZ

T.C.
Karabük Üniversitesi
Lisansüstü Eğitim Enstitüsü
Finans ve Katılım Bankacılığı Anabilim Dalında
Yüksek Lisans Tezi
Olarak Hazırlanmıştır

KARABÜK
Ocak 2023

İÇİNDEKİLER

TEZ ONAY SAYFASI

Nurlan HUSEYNLİ tarafından hazırlanan "TEMEL BLOKZİNCİR TEKNOLOJİLERİ" başlıklı bu tezin Yüksek Lisans Tezi olarak uygun olduğunu onaylarım.

Dr. Öğr. Üyesi Hakim AZİZ .....

Tez Danışmanı, Ticaret Hukuku Anabilim Dalı

Bu çalışma, jürimiz tarafından Oy Birliği ile Finans ve Katılım Bankacılığı Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir. 05/01/2023

Ünvanı, Adı SOYADI (Kurumu) **İmzası**

Başkan : Prof. Dr. Saim KAYADİBİ (KBU) .....

Üye : Dr. Öğr. Üyesi Hakim AZİZ (KBU) .....

Üye : Prof. Dr. Mehmet İSLAMOĞLU (KBU) .....

KBÜ Lisansüstü Eğitim Enstitüsü Yönetim Kurulu, bu tez ile, Yüksek Lisans Tezi derecesini onamıştır.

Prof. Dr. Müslüm KUZU .....

Lisansüstü Eğitim Enstitüsü Müdürü

DOĞRULUK BEYANI

Yüksek lisans tezi olarak sunduğum bu çalışmayı bilimsel ahlak ve geleneklere aykırı herhangi bir yola tevessül etmeden yazdığımı, araştırmamı yaparken hangi tür alıntıların intihal kusuru sayılacağını bildiğimi, intihal kusuru sayılabilecek herhangi bir bölüme araştırmamda yer vermediğimi, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu ve bu eserlere metin içerisinde uygun şekilde atıf yapıldığını beyan ederim.

Enstitü tarafından belli bir zamana bağlı olmaksızın, tezimle ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak ahlaki ve hukuki tüm sonuçlara katlanmayı kabul ederim.

Adı Soyadı: Nurlan HUSEYNLİ

İmza :

ÖNSÖZ

Bu tez çalışmasında, blokzincir teknolojileri, kripto paralar ve grafik analizi gibi konular detaylıca araştırılıp öğretici bir kaynak ortaya konulmuştur.

Bu tez çalışmasının planlanmasında, araştırılmasında, yürütülmesinde ve oluşumunda ilgi, destek, teşvik ve uzman tavsiyesini esirgemeyen, sayın hocam Dr. Öğr. Üyesi Hakim AZİZ'e sonsuz teşekkürlerimi sunarım. Çalışma süresince her zaman yanımda olan, tez çalışmam süresince bana ümit verdiği ve yoğun çalışmalarım sırasında benden desteğini hiç esirgemediği için Arzu YILDIZ'a teşekkür ederim. Sevgili aileme manevi hiçbir yardımı esirgemeden yanımda oldukları için teşekkürlerimi bir borç bilirim.

ÖZ

Dijital bir çağ ile gelişen teknolojik yaptırımlar sonucunda teknoloji, finans, endüstri vb. birçok alanda çalışmakta olan kurumların, firmaların ve hatta şahısların dahi teknolojik gelişmelere ayak uydurması günümüz dünyasında kaçınılmaz olmuştur. Blok zincir kullanımı ile günlük hayatta sözleşmelerin dijital bir koda indirgendiği güvenilir ve şeffaf bir dünya sağlanmaktadır. Kurumlar, bireyler, yapay zekâ ve robotlar; rakipleri ve kendileriyle basit bir şekilde etkileşimde bulunabilmektedir. Böylelikle blok zincir kavramı dünyada hızını kesmeden ivmelenmeye devam etmiştir.

Bu tez çalışmasının amacı, teknolojinin gelişmesiyle birlikte tüm dünyada yıkıcı bir etkiye sahip olan blok zincir ve kripto para bileşenlerini temel olarak analiz etmek ve böylelikle güncel literatüre yeni bir bakış açısı kazandırıp akademik katkı sağlamaktır.

Anahtar Sözcükler: Blokzincir; Kripto Para; Sanal Para; Bitcoin; Ethereum; Tether; BNB; Metaverse; Borsa; Teknoloji.

Bilim Kodu: 115303.

ABSTRACT

As a result of the technological sanctions that have developed in a digital age, it has become inevitable in today's world that institutions, not only technology, finance, or industry, but also companies and even individuals working in many fields, keep up with technological developments. With the use of blockchain, a reliable and transparent world is provided in which contracts are reduced to a digital code in daily life. Institutions, individuals, artificial intelligence, and robots can interact with their competitors and themselves in a simple way. Thus, the concept of blockchain continued to accelerate in the world without slowing down.

The aim of this thesis is to analyze the components of blockchain and crypto money, which have a devastating effect all over the world with the development of technology, and thus provide an academic contribution by providing a new perspective to the current literature.

Keywords: Blockchain; Crypto Money; Virtual Money; Bitcoin; Ethereum; Tether; BNB; Metaverse; Stock Market; Technology.

Science Code: 115303.

ARŞİV KAYIT BİLGİLERİ

Tezin Adı	Temel Blokzincir Teknolojileri
Tezin Yazarı	Nurlan HUSEYNLİ
Tezin Danışmanı	Dr. Öğr. Üyesi Hakim AZİZ
Tezin Derecesi	Yüksek Lisans
Tezin Tarihi	05/01/2023
Tezin Alanı	Finans ve Katılım Bankacılığı Anabilim Dalı
Tezin Yeri	KBÜ/LEE
Tezin Sayfa Sayısı	84
Anahtar Kelimeler	Blokzincir; Kripto Para; Sanal Para; Bitcoin; Ethereum; Tether; BNB; Metaverse; Borsa; Teknoloji

ARCHIVE RECORD INFORMATION

Name of the Thesis	Essentıal Blockchaın Technologıes
Author of the Thesis	Nurlan HUSEYNLİ
Advisor of the Thesis	Assist. Prof. Dr. Hakim AZİZ
Status of the Thesis	Master's Degree
Date of the Thesis	05/01/2023
Field of the Thesis	Department of Finance and Participation Banking
Place of the Thesis	UNIKA/IGP
Total Page Number	84
Keywords	Blockchain; Crypto Money; Virtual Money; Bitcoin; Ethereum; Tether; BNB; Metaverse; Stock Market; Technology.

KISALTMALAR

NFT : Non-Fungible Token (Değiştirilemez Belirteç)

DLT : Distributed Ledger Technology (Dağıtılmış Defter Teknolojisi)

ETH : Ether

FFM : Files FM Token (Dosyalar FM Belirteci)

PoA : Proof of Authority (Otorite İspatı)

PoS : Proof of Stake (Hisse İspatı)

PoW : Proof of Work (Emek İspatı)

BTC : Bitcoin

UNI : Uniswap

BNT : Bancor

COMP : Compound(Birleşik)

MKR : Maker (Yapıcı)

SNX : Synthetix Network Token (Synthetix Ağ Simgesi)

ZRX : 0x

KNC : Kyber Network (Kyber Ağı)

Dapp : Decentralized Application (Merkezi Olmayan Uygulama)

DeFi : Decentralized finance (Merkeziyetsiz Finans)

P2P : Peer-to-peer (Eşe eş)

CPU : Central Processing Unit (Merkezi İşlem Birimi)

USD : United States Dollar (ABD Doları)

GUSD : Gemini United States Dollar (Gemini Doları)

SAI : Single Collateral DAI (Tek Teminatlı DAI)

DGX : Digix Gold Token (Digix Altın Belirteç)

EURS : Euro’lar

BNB : BNB (Binance Coin)

PKC : Public Key Cryptography(Açık Anahtarlı Şifreleme)

DEX : Decentralized Exchanges (Merkezi Olmayan Borsalar)

IP : Intellectual Property (Fikrî mülkiyet hukuku)

BCF : Barzani Charity Foundation (Barzani Yardım Vakfı)

EIP : Ethereum Improvement Proposal (Ethereum İyileştirme Önerisi)

DARPA: The Defense Advanced Research Projects Agency (Savunma İleri Araştırma Projeler Ajansı)

DJIA : Dow Jones Industrial Avarage(Dow Jones Endüstriyel Ortlaması)

TA : Technical Analysis (Teknik analiz)

MACD : Moving Average Convergence/Divergence(Hareketli Ortalama Yakınsaması / Iraksaması)

SMA : Simple Moving Averages(Basit Hareketli Ortalamalar)

EMA : Exponential Moving Averages(Üstel Hareketli Ortalamalar)

RSI : Relative Strength Index(Göreceli Güç Endeksi

ARAŞTIRMANIN KONUSU

Günümüzde gelişen teknoloji ile dijitalleşen finans sektöründe yer alan blok zincir, kripto para birimleri ve merkeziyetsiz finans konuları geliştirilen yüksek lisans tezi ile ortaya konmuştur.

ARAŞTIRMANIN AMACI VE ÖNEMİ

Bu tez çalışmasında son yıllarda tüm dünyayı etkisi altına almış yenilikçi bir teknoloji olan blokzincir ve kripto para bileşenlerini anlamak, analiz etmek ve böylelikle güncel bilgilerle yeni bir bakış açısı kazandırıp akademik katkı sağlamak amaçlanmıştır.

ARAŞTIRMANIN YÖNTEMİ

Çalışma sırasında yapılan analizler, analitik araştırmalar yaklaşımı ve belge analizi yöntemi başta olmak üzere ek olarak betimsel yaklaşımla desteklenmektedir.

ARAŞTIRMA HİPOTEZLERİ / PROBLEM

Blokzincir teknolojileri güvenilir midir? Kripto paralarda kâr- zarar durumları nedir? Kripto para borsalarında grafik analizi ile kar etmek mümkün mü?

Hipotezler:

1. Kripto para birimleri küresel olarak kullanılabilir.
2. Akıllı Sözleşmeler doğrulama, yürütme ve dolandırıcılık önleme maliyetlerini büyük ölçüde azaltır ve şeffaf sözleşme sağlayabilir.
3. Blokzincir teknolojileri sayesinde dünyanın her yerine çok ucuz, hızlı ve güvenli para transferi yapılabilir.
4. Akıllı sözleşmelerde el yazısının yerini dijital imzalar alabilir.

KAPSAM VE SINIRLILIKLAR/KARŞILAŞILAN GÜÇLÜKLER

Araştırma kapsamında ele alınan çalışmalar, 2007-2022 yılları arasında gerçekleştirilen “makale” ve “dijital araştırmalar” türlerindeki çalışmalardan elde edilmiştir.

GİRİŞ

Blok zinciri (Blockchain) teknolojisi, son zamanlarda literatürde sıkça yer verilen ve kendine ait spesifik öz nitelikleri iç yapısında barındıran bir veri tabanı çeşididir. Teknolojinin finansman ve maliyet endüstrisi, başlıca kullanıcısı olarak görülmektedir. Bu durumun en büyük sebeplerinden bir tanesi bu alanda yapılan çalışmaların ve uygulamaların daha sık ve güncel olmasından kaynaklanmaktadır. Bu teknolojide verinin nasıl ekleneceğine yönelik kurallar bulunur ve veri bir kez kaydedildiğinde bu veriyi silmek ya da değiştirmek neredeyse imkânsızdır. Blokzincir, içerisinde veriler olarak çağımızda en can alıcı varlıklar olan blokları barındırır. Bu blok verileri art arda yapılar ile birbirine zincirlenir. Böylelikle art arda gelen bloklar, bir önünde duran bloktan bir özellik alarak hafızasında yer tutar. Bunun sonucunda en son güncellenmiş bloğa bakılarak ve sonda yer alan veri bloğunun üstüne konularak kontrol edilmesi mümkündür.

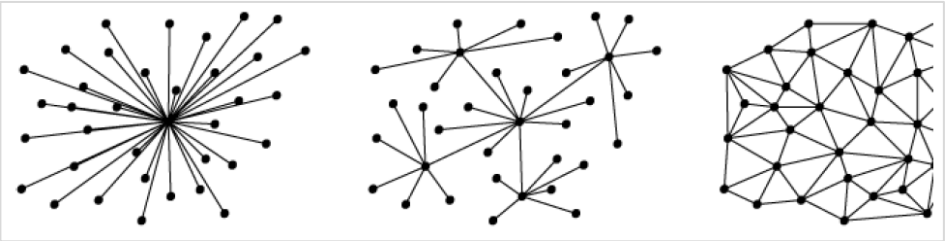
Çalışma kapsamında var olan bölümlerden ilki olan giriş bölümünde, gerçekleştirilen tez çalışmasının kısa özetine ve amacına yer verilmiştir. Çalışmanın birinci bölümünde, tez çalışmasının ana hedefi olan Blokzincir teknolojilerinin gelişen teknoloji ve verimlilik ile birlikte değişimine yer verilmektedir. İkinci bölümde, bu tez çalışmasında ana unsur olan blokzincir, kripto para birimlerine ve merkeziyetsiz finans kavramlarına yer verilmektedir. Bir sonraki bölüm olan üçüncü bölümde ise finansal açıdan piyasalar ve Blokzincir teknolojisinin bağlantıları analiz edilerek dijital finansallaşma ile tüm detayları verilecek biçimde tanıtılmıştır. Bu bölümde Blokzincir teknolojisinin geleceğe yönelik uygulamalarından olan Değiştirilemez Belirteç (NFT), kuantum bilgisayarlar, spot piyasa ve spot alım satımı kavramlarına yer verilmiştir. Çalışmanın son bölümünde, tez dönemi boyunca araştırılan kripto para birimleri ve Blokzincir teknolojisinin kullanım alanları hakkındaki çalışmalara ve nihai sonuçlarına yer verilmiştir.

1. BLOKZİNCİR VE TEKNOLOJİLERİ

Günümüz dünyasında teknolojinin ve dijital dünyanın gelişmesiyle birlikte birçok alanda Blokzincir teknolojisi ve finansal araştırmalar büyük çapta ilgi görmekte ve birbirinden farklı birçok sektörde projelere yön vermektedir. Birden fazla alana yön veren Blokzincir teknolojisinin asıl tematiği finans sektörünü işaret etmektedir. Çünkü finans ve ekonomi alanında Blokzincir kavramı başlıca kullanıcı olarak görülmektedir [1]. Blokzincir kavramının soyutsal açıdan oluşturulma adımları göz önüne alınıp incelendiğinde, tıpkı bir zinciri andırdığı için blok zincir yapısının oluşturulmasını görmek oldukça mümkündür [2]. Blokzincir teknolojisi ise medikal, ekonomi, bankacılık, finans ve medya platformları gibi bireylerin ihtiyaç duyduğu birçok platformda yer alarak farklı bakış açıları sunmaktadır. Ayrıca, şifreleme algoritmaları başta olmak üzere kriptografi alanlarında birçok güven problemine çözüm üretmektedir [3]. Sınıflardan oluşan sosyal topluluklar ve finansal yaşantının henüz yakın gelecekteki çarpıcı değişikliklerini ortaya çıkaran Blokzincir, günden güne artan ve geliştirilen birçok alanda yer almaktadır. Blokzincir; kamusal, örgütsel ve şahsi servislerin sunumuna dayalı aktiviteleri değiştirme şansına sahip olduğu için hayati ehemmiyet arz etmektedir [4]. Özetle, tüm durumlar için özelleştirilebilen zincir yapısının özelliklerini tanımlayan bir protokol üzerinde çalışılır [5].

Temel yapısı gereği blok zincirler, her bir satır kaydın veya blokların güvence altına alındığı ve ardışık bloklarına ***hash*** işlevleri ile bağlandığı ve böylece bu blok zinciriyle sonuçlanan dağıtılmış bir defter olma temel özelliğinden türetilmiştir. Ardışık her blok, önceki bloğun hash kodunu saklar. Böylece, önceki bloğa herhangi bir değişiklik yapılırsa buna karşılık gelen karma değiştirilir ve bu nedenle burada, depolanan ile bir uyumsuzluk ortaya çıkar. Böylelikle bu özellik, blok zinciri kurcalamaya karşı dayanıklı hale getirir [6].

Şekil 1 incelenip konvansiyonel yöntemler ile kıyaslandığında Blokzincir kavramının temel farklılıklarından birisi, merkezi olmayan bir yönü merkezi bir çekirdek ile birleştirmek yerine tamamen dağıtık (distributed) sistemlere izin vermesidir [5].



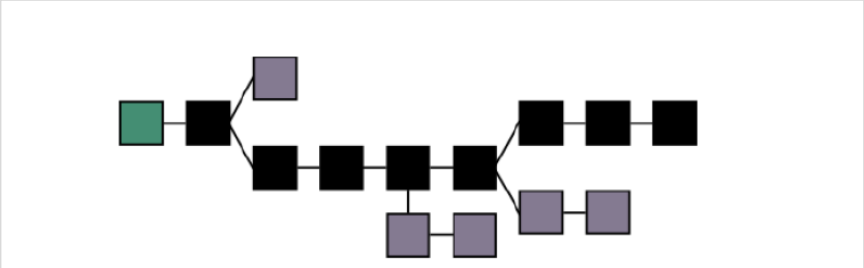
Şekil 1. Merkezi, merkezi olmayan ve dağıtılmış modlar şematik fark [7].

Blokzincir teknolojisinde yer alan bloklardaki zincir verileri, her bir girdi verisinde birleştirilen ve depolanan süreçler ile ilgili detaylı özellikleri içermektedir. Getirilen ve oluşturulan her bir yeni (seri) veri, kullanılabilir olduğu zaman yeni blok verileri halinde düzenlenir ve bloklardaki zincirlere ek olarak ilave edilir [5]. Blokzincir kavramı detaylı incelenecek olursa iki sütunlu bir çizelge olduğu varsayıldığında ilk satırın ilk hücresine kaydedilmek istenen bir veri girilmesi söz konusudur. Girilen hücrenin bilgisi, otomatik olarak arka planda iki harfli bir belirtece (token) çevrilir. Ardından bir sonraki gelecek girdi verisinin ise oluşturulduğu bir alanı temsil eder. Varsayılan örnekteki iki harfli belirteç olan **KP**, alttaki veride bulunan sonraki hücreyi doldururken kullanılmaktadır (**defKP**).

Tablo 1. Girilen her girdinin bir öncekine bağlı olduğu bir veritabanı örneği [6].

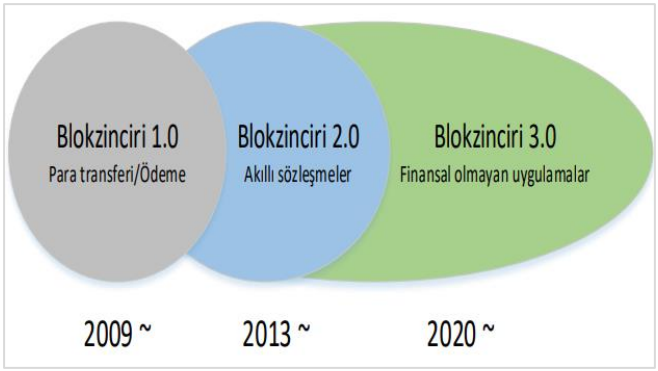
0	abcAA	KP
1	defKP	CD
2	ghiCD	BM
3	jklBM	NS
4	mnoNS	TH

Tablo 1, göz önünde bulundurulduğunda, girdi olarak bilgisi verilen veri değiştirildiğinde, otomatik olarak değiştirildiği sonucuna da ulaşılmaktadır [6]. İlk indiste yer alan satırın son durumuna bakıldığında oluşturulmuş son belirtecin “TH” olduğu sonucuna ulaşılacaktır. Bununla birlikte, tüm oluşan belirteçler ve zincirleme yapısı düşünüldüğünde Blokzincir kavramının hayata nasıl geçirildiğine dair somut kanıtlara ulaşılmıştır.



Şekil 2. Tematik bir blok zincirin şematik gösterimi [8].

Blokzincir teknolojisinin sürdürülebilirliği, süreçlerin ve belirteçlerin geçerliliğini doğrulayan ve veri madenciliği süreciyle yeni bloklara eklenen bir düğüm ağıyla sağlanır. Blokzincir ağı sırasında, uygulanan prosedürleri bloklara ayırma ve ilave etme sürecini madenciler gerçekleştirir [9]. Şekil 2'de yer alan Blokzincirin yapıları, veri blokları açısından sadece uygulamalar için kullanışlıdır. Ancak birbirini ayırt edemeyen bireylerin eş güdümlü olabilmesini sağlayan araçlar kullanıldığı zaman ilgi çekici hale gelmektedir [6]. Günümüzde Blokzincir uygulamaları; geliştirme aşamalarına göre 1.0, 2.0 ve 3.0 aşamaları olmak üzere üç geniş kategoriye ayrılır.



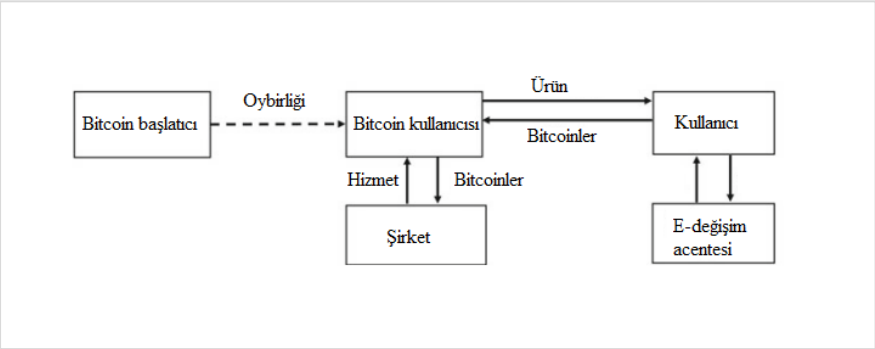
Şekil 3. Blokzincir teknolojisinin yıllara göre evrimi [9].

Şekil 3'te görüldüğü üzere yıllara göre Blokzincir teknolojileri 1.0 versiyonundan başlayarak 3.0'a kadar belirli zaman aralıklarında ilerlemektedir. Bl

Blokzincir 1.0 döneminde yalnızca para transferi ve ödeme transferi sağlanırken; 3.0 ve türevlerinde finansal olmayan daha teknolojik ve gelişmiş uygulamalar dönemine geçildiği görülmektedir.

1.1. Blokzincir 1.0 Teknolojisi

Blokzincir 1.0 teknolojisi veya dijital para safhası, nakit aktarımı ve dijital ödeme gib tatbikatları içerisinde bulunduran kripto paraları anlatmaktadır [10]. "Blokzincir 1.0" kategorisi, gerçek para birimlerine alternatif olarak kullanılabilen Bitcoin (ör. euro veya dolar) gibi sanal (kripto) para birimlerini içerir. Bu zamana kadar Bitcoin, halk için en iyi bilinen Blokzincir uygulaması olmaya devam ediyor ve giderek daha popüler hale gelmektedir [11].



Şekil 4. Bitcoin kullanımı ile çalışma prensibi [12].

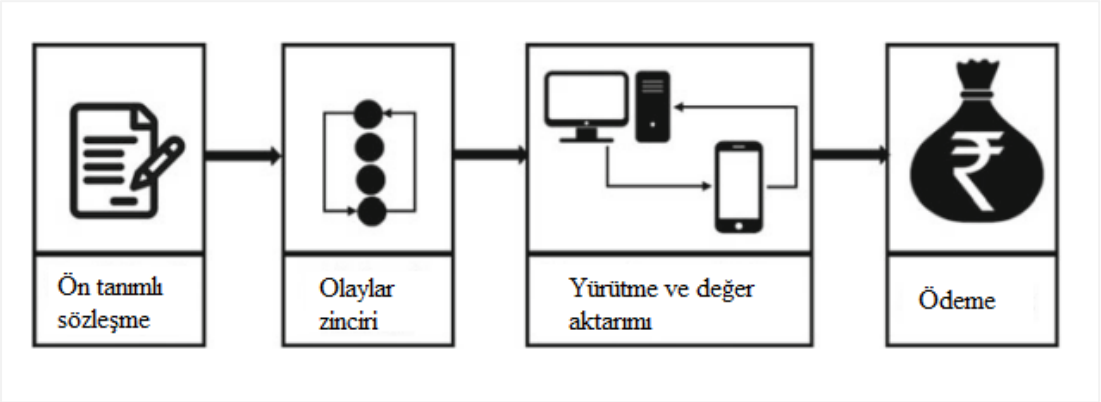
Şekil 4, Bitcoin yapıları ile genel çalışmayı verir. Birinci nesil Blokzincir, Blokzincir 1.0, Dağıtılmış Defter Teknolojisi (DLT) kavramından yola çıkmıştır. Dağıtılmış defter, birkaç katılımcı arasında mutabakatla paylaşılan bir veri tabanıdır ve böylece kamu tanıklarının çifte harcama senaryolarını ortadan kaldırmasını sağlar. DLT'nin en belirgin uygulaması, Bitcoin'in çok önemli bir rol oynadığı kripto para birimiydi. Bitcoin böylece "internet için nakit" oldu ve "Paranın İnterneti" için yolu açmıştır. 2009 yılında piyasaya sürülmesinden sonra Bitcoin, işlem kayıtlarını takip etmek ve bu kayıtların yetkisini bir kullanıcıdan diğerine doğrudan aktarmak için istikrarını, güvenilirliğini, verimliliğini, basitliğini, bağımsızlığını ve güvenliğini kanıtlamıştır [12].

1.2. Blokzincir 2.0 Teknolojisi

Birinci nesil Blokzincir'in savurgan madenciliği ve zayıf ölçeklenebilirliği, Buterin'i Blokzincir kavramını para biriminin ötesine genişletmeye teşvik etmiştir. Bu, Proof of Work konsensüs mekanizmalarıyla birlikte yeni akıllı sözleşme kavramlarına dayanan ikinci nesil Blokzincir yani Ethereum'un ortaya çıkmasına yol açmıştır [12].

Blokzincir 2.0 teknolojisi kapsamında, Ethereum yalnızca bir kripto para biriminden ibaret olmayıp aynı zamanda dağıtık bir yapıdan oluşmaktadır. Buna ek olarak, Ethereum biriminin üzerinde daha sonradan 'Ether' adında kripto para inşa edilmiştir [11]. Bahsi geçen kripto para birimlerine, tez çalışmasında Bölüm 3'te detaylı bir şekilde yer verilmiştir.

Akıllı Sözleşmeler [13], iki taraf arasında önceden tanımlanmış maddeler temelinde otomatik olarak yürütülen otonom, kendi kendini yöneten bilgisayar programlarıdır. Bu sözleşmelerin çalınması veya tahrif edilmesi imkânsızdır. Bu nedenle Akıllı Sözleşmeler [14]; doğrulama, yürütme ve dolandırıcılık önleme maliyetlerini büyük ölçüde azaltır ve şeffaf sözleşme tanımını etkinleştirir [12].



Şekil 5. Akıllı sözleşmenin çalışma prensibi [12].

Şekil 5, akıllı sözleşmelerin nasıl çalıştığını gösterir. İlk adım, iki taraf arasındaki sözleşmenin formüle edilmesidir. Anlaşmanın şartlarını, kurallarını ve koşullarını iki muhatap tarafından kabul edilmesi ve bir koda dönüştürülmesini içerir. İlgili tarafların rızası olmadan sözleşmede herhangi bir değişiklik yapılamaz. Akıllı sözleşme daha sonra blok zincirine yerleştirilir. Sözleşmede belirtilen olaylar gerçekleşir gerçekleşmez kod otomatik olarak yürütülür. Bu tür olayların pratik örneği, bir sigorta poliçesinin sona ermesi veya mal teslimi olabilir. Kodun yürütülmesi sona erdiğinde sözleşme değeri otomatik olarak ilgili alıcıya aktaracaktır. Böylece yerleşim, anında güvenli ve verimli bir şekilde tamamlanır. Bu transfer de blok zincirine kaydedilir [12]. Böylece güvenli ve hızlı bir ticari işlem yapılmış olabilir.

1.3. Blokzincir 3.0 Teknolojisi

Blokzincir 1.0 ve 2.0 teknolojilerinin en büyük dezavantajı, çoğunlukla İş Kanıtı'na dayalı olarak ölçeklenemez olmaları ve işlemleri onaylamak için saatler sürmesidir. Bütün bunlar, kripto para birimlerini küresel olarak uygulanabilir hale getirmeyi amaçlayan Blokzincir 3.0 adlı mevcut nesil Blokzincir'in doğuşuna izin verdi. Akıllı sözleşmelerin yanı sıra, üçüncü nesil Blokzincir esas olarak Merkezi Olmayan Uygulamaları (dApps) içerir [17]. Tek bir bilgisayar yerine Blokzincir bilgisayar ağında çalışan dijital programlardır ve bu nedenle herhangi bir merkezi otoritenin kapsamı dışındadır. Dolayısıyla bu nesil, parçalama gibi tekniklerin yardımıyla zincirler arası işlemleri teşvik etme yeteneğine sahiptir [18]. Parçalama, her bir Blokzincir düğümünün, tam bilgiyi değil, üzerindeki verilerin yalnızca bir kısmını içerdiğini ifade eder. Bu, yükü yayar ve sistemi verimli ve izinsiz girişlere karşı dayanıklı hale getirir [12].

Blokzincir 3.0 ayrıca, ayrı işlem ücreti olmaksızın akıllı sözleşmeler için artırılmış hız ve bilgi işlem gücü sağlamak için Proof of Stake ve Proof of Authority [19] konsensüs mekanizmalarını kullanır. Blokzincir 3.0 başlangıçta olmasına rağmen, Hızlı, Hissiz ve Madensiz'in kısaltması olan "FFM" konsepti üzerine tasarlandıkları için önceki nesillerin ölçeklenebilirliğini, birlikte çalışabilirliğini, gizliliğini ve sürdürülebilirliğini iyileştirmeyi hedefliyor. Blokzincir 3.0, bu nedenle, işlemleri doğrulamak ve doğrulamak için madencilere olan bağımlılığı ortadan kaldırır ve bunun yerine bunun için yerleşik mekanizmaları kullanır. Bu nedenle, önceki nesillerinden farklı olarak saniyede binlerce işleme izin vermek için son derece hızlıdırlar [12].

1.3.1. Proof of Work (PoW)

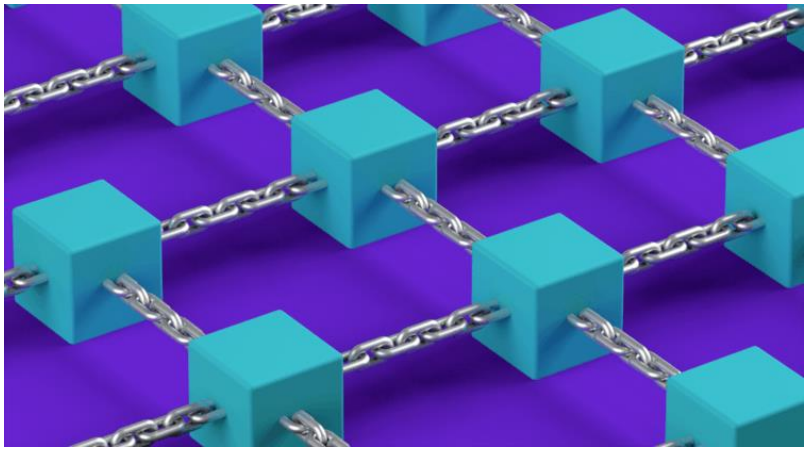
Proof of work (PoW), istenmeyen e-postalar göndermek veya hizmet reddi saldırıları başlatmak gibi bilgi işlem gücünün anlamsız veya kötü niyetli kullanımlarını caydırmak için önemsiz olmayan ancak uygulanabilir miktarda çaba gerektiren bir sistemi tanımlar [20]. Özetlemek gerekirse, istenmeyen siber hücumlara karşı tedbir olarak bildirilen ve Blokzincir ağlarında yer alan bir protokoldür [21].

1.3.2. Proof of Stake (PoS)

PoW protokolüne işlem gücü veya hesaplama gücüne bakılmaksızın seçenek olarak ortaya çıkmıştır. PoS protokolünde gerçekleştirilen prosedürlerde var olan blok zincirlerinin konfirmasyonu kripto para birimleri vasıtasıyla ortaya konmaktadır [21]. PoS, işlemleri işlemek ve bir blok zincirinde yeni bloklar oluşturmak için bir kripto para birimi konsensüs mekanizmasıdır. Bir fikir birliği mekanizması, dağıtılmış bir veri tabanına girişleri doğrulamak ve veri tabanını güvenli tutmak için bir yöntemdir. Kripto para birimi söz konusu olduğunda, veritabanına blok zinciri adı verilir. Bu nedenle fikir birliği mekanizması blok zincirini korur [12].

1.4. Ağlar Arası Köprü

Bir Blokzincir köprüsü, aralarında etkileşimi sağlamak için iki blok zincirini birbirine bağlayan bir protokoldür. Bitcoin sahibi olup Ethereum ağındaki DeFi etkinliğine katılım sağlandığında bir Blokzincir köprüsü, Bitcoin varlığının satılmadan yapılmasını sağlar. Blokzinciri köprüleri, blok zinciri alanı içinde birlikte çalışabilirliği sağlamak için esastır [22].



Şekil 6. Örnek bir blokzincir köprü bağlantısı [22].

Blokzincir köprüleri, Bitcoin ve Ethereum gibi çok farklı ağlar arasında ve bir ana blok zinciri ile yan zincir adı verilen ve farklı fikir birliği kuralları altında çalışan veya güvenliğini ana blok zincirinden devralan alt zinciri arasında birlikte çalışabilirliği sağlar. Bu birlikte çalışabilirlik, bağımsız platformlar arasında belirteçlerin, verilerin ve hatta akıllı sözleşme talimatlarının transferini içerebilir ve kullanıcıların şunları yapmasına olanak tanır:

- Bir blok zincirinde barındırılan dijital varlıklar diğerinde Dapp varlıklarına dağıtılmalıdır. Aksi takdirde daha az ölçeklenebilir zincirlerde barındırılan jetonlarla, hızlı ve düşük maliyetli işlemler gerçekleştirilir.
- Dapp'ler birden fazla platformda yürütülmelidir.
- Bazı blok zinciri köprüleri merkezileştirilirken, diğerleri Merkeziyetsiz Finans (DeFi) protokollerinin güvenliğini ve açıklığını sağlamaya yardımcı olan tüm önemli ademi merkeziyetçiliği korur [23].

Şekil 7. Varlıkları kilitlemek ve başka platformda basma özellikleri [23].

Şekil 7 incelendiğinde bir kullanıcı, merkezi olmayan bir köprü kullanarak varlıkları bir blok zincirinden diğerine aktardığında bu varlıklar tam anlamıyla yeniden konumlandırılmaz veya herhangi bir yere gönderilmez. Bunun yerine, işlevsellik iki aşamalı bir süreçle güçlendirilir: İlk olarak, varlıklar bir akıllı sözleşme veya akıllı sözleşmeler desteklenmiyorsa başka bir mekanizma kullanılarak yaşadıkları blok zincirinde kilitlenir veya dondurulur. Ardından, alıcı blok zincirinde eşit miktarda yeni jetonlar oluşturulur. Kullanıcı varlıkları kullanmak istediğinde eş değer jetonlar yakılır ve ardından orijinal varlıkların kilidi açılır. Bu işlem, varlıkların aynı anda her iki zincirde de herhangi bir şekilde kullanılmasını engeller.

2. BLOKZİNCİR VE KRİPTO PARA İLİŞKİSİ

Blokzincir, Bitcoin dahil olmak üzere ortaya çıkan kripto para birimlerinin altında yatan temel teknolojidir. Blok zincirinin en önemli avantajı yaygın olarak ademi merkeziyetçilik olarak kabul edilir ve veri şifreleme, zaman gibi tekniklere dayalı olarak bireysel düğümler arasında karşılıklı güven ve merkezi kontrol olmaksızın aracısız eşler arası (eşler arası(P2P) işlemleri, koordinasyon ve dağıtılmış sistemlerde iş birliği) kurulmasına yardımcı olabilir [24]. Bir para birimi, parasal değerleme ile ilgilenir; bu nedenle, piyasa değerini belirlemek gereklidir. Kripto para borsaları aracılığıyla getirilebilir [25].

2.1. Blokzincir ve Kripto Para Birimleri

Bitcoin, 2016'ya kadar Blokzincir'in en başarılı uygulama senaryolarından biridir. Blockchain.info izleme web sitesinde [26] bildirilen en son istatistiklere göre, günlük ortalama olarak Bitcoin, Blokzincir defterine 75 milyon dolar transfer edilen 120.000'den fazla işlem yazıldı ve şu anda 500.000'den fazla blok oluşturuldu. Ayrıca coinmarketcap.com web sitesi tarafından, 2018'de toplam piyasa değeri 500 milyar doları aşan blok zincirle çalışan piyasalarda 1500'den fazla kripto para birimi türü olduğu ve Bitcoin'in bir piyasa değeri muhasebesi ile baskın konumda olduğu bildiriliyor. Bu durum toplam değerin %37'sinden fazlası için ve ETH ve Ripple sırasıyla ikinci ve üçüncü sırada yer alıyor [27, 28].

2.1.1. Bitcoin (BTC)

Bitcoin ve diğer kripto para birimlerinin çoğu, aşağıdaki beş açıdan geleneksel elektronik nakitten farklıdır: Birincisi; Bitcoin, merkezi kontrol veya hiyerarşik yapı olmadan tamamen merkezi değildir. Aslında Bitcoin, P2P ağlarındaki bilgi işlem düğümleri arasında çalışan dağıtılmış fikir birliği algoritmaları tarafından kontrol edilir. Bununla birlikte, geleneksel elektronik nakit paralar tipik olarak merkezi hizmet sağlayıcılara ihtiyaç duyar ve bu nedenle hükümetler veya belirli şirketler tarafından merkezi olarak kontrol edilir. İkincisi, Bitcoin e-posta gibi sözde anonimdir. Bir Bitcoin kullanıcısının adresi bilinebilir, ancak tam olarak kim olduğu bilinemez. Aksine, çoğu

geleneksel elektronik para anonim değildir ve kullanıcı kimlikleri merkezi hizmet sağlayıcılar tarafından kaydedilecektir [28].

Şekil 8. CoinMarketCap bitcoin görseli [29].

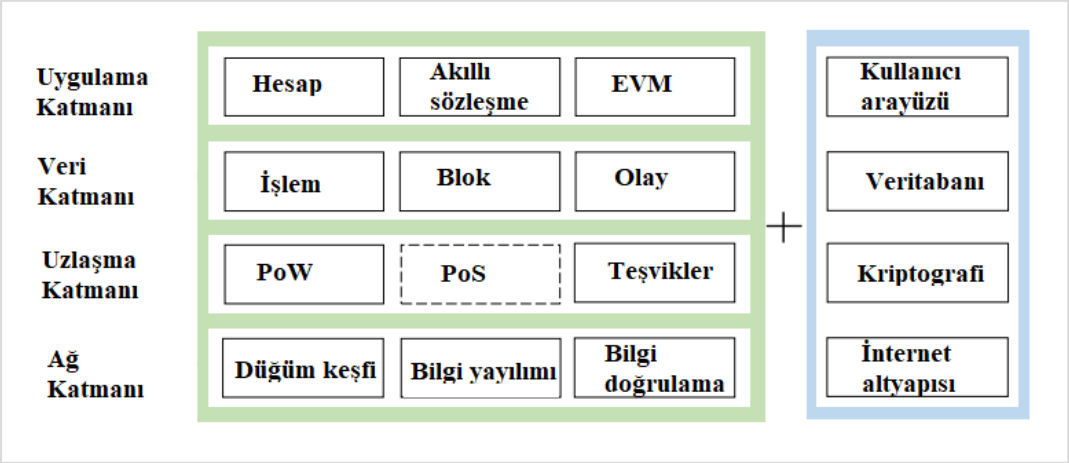
Bitcoin halka açık kaynaktır. Herkes Bitcoin'in kaynak kodunu kontrol edebilir ve böylece her biri Bitcoin ihracının altında yatan mekanizmaları anlayacaktır. Bununla birlikte, çoğu geleneksel elektronik paralar kapalı kaynaklıdır ve kritik iş mantığı her zaman kullanıcılar için gizli tutulur. Son olarak, Bitcoin'in kendisinin bir değeri yoktur, sadece sıfırlar ve birler dizisidir. Ancak Bitcoin kullanıcı sayısını artırarak değer kazanabilir. Kullanıcı ne kadar çok Bitcoin'e güvenir ve kullanırsa Bitcoin o kadar değerli olacaktır. Buna karşılık, neredeyse tüm geleneksel elektronik paralar Fiat para tarafından onaylanır [28].

Bitcoin, esasen dağıtık sistemlerde üretilen elektronik bir nakittir. Bitcoin ihracı, belirli bir merkezi otorite yerine PoW tabanlı madencilik olarak bilinen dağıtılmış ağ düğümleri arasında bir fikir birliği rekabetine dayanır. PoW tabanlı fikir birliği sürecinde P2P ağındaki her bir bilgi işlem düğümü, kendi bilgi işlem kaynağına (CPU) katkıda bulunur ve dinamik olarak ayarlanabilen zorluklarla matematiksel olarak zor bir bulmacayı çözmek için rekabet eder. Daha spesifik olarak mutabakat sürecinin her turunda, yeni Bitcoin işlemleri P2P ağına yayınlanacaktır [28].

2.1.2. Ethereum (ETH)

Ethereum, akıllı sözleşmeler için büyük bir blok zinciri tabanlı platformdur. Karşılıklı olarak güvenilmeyen düğümlerden oluşan eşler arası bir ağ, genel duruma ilişkin ortak bir görüş sağlar ve istek üzerine kod yürütür. Belirtilenler, Bitcoin'dekine benzer bir iş kanıtı konsensüs mekanizması ile güvence altına alınmış bir blok zincirinde saklanır. Ethereum'un temel değer önerisi, karmaşık iş mantığını uygulamaya uygun tam özellikli bir programlama dilidir.

Güvenilir bir üçüncü taraf olmadan merkezi olmayan uygulamalar, kitle fonlaması, finansal hizmetler, kimlik yönetimi ve kumar gibi alanlarda çekicidir. Akıllı sözleşmeler, kriptografi, fikir birliği algoritmaları ve programlama dillerinden yönetişim, finans ve hukuka kadar uzanan alanları kapsayan zorlu bir araştırma konusudur [30].



Şekil 9. Ethereum blok zincirinin mimarisi ve çalıştığı ortamı [31].

Şekil 9 incelendiğinde ortam, uygulamalarla etkileşim kurmak için bir web kullanıcı arayüzü, blok zinciri verilerini depolamak için veri tabanları, fikir birliği protokollerini desteklemek için kriptografik mekanizmalar ve ağ katmanı için İnternet hizmeti aracılığıyla Ethereum mimarisinin dört katmanına hizmet ettiği sonucuna varılmaktadır [31]. Bölüm 2'de anlatılan PoW ve PoS varlıklarının uzlaşma katmanında yer aldığı görülmektedir. Şekilde mavi kutucuklara ayrılan altyapı ve varlıkların ise çevresel etkenlerden kaynaklandığı sonucuna varılmıştır.

Şekil 9 Ethereum'un dört katmanlı mimarisini vurgulamaktadır. Uygulama katmanında Ethereum istemcileri, akıllı sözleşmelerin Ethereum hesaplarıyla ilişkilendirildiği EVM'de akıllı sözleşmeler yürütür. Veri katmanı, blok zinciri veri

yapılarını içerir. Konsensüs katmanı, blok zincirinin tutarlı bir durumunu garanti eder. Ethereum'un mevcut İş Kanıtı (PoW) kullanımını Hisse Kanıtı (PoS) ile değiştirmeyi planladığı unutulmamalıdır [31]. Ağ katmanı ise bir düğümün her zaman bazı aktif düğümlerden blok zincirinin güncel durumunu alabilmesi için bir Ethereum P2P düğümler veya istemciler ağını yönetir.

Ethereum, Vitalik Buterin'in makalesinde [32] tanıtılmıştır ve bu makalede Bitcoin'in komut dosyası dilinin çeşitli sınırlamalarına değinilmiştir. Ana katkılar tam Turing bütünlüğüdür. Yani Ethereum, döngüler dahil her türlü hesaplamayı destekler. Ardından Ethereum, işlemin durumunu ve Blokzincir yapısındaki diğer birkaç iyileştirmeyi destekler [30].

2.1.3. Kararlı Para (Stable Coin)

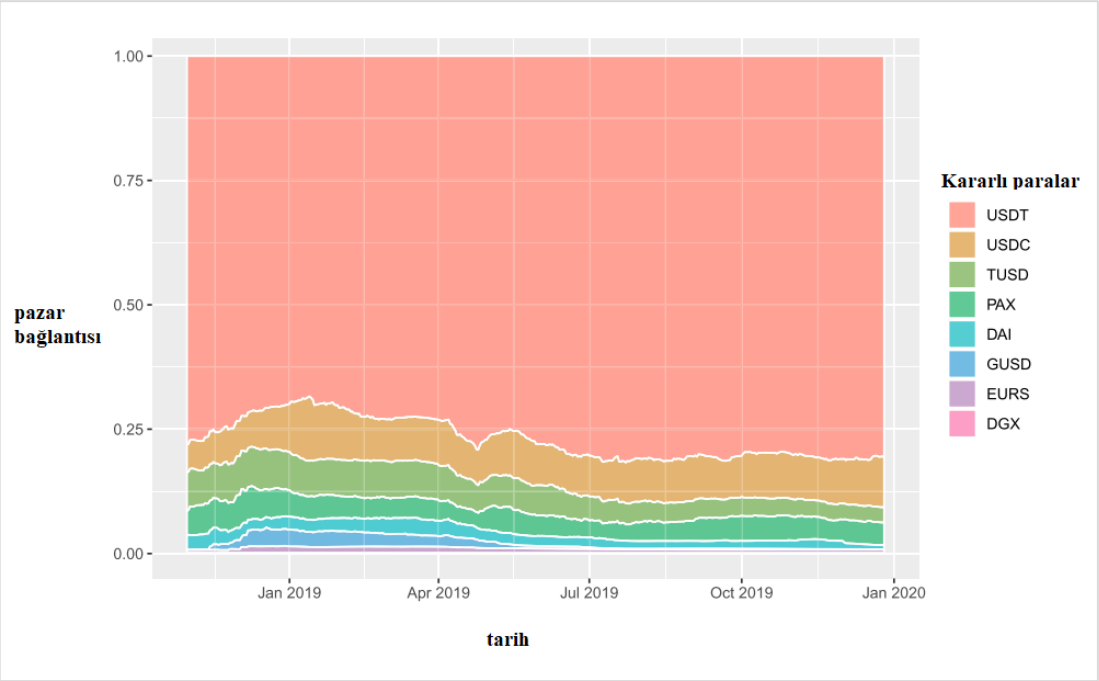
İlk kripto para olan Bitcoin 2008'de, ilk kararlı paralar (bitUSD ve Tether) 2014 yılında oluşturulmuştur. Kararlı paralar birkaç yıldan beri var olmasına rağmen, akademik çevreler henüz onlara fazla ilgi göstermedi. D. Bullmann, J. Klemm ve A. Pinna [33] tarafından yapılan bir çalışma ve W.C. Wei [34] uzman ve iş analizlerinden oluşmaktadır. Kararlı paralar üzerine yapılan çalışmaların azlığı, fenomenin tek bir tanımının olmamasına neden olmaktadır. T. Sameeh, "stable coin" teriminin herhangi bir kripto para birimini veya jetonunu ifade ettiğini belirtmektedir [35]. G. Calle ve D. Zalles ise blokzinciri tabanlı ödeme yapanlar olduklarına göre, ödeme yapısına kesinlikle atıfta bulunan bir tanım önermektedir. Yukarıda sunulan tanımların karşılaştırılması, belirli gözlemleri ima eder. İlk olarak, bir dizi tanım kripto para ve token kavramlarını kullanır. Böyle bir yaklaşım, çok kısa ve basit bir tanımlamaya yol açabilir (Blokzincir tarafından uygulanan gibi). Bununla birlikte, kripto para birimi kavramı da çeşitli şekillerde tanımlanabileceğinden, bu basitlik aldatıcı olabilir. Bunun da ötesinde, G. Samman ve A. Masanto tarafından yapılan tanım, token yerine madeni para olan kararlı paraların hesaba katılması gerekip gerekmediği konusunda bazı şüpheleri tetikliyor. Bu, daha geniş veya daha dar bağlamda kullanılabilen jeton kavramının kullanımından kaynaklanmaktadır (ikincisi madeni para kavramı hariç) [36].

Çoğu kararlı para, belirli bir referans para birimine veya bir para birimi sepetine karşı istikrarlı bir döviz kurunu korumaya çalışır. Bununla birlikte, kripto para

piyasasında altın paritesinin modern bir versiyonunu yaratarak değeri sabitleyen bazı çözümler var. Bu çözüm altında token, "gold tokenization" (altın simgeleştirme) olarak bilinen bir süreçte belirli bir miktarda altının (örneğin 1 gram) dijital bir temsili haline gelir. Kararlı para yaratıcılarının ve ayrıca altını temsil eden tokenların-istikrar kavramını nasıl algıladıklarına dair ilginç bir fikir, G. Samman ve A. Masanto tarafından hazırlanan şu raporda bulunabilir:

- Stability (istikrar), bir günden diğerine benzer bir mal ve hizmet sepeti satın alma olasılığı anlamına gelir.
- İstikrar, sabit paranın sabitlendiği karşılık gelen varlık miktarı için kolayca itfa edilebilir olmak anlamına gelir.
- İstikrar, fiyat çıktıları açısından kolayca tahmin edilebilir olmak anlamına gelir.
- İstikrar, yerel enflasyon oranında büyüme anlamına gelir. Bu da değeri reel olarak korumak anlamına gelir.
- İstikrar, diğer para birimlerinin oynaklığına karşı görecelidir. Daha da önemlisi, istikrara ulaşmak için operasyonel hedeflerin ve mekanizmaların çeşitliliği, en azından kısmen, istikrarın çoklu tanımlarının bir sonucudur [36].

Karar, genellikle itibari para birimi olan ve uçucu olmayan değerlere sabitlenen dijital para birimleridir. İtibari para biriminin aksine sabit paralar tamamen şeffaftır, her transfer halka açık bir blok zincirine kaydedilir. Bu bağlamda, şeffaf para akışlarının finansal piyasalar üzerindeki yıkıcı etkisine ilişkin değerli bir vaka çalışması olarak hizmet edebilir. Kararlı para transferlerinin etrafındaki saatlerde oldukça önemli pozitif anormal işlem hacmi ve önemli anormal getiriler buluyoruz. Her transferin göndericisi ve alıcısı (1) bilinmeyen, (2) kripto para birimi değişimi veya (3) sabit para hazinesi olarak kategorize edilir. İşlem hacmi ve getiriler üzerindeki etkiler, sonuçta ortaya çıkan dokuz alt örnek arasında farklılık gösterir; bu, piyasa katılımcılarının her bir gönderici-alıcı kombinasyonu için farklı transfer motifleri ve değişen derecelerde bilgi asimetrisi varsaydığını gösterir. Bulgular, kripto para piyasaları ve sabit para kullanımı arasındaki geri bildirim etkilerini göstermektedir ve şeffaf para akışlarının piyasa verimliliğini artırabileceğini öne sürmektedir [37].



Şekil 10. Kararlı para pazar payları grafiği [37].

Şekil 10, araştırma döneminde, sekiz kararlı paranın pazar paylarını göstermektedir. Yeterli rezervleri gösteren geçerli kanıtı sağlayamasa da Tether'in istikrarlı para piyasasına hâkim olduğu ve 2019 boyunca pazar paylarını artırdığı sonucuna varılmaktadır. Öte yandan, kripto para birimi olan Ethereum tarafından desteklenen tek para olan SAI'nin piyasa değeri küçük kalmıştır. Bu arada GUSD, rezervlerinin düzenli olarak denetlenmesine rağmen 2019'da aşırı bir düşüş yaşamıştır. USD'ye endeksli olmayan kararlı paraların (EURS ve DGX) pazar payları önemsiz ve aynı zamanda örnekleme dönemi boyunca azalan bir trend sergilemektedir [37].

2.1.4. Binance Coin (BNB)

Binance Coin ve Bitcoin'in günümüzde piyasa değeri ve işlem hacmi çok büyüktür. Binance Coin sıralamada üçüncü sırada yer alırken; Bitcoin ise birinci sırada yer almaktadır. Bitcoin piyasasındaki verimsizlik, Bitcoin oynaklığının Binance madeni para oynaklığına etkisi ile gösterilir ve şok emilimi için yeterli zaman sağlanarak tam oynaklık etkisi kontrol edilebilir. Özellikle bu kripto-serisi, önemli kârlar için yeterli alan sağlar ve aktif olarak işlem gören bu kripto para biriminde gelecekteki fiyatları tahmin etmek için tüccarların ve yatırımcıların zihninde bir ilgi yaratmaktadır [38].

Şekil 11. Binance Coin orijinal logo görseli [39].

Ticaret ile uğraşan bireyler ve yatırımcılar bu türev piyasasında kârlı bir strateji oluşturabilirler. Kripto para piyasasında kârlı bir strateji oluşturmak, yüksek düzeyde işlem görmeyen herhangi bir kripto para birimini portföylerine dahil etmekten çekinen tüccarlar ve yatırımcılar için zorunludur. Bu nedenle, Bitcoin'e sahip olmak büyük getiriler sağlayarak fayda sağlayabilir ancak Bitcoin (BTC) ve Binance madeni para (BNB) pazarındaki yavaş talep sırasında bir riskten korunma fonu olarak faydalı olmayabilir. Ek olarak Binance borsası, Binance kripto parasını (BNB) çalıştırır ve ticaret sembolü BNB'dir. Binance coin (BNB) ayrıca Ethereum, Litecoin, Bitcoin vb. gibi diğer kripto para birimleri ile takas edilebilir. Binance Coin ilk olarak Temmuz 2017'de üretilmiş ve ERC-20 jetonu ile Ethereum blok zincirinde çalışmıştır [38].

BNB'nin birden fazla kullanım durumu vardır ancak Binance Exchange ekosisteminde, kullanıcıların alım satım ücretlerini öderken indirim almalarını sağlayan bir yardımcı program jetonu olarak kullanılır. Ayrıca, ücret yapısı işlem hacmine (30 gün) ve hesabın katman düzeyine göre de değişmektedir. Ayrıca Binance Charity Foundation (BCF) projesi aracılığıyla hayır kurumlarına etkili bağışlar da yapılabilmektedir. Yakın bir gelecekte BNB, Binance Chain ve Binance Merkezi Olmayan Borsa'da (DEX) kullanılacaktır [40].

2.2. Merkeziyetsiz Finans (Decentralızedfınance, Defı)

Merkezi olmayan finans (DeFi); kripto para birimleri tarafından kullanılanlara benzer, güvenli dağıtılmış defterlere dayanan, gelişmekte olan bir finansal teknolojidir. Sistem; bankaların ve kurumların para, finansal ürünler ve finansal hizmetler üzerindeki kontrolünü ortadan kaldırır [41]. Birçok tüketici için DeFi'nin en önemli özelliklerinden bazıları şunlardır:

- Bankaların ve diğer finans şirketlerinin hizmetlerini kullanmak için talep ettikleri ücretleri ortadan kaldırır.
- Sahip olunan paraların bankada tutulması yerine güvenli bir dijital cüzdanda saklama durumuna sahip kıldırır.
- İnternet bağlantısı olan herkes onaya gereksinim duymadan kullanabilir.
- Saniyeler ve dakikalar içinde para transferi yapılabilir [42].

Merkezi olmayan finans (DeFi), son zamanlarda çok fazla ilgi gören blok zinciri tabanlı bir finansal altyapıdır. Terim genellikle Ethereum blok zinciri gibi halka açık akıllı sözleşme platformları üzerine inşa edilmiş açık, izinsiz ve yüksek düzeyde birlikte çalışabilir bir protokol yığınını ifade eder [32]. Mevcut finansal hizmetleri daha açık ve şeffaf bir şekilde çoğaltır. Özellikle DeFi, aracılara ve merkezi kurumlara güvenmiyor. Bunun yerine, açık protokollere ve merkezi olmayan uygulamalara (DApps) dayanır. Anlaşmalar kodla uygulanır, işlemler güvenli ve doğrulanabilir bir şekilde yürütülür ve yasal durum değişiklikleri halka açık bir blok zincirinde devam eder. Böylece bu mimari; benzeri görülmemiş şeffaflık, eşit erişim hakları ve koruyuculara, merkezi takas odalarına veya emanet hizmetlerine çok az ihtiyaç duyulan, değişmez ve son derece birlikte çalışabilir bir finansal sistem yaratabilir çünkü bu rollerin çoğu "akıllı sözleşmeler" tarafından üstlenilebilir [42].

DeFi, merkeziyetsiz (decentralized) ve finans (finance) kelimelerinden birleşiminden oluşan hiçbir otoriteye veyahut merkeze bağlı olmayan finansal yapılar için kullanılan genel isimdir. Örneğin Bitcoin ve Ethereum gibi merkeziyetsiz ve otoritesiz sistemler DeFi'dir. Merkeziyetsiz finans (Decentralized finance – DeFi) kavramı en temel anlatımla, belirli bir otoritenin sunduğu somut bir güvenceye bağlı olmaksızın şekillenen bir finans sistemi olarak tanımlanabilir [43]. Merkeziyetsiz finans, son zamanlarda ortaya çıkmış olup klasik finans dünyasını yeniden şekillendirmeyi ve merkezi finansın sahip olduğu dezavantajları gidermeyi hedeflemektedir.

Finansal gereçler para alma ve gönderme işlemlerinden daha gelişmiş finansal işlevlere sahiptir. Bunlar arasında merkeziyetsiz borsa, kredi alma-verme, pazaryeri, alışveriş, sigorta vb. işlevler vardır. Bu işlevlere imkân sağlayanlar için borsalarda tokenları bulunan Uniswap (UNI), Bancor (BNT), Compound (COMP), Maker (MKR), Aave (LEND), Synthetix Network Token (SNX), 0x(ZRX) ve Kyber Network (KNC) sayılabilir. Merkeziyetsiz yapılar ilgi çekici olsa da kötü amaçlar içinde kullanılabilir. DeFi yapısı gereği bozulmaz ve değiştirilemezdir. Bu özellikleri ile güven vericidir.

DeFi sistemlerinde yapılabilecek işlemler belirlidir ve kurallar çerçevesinde gerçekleşir. Bu sistemlerde işlemler nettir ve neden sonuç ilişkisi mevcuttur. DeFi sistemlerde Konsensüs protokolleri, Merkezsiz uygulamalar ve Akıllı sözleşmeler önemli bir yere sahiptir. Merkeziyetsiz finans alanı son yıllarda oldukça hızlı bir şekilde gelişmekte olup klasik finans araçlarına alternatif teşkil etme iddiası ile finans alanında oldukça köklü bir değişimin eşiğinde olduğumuz kanaatini uyandırmaktadır [44].

2.2.1. DeFi Sistemlerinin Avantajları ve Kullanım Alanları

2008 yılında yaşanan ekonomik kriz sebebiyle özel bankalara ve devlet bankalarına karşı itimat azalmıştır. Hükümetlerin istedikleri zaman para basabilmeleri, paranın değerini değiştirebilmeleri ve insanların buna müdahale edememeleri merkeziyetsiz sistemlere ilgiyi artırmıştır. DeFi sistemler alanında ortaya çıkan en önemli varlık ise Bitcoin olmuştur. Merkeziyetsiz olan bu sistem, kullanıcılara hem kullanıcı hem de yönetici olma imkânı sağlamaktadır.

Blokzincir teknolojisi, merkezi otoriteye gerek duymadığından finans alanında özgür olunmaya başlandı. Kullanıcılar aracıya ihtiyaç duymadan birbirleri ile etkileşime geçebilir ve güvenilir, gizli anlaşmalar ile daha az maliyetli daha hızlı işlemlerini gerçekleştirmektedir. Merkezi olmayan finans (DeFi), akıllı sözleşmeye dayalı blok zincirlerin üzerine inşa edilen merkezileştirilmiş olanın aksine alternatif bir finansal alt yapıyı ifade eder [42]. DeFi geleneksel finans sistemlerine oranla daha iyi bir sistem sunmaktadır.

DeFi'nin geleneksel kullanım alanlarına göre avantajları şunlardır:

- Dünyanın her yerine çok ucuz, hızlı ve güvenli para transferi yapabilmek.

- Kurulan borçlanma sistemleri ile kullanıcılar hem borç alabiliyor hem de borç verebiliyorlar.
- Sahip olunan bir varlığı jetonlaştırabilme. Böylece o varlığa hem bir değer verilmektedir hem de transfer edilebilmesi sağlanmaktadır.
- Aracı kurumlar ortadan kaldırılmıştır ve dolayısıyla bankaya ödenen komisyonlar da ortadan kalkmıştır.
- Hisseleştirme gibi işlemlerde verilen faiz, bankaların mevduat faizlerine göre çok daha yüksek olabilmektedir [45].

2.2.2. DeFi Sistemlerinin Dezavantajları ve Kullanım Alanları

DeFi ile geleneksel finans kökten değiştirilecektir. Var olan bu değişimin henüz başlarında olmakla birlikte bu kadar yeni olması beraberinde eksikliklerinin de çok olduğu anlamına gelmektedir [45]. Günümüzde DeFi'nin eksik olabileceği yönleri:

- DeFi kullanan kişi sayısı çok azdır.
- Bütün yapının açık olması ve her işlemin veri olarak tutulması için yeterli altyapı bulunmamaktadır.

2.2.3. DeFi Piyasasında Kredi Verme ve Kredi Çekme

Hem kripto finans hem de geleneksel finans alanında kredi çekme ve borç verme, taraflardan birinin sunduğu sabit gelir akışı karşılığında diğerine itibari veya dijital para sunulmasıdır [46]. Yıllardır kullanılan "borç verme ve borçlanma" kavramları tüm dünyada sıkça kullanılan "Franksiyonel Bankacılık" yapısının temel kavramlarındandır. Sistem basittir:

- Borç verenler, belirli bir faiz karşılığında borçlulara fon sağlar. Geleneksel finans siteminde kullanılan bu tür anlaşmalar, finans kurumu veyahut P2P borç veren yapılar tarafından kolaylaştırılır.

Kripto para birimleri tarafından değerlendirildiğinde, Celsius ve BlockFi gibi merkezi yapıların dışında Aave ve Maker gibi merkeziyetsiz finans protokollerinde kullanılmaktadır [46]. Merkezi finans platformları (Centralized Finance, CeFi),

geleneksel bankalar gibi çalışır. Müşterinin yatırdığı varlıkların sorumluluğunu alır ve bu varlıklarla üçüncü şahıslara kredi imkânı sunar. CeFi kâğıt üzerinde iyi görünse de bilgisayar korsanlığı, iç ve dış saldırı ve hırsızlıklar gibi sorunlarla çok sık karşılaşmaktadır. Fakat DeFi tamamıyla merkeziyet bir biçimde kullanıcıların borç veren de alan da olmasını sağlar. Böylece kullanıcı fonlar üzerinde kontrol sağlayabilirler. Bu durum DeFi, Ethereum gibi açık Blokzincir ağları üzerinde çalışan akıllı sözleşme kullanılarak mümkün hale gelir. CeFi'nin aksine DeFi otoriteyi merkeze devretmek zorunda bırakmaz ve her zaman her yerden herkes tarafında kullanılabilir [47].

2.2.4. Merkeziyetsiz Pazar Yerleri

DeFi'nin en önemli uygulamalarından birisi de merkeziyetsiz borsalardır (DEX). Örneğin Uniswap, Pancake gibi platformlar kullanıcıların fonlarıyla aracılar(borsalar) olmadan dijital varlıklar alıp satabileceği bir ortam sunar. Alışveriş akıllı sözleşmeler sayesinde kullanıcı cüzdanları arasında olur. Merkeziyetsiz borsalar, geleneksel borsalara göre daha düşük işlem ücretlerine sahiptirler.

2.2.4.1. DEX'in Avantajları

- Gizlilik: Merkezi olmayan borsalar, kullanıcılarından KYC bilgileri gibi gereksinimlere ihtiyaç duymazlar.
- Seçenek Çeşitliliği: Uniswap gibi DEX'ler, her bireyin bir token çifti oluşturmasına izin verir ve işlemleri çok kolay ve hızlı gerçekleştirebilirsiniz. Banka ya da başka bir finansal kuruma ihtiyaç duymadan borç alabilirsiniz, borç verebilirsiniz ve ticaret yapabilirsiniz
- Düşük Risk: Belirteçleri, merkezi bir borsada değil de sahip olduğunuz özel anahtarların bulunduğu bir cüzdanda tutulduğundan dolayı güvenlidir [75].

2.2.4.2. DEX'in Dezavantajları

- Banka ve Kredi Kartlarınız Kullanılamaz: DEX'ler, sadece kripto paralar ile çalışır, DEX kullanmak için kripto para sahibi olmalısınız.

- Karmaşık bir Yapıya Sahiptirler: Uniswap ve diğer birçok DEX, Ethereum blok zincir üzerine geliştirilmiştir. Orada işlem gören bir token, Ethereum ağında olmalıdır. Yani bunun anlamı, Bitcoin ve diğer birçok Blokzincir üzerinde geliştirilmiş popüler olsa dahi bu kripto paraların Ethereum blok zincir üzerine inşa edilmiş DEX'te işlem göremez.
- Sorumluluk tamamen sizdedir: DEX kullanıcıları, kendi varlıklarından sorumludur [75].

2.2.4.3. Akıllı Kontratların DeFi'deki Rolleri

Akıllı kontratlar, kaynak kodlarında belirli olaylar meydana geldiğinde veya belirli girdiler yapıldığında önceden tanımlanmış eylemleri veya bir veri kaydındaki değişiklikleri gerçekleştirmelerini sağlayan değişmez kurallar içeren bilgisayar protokolleridir [75]. Akıllı kontrat kavramı, genellikle sözleşme kavramıyla karıştırılmaktadır. Akıllı kontrat kavramında kontrat terimi bulunuyorsa da hukuki anlamda sözleşme icra etmezler. Akıllı kontratlar yalnızca önceden uygulanmış bir sözleşmenin yerine getirilmesi konusunda bir icra aşamasıdır [76].

Akıllı sözleşmelerin hedefi, yazılım kodları kullanılarak sözleşmelerin işlenmesini otomatikleştirmektir. Merkeziyetsiz finansın mevcut yapısı, akıllı kontratların kullanılmasını zorunlu kılar. Akıllı kontratlar sayesinde DeFi güvenilirliğini sürdürmektedir. Akıllı kontratlarda geleneksel kontratların aksine bilgisayar kodları kullanılır. Akıllı kontratların şartları bilgisayar kodu ile yazıldığından bu kontratlarında bilgisayar kodu ile çözümlenir. Böylelikle şu anlık manuel gerçekleşen süreci güvenilir bir şekilde otomatikleştirmektedir [47]. Akıllı kontratlar daha hızlı, daha kolaylık sunmanın yanı sıra riskleri azaltır ve güvenilir bir ortam hazırlar. Ayrıca, akıllı kontratlarında kendisine özgü riskleri mevcuttur. Örneğin, bilgisayar kodunun hataları ve açıkları olabilir. Bu durumda gizli bilgiler risk altında demektir.

2.2.5. DeFi'nin Karşılaştığı Zorluklar

- Zayıf performans: Blok zincir, merkezi birimlerden daha yavaştır bu da kullanıldığı uygulamalarında yavaş olmasına sebep olur. DeFi uygulamalarının geliştiricileri bu durumu gözden kaçırmamalı ve ürünlerini bu duruma uygun optimize etmelidir.
- Yüksek kullanıcı hatası riski: DeFi sorumlulukları aracılardan alıp kullanıcılara verir.

- Kötü kullanıcı deneyimi: DeFi uygulamalarının küreselleşmesi için kullanıcıların geleneksel finans sistemlerini bırakıp DeFi'ye geçmesi gerekmektedir bunun için de kullanıcının DEFi'den maddi fayda sağlaması gerekmektedir.
- Dağınık ekosistem: Henüz yeni bir sistem olduğu için spesifik ihtiyaca yönelik uygulama bulmak çok zordur [47].

2.2.6. Merkeziyetsiz Uygulamalar

Merkeziyetsiz uygulama anlamını taşıyan DApp, P2P (eşler arası protokol) ve Blokzincir temellerine inşa edilebilir bir yapıdadır. Blokzincir tabanlı DApp uygulamaları kripto para işlemlerine imkân sağlar. Uygulamanın kullanıcıları kripto para kazanabilir, kripto para transferi yapabilir.

2.2.6.1. Web3

DARPA (The Defense Advanced Research Projects Agency- Savunma İleri Araştırma Projeler Ajansı) 1989'da Tim Bernes-Lee tarafınca internetin ilk sürümü olan Web 1.0'ı hayatımıza sokmuştur. 2004 tarihinde Web 1.0 yerini Web 2.0 teknolojilerine bırakmıştır. Web 2.0 ile yazılım dünyası çokça dinamik web siteleri üretmeye başlamıştır. Web 2.0 ile sosyal medya platformları popüler hale gelmiştir. Blokzincir'in hayatımızdaki yoğunluğu arttıkça yeni bir teknoloji gereksinimleri artmıştır. 2014 yılında aynı zamanda Ethereum'un da kurucu ortağı olan Gavin Wood tarafından Web 3.0 'ın temelleri Blokzincir ve yapay zeka tabanlı atılmıştır.

Web3 şeffaf yapılı, merkeziyetsiz internet ve Blokzincir kavramlarına dayalıdır. Blokzincir, dApp(merkeziyetsiz uygulama), NFT, Kripto para gibi kavramların oluşmasında Web3 büyük rol oynuyor. Merkeziyetsizlik dijital ekelciliği en aza indirmeyi hedefler ve bu konuda Web3 sayesinde oldukça başarılıdır. Avantajları gibi dezavantajları da vardır tabii ki; merkeziyetsiz sitemlerde zorbalık, nefret söylemi, siber suçlar gibi yasadışı olayların tespiti oldukça zordur [48].

2.2.6.2. MetaMask

Kripto dünyasında işlem yapabilmesi için cüzdan sahibi olmak gerekir. Kripto paralarımız da geleneksel paralar gibi cüzdanlarda barındırılır. Bu cüzdanlar kişiye özel

anahtarlar barındıran dijital cüzdanlardır. Bu cüzdanları oluşturmak ücretsizdir. Cüzdanlar arasında uyumluluk çok önemlidir aksi takdirde işlem yapılamaz veyahut kripto paralar kaybolabilir. Bu gibi durumlarda yardımcı uygulamalar kullanılır.

Örneğin Meta Mask; Web3 destekli en çok kullanılan, tarayıcı entegrasyonlu, kolay arayüzlü, güvenilir kripto cüzdanıdır.2016 yılında ConsenSys Software Inc. tarafından ETH işlemlerini basitçe gerçekleştirebilmek için kullanıcıyı Ethereum Blokzincir'e bağlayan cüzdan olarak ortaya çıkmıştır. Proje tahmin edilenden çok fazla büyüyerek en büyük Web3 şirketlerinden olmuştur.

Meta Mask, tarayıcı eklentisi veyahut mobil uygulama olarak kullanılabilen

ETH cüzdanlarına erişime imkân sağlayan bir kripto cüzdanıdır [49][50]. Meta Mask oldukça yaygın kullanıma sahiptir. Financi Times'a göre Nisan 2012 itibarıyla aylık yaklaşık 10 milyon aktif kullanıcıya sahiptir [51].

2016 yılında yalnızca tarayıcı eklentisi olarak hayatımıza giren Meta Mask yaygın kullanımdan sonra 2019 yılında IOS ve Android uygulamalarını kullanıcıların kullanımına sunmuştur. 2020 yılında ise DEX toplama hizmetli Meta Mask Swaps ortaya çıktı [52].

2.3. Kripto Paralarda Boğa ve Ayı Piyasaları

Yatırımcılar, kripto paraların veyahut farklı bir varlığın finansal eğilimlerini belirtmek için ayı piyasası veya boğa piyasası terimlerini kullanırlar. Bu terimler varlığın geleceği hakkında tahmin yürütmelerine ve bu tahminlere göre işlem yapmalarına imkân sağlar.

2.3.1. Boğa Piyasaları

Boğa piyasası, kökeni borsadan gelen fakat diğer finans piyasalarında da kullanılan bir terimdir. Boğa piyasası, kripto paraların fiyatlarının hızlı ve sürekli yukarı artış gösterdiği piyasalardır. Boğa piyasasında yatırımcılar satın alma ve elinde tutma eğilimindedir. Sürekli artan değerli kripto paralarını satmak istemezler. Bu sebeple talep fazla, arz azdır. Aslında boğa piyasasında fiyatlar yalnızca artmaz. Uzun vadede pozitif bir artış gözlenir fakat kısa anlık fırsat düşüşleri yaşanabilir. Boğa piyasası, kripto

paraların fiyatlarının %20'lik iki düşüşün ardından %20 artmasıdır. Boğa piyasasını önceden tahmin etmek oldukça zordur genellikle gerçekleştikten sonra fark edilir. Boğa piyasaları aylarca hatta yıllarca sürme eğilimindedir. Kripto para borsalarındaki boğa piyasaları aynı geleneksel borsalardaki gibidir. Fakat fiyatlardaki fiyat değişiklik yüzdeleri farklıdır [53].

Boğa Piyasasının Özellikleri

Boğa piyasasının özellikleri aşağıdaki gibi sıralanabilir;

- Bir süre sürekli fiyatlarda artış gözlenir.
- Zayıf arz karşısında güçlü talep vardır.
- Yatırımcı güveninde artış gözlenir.
- Projelerin aşırı fiyatlanması söz konusudur.
- Kripto para birimlerinin popülerleşmesi ve sosyal medya ve ana medyada adından sıkça söz ettirir.
- Projeler hakkındaki iyi haberler, fiyatlarda sert artışa; kötü haberler ise hafif bir azalışa sebep olur.

Yatırımcıların Kar Etmesini Sağladığı Düşünülen Stratejiler

Yatırımcıların kar etmesini sağladığı düşünülen stratejiler aşağıdaki gibi sıralanabilir;

- **Satın Al ve Beklet:** Boğa piyasalarından faydalanmak için yatırımcıların kripto paraları erkenden alıp yükselişi bekleyip zirvede satış yapmaları gerekmektedir.
- **Artan Al ve Tut:** Satın al ve beklete benzer fakat daha fazla risklidir.Yatırımcı kripto paranın artmaya devam ettiği süreçte alır ve daha da artmasını bekler.
- **Geri İzleme Eklemeleri:** Boğa piyasalarında sürekli artış gözlenmez. Bazen anlık geri çekilmeler olur fiyatlar düşer. Yatırımcılar bu düşüşlerde satın alma yapabilir.
- **Tam Swing Ticareti:** Yatırımcılar, daha büyük boğa piyasasında değişimler oldukça maksimum kâr elde etmek için açığa satış ve diğer teknikler ile aktif roller üstlenirler.

Boğa Piyasasının Örnekleri

Bazı örnekler aşağıda verilmiştir.

- 1982'de başlayıp 2000'de dotcom çöküşüyle sona eren Dow Jones Endüstriyel Ortalaması (Dow Jones Industrial Avarage -DJIA) Amerikan tarihin en büyük boğa piyasası yıllık ortalama %15 kar elde ettirmiştir [54].
- 1995'de başlayıp 2000 yıllarına kadar süren Teknoloji ağırlıklı borsalardan NASDAQ'ın piyasa değerini 3 kat artırarak 755'ten 2400 'lü değerlere çıkmıştır. Sonrasında uzun bir ayı piyasası olmuştur [55][56].
- 2003'de başlayıp 2007'de biten S&P 500 boğa piyasası örneklerindendir [57][58].
- 2017'de başlayıp tarihsel olarak, kripto para birimi bir boğa piyasasında büyük kazançlar sağladı. 2017 yılına 985 dolar olarak başlayan BTC Japonya'nın Bitcoin ile ödeme yöntemlerini kabul etmesiyle 2018 yılında Bitcoin 20000 dolar seviyelerine fırladı ve toplam kripto piyasası değeri 830 milyar USD'ye ulaştı [53].
- 2020 yılının sonlarında 29551 dolar seviyelerinde olan BTC 2021 Nisan ayında 61000 dolara kadar yükselmiştir [59].

2.3.2.Ayı Piyasaları

Ayı piyasası, uzun süreli ve sürekli fiyat düşüşlerinin yaşandığı piyasalardır. Piyasada karamsarlık hakimdir ve olumsuz fiyatlar vardır. Son dönemdeki yüksek fiyatlardan %20 veyahut daha fazla düşüşlerin olduğu piyasalardır. Ayı piyasalarında durgunluk gibi ekonomik gerileme dönemleri de yaşanabilir. Ayı piyasaları uzun vadeli veyahut döngüsel olabilir. İlk ayı piyasası kısa süreli (birkaç hafta veya ay) sonraki ayı piyasaları ise uzun süreli (birkaç yıl hatta onlarca yıl) sürebilir. Ayı piyasalarında acemi yatırımcılar için işlem yapmak oldukça zordur. Çünkü ayı piyasasının ne zaman sona ereceğini tahin etmek oldukça zordur. Geri sıçramalar yatırımcı psikolojisi, ekonomik büyüme, dünya olayları ve haberler gibi birçok etkene duyarlıdır. Ayı piyasaları öngörülemeyen yavaş bir süreçtir.

Ayı piyasaları, tecrübeli yatırımcılar için birçok fırsatı da beraberinde getirir. Uzun vadeli yatırımlarda ayı piyasasındaki düşüşlerden satın alarak iyi bir kar elde edilebilir. Kısa vadede ise anlık al sat yapılabilir.

Ayı Piyasasının Özellikleri

Ayı piyasasının özellikleri aşağıdaki gibi sıralanabilir;

- Bir süre sürekli fiyatlarda düşüş gözlenir.
- Güçlü arz karşısında zayıf talep vardır.
- Yatırımcı güveninde azalış gözlenir.
- Projelerin değerlerinde aşırı derecede düşüş söz konusudur.
- Projeler hakkındaki kötü haberler fiyat sert düşüşlere, iyi haberler ise hafif bir artışa sebep olur.

Ayı Piyasasının Örnekleri

1900'den başlayıp 2018 yılları arasında her 3,5 yılda bir toplam 33 ayı piyasası yaşanmıştır. Bazı örnekler aşağıda verilmiştir.

- 1987'de Wall Street'teki Kara Pazartesi olayında üç ay süren ayı piyasasında %29,6 düşüş yaşanmıştır.
- 2007 Ekim'de başlayıp 2009 Mart ayına kadar süren küresel mali krizde DJIA (Dow Jones Industrial Avarage - Dow Jones Endüstriyel Ortlaması) %54 düşüş yaşamıştır.
- 2007'de başlayıp 2009'da sona eren mali krizden S&P 500 de etkilenmiş ve %50 düşüş yaşamıştır.
- 2013 ortalarında, 2011 yılında zirveyi görmüş olan altın 1900 dolar ons seviyelerinden 1500 dolar ons seviyelerine düşerek %30 düşüş yaşamıştır [60].
- 2014'de Bitcoin,880 dolar seviyelerinden 302 dolar seviyelerine düşmüştür.
- 2014 yılına 880 dolar ile başlayan kripto para birimi BTC, 2014 yılını 302 dolar seviyesinde kapattı [59].
- 2018 yılında bir önceki yıl 14000 dolar seviyesinde olan Bitcoin, 7232 dolara kadar düşmüştür [59].

- 2020’de küresel korona virüs salgınından sonra küresel bir ayı piyasasına girilmiştir [61].
- 2022’de Bitcoin, 2021 yılında 61000 dolarlardan 21000 dolar seviyelerine sert bir düşüş yaşamıştır [62].

2.3.3. Boğa Piyasası ile Ayı Piyasası Farkları

Boğa ile Ayı piyasaları mantık olarak birbirlerinin tam tersleridirler. Fiyat değer grafiklerinde eğim yükseliyor ise boğa, düşüyor ise ayı piyasasıdır.

Boğa ve ayı piyasaları genel olarak döngüsel 4 aşamadan oluşur;

1. Genişleme
2. Zirve
3. Daralma
4. Dip

Boğa piyasası ekonomik genişlemeyle başlar. Ayı piyasası ise ekonomik daralmadan önce başlar. Örneğin; kripto para piyasalarında yatırımcı ayı sezonunun dibinde boğa piyasası yatırımcısı konumundadır. Boğa piyasasında fiyatlar hızlı bir şekilde artacak ama bu artış kısa sürecektir. Yatırımcılar kârını alıp çıkmaya başlayınca boğa sezonu yerini ayı sezonuna bırakacaktır.

1. Arz ve Talep

Boğa piyasasında, talep yüksek arz ise düşüktür. Yatırımcılar kripto paraları satın almak için rekabet ederken kripto paraların fiyatlarını artırırlar. Ayı piyasasında ise durum tam tersidir. Talep düşük arz çok yüksektir. Yatırımcılar, kripto paranın değeri daha da düşmeden elinden çıkarmak isterler ve bu durum fiyatların dibe vurmasına sebep olur.

2. Ekonomi Üzerindeki Etkisi

Boğa piyasasında, ticaret yüksek fiyatlarla ilerler ve kârlar yüksektir bu sebeple boğa piyasalarında ekonomi güçlüdür. Öte yandan, ayı piyasası ise yatırımcılar hedefledikleri gelirlere ulaşamadığı için ticaret yapmazlar ve kârlar düşer ve ekonomi zayıflar.

3. Likidite

Boğa piyasasında, yatırımcılar istikrarlı, hızlı getirilere yüksek güven duyarlar ve bu sebeple işlem maliyetlerinde düşüklük mevcuttur ve likidite yüksektir. Fakat ayı piyasasında, hızlı düşüşler güven eksikliğine yol açar ve likidite düşüktür.

2.4. Kripto Paralarda Analizler

Kripto paralar doğası gereği oldukça değişken fiyatlara sahiptir. Yatırımcılar bu değişken fiyatlarda alış-satış yaparak yüksek karlar elde edebilir. İyi bir strateji belirlemek için kripto paraların alış – satış derinliklerle dolu dünyasını anlamak, temel ve teknik analizlerde beceriler geliştirmek oldukça önemlidir.

2.4.1. Teknik Analiz

Kripto paralarda Teknik Analiz (TA) yaparken geleneksel finans piyasalarındaki temel analiz yöntemlerinden yararlanılabilir. Geleneksel finans piyasalarından olan Forex'de alım satım yaparken kullanılan Bollinger Bantları, MACD ve RSI gibi araçlar kripto paraların alım- satım işlemlerinde de kullanılır. Ancak tam tersi bir durum denenmiş fakat başarılı olunamamıştır. Kripto para piyasalarında kullanılan araçlar geleneksel piyasalarda başarısız olmuştur [63].

2.4.1.1. Teknik Analizde Popüler Göstergeler

MACD (Hareketli Ortalama Yakınsaması / Iraksaması) Göstergesi

1970 yılında Gerald Appel tarafından geliştirilen MACD, traderlar(alım satım yapan yatırımcılar) tarafından kullanılan osilatör tipi teknik analiz aracıdır. MACD, trendi kripto paraların veyahut farklı bir ticari arlığın momentumunu yani hareketli ortalamalarını kullanarak takip eden araçtır. Geçmiş fiyatlar ve verilere dayanarak kripto paraların fiyatlarını tahmin etmede kullanılır.

MACD ikiye ayrılır;

- **SMA(Basit Hareketli Ortalamalar):** bütün girdi verilerine eşit ağırlık verilir.
- **EMA(Üstel Hareketli Ortalamalar):** sonuncu verilere yani en yeni fiyatlara ağırlık verilir.

MACD 3 elementten oluşur:

1. **MACD hattı**: Aşağı ya da yukarı momentumun belirlenmesinde kullanılır. İki EMA çıkarılarak hesaplanır.
2. **Sinyal hattı:** Sinyal hattı ile MACD hattının kombine analiziyle ortaya çıkan ihtimali ters yönde ivme veyahut giriş çıkış noktalarının belirlenmesinde kullanılır.
3. **Histogram:** Sinyal ve MACD hattının yakınsama ve uzaklaşmasının grafiksel gösterim şeklidir. İki satır arasındaki farklardan hesaplanır [64].

RSI (Göreceli Güç Endeksi) Göstergesi

1978'de J.Welles Wilder tarafından bir hissenin belirli bir sürede gösterdiği ivmeyi inceleyerek matematiksel formüllere döktüğü osilatör araçtır. RSI 14 günlük periyotlarla değişimi ölçer. Eğer ivme düşerse yatırımcıların hisseye ilgisinin azaldığını; eğer ivme artarsa yatırımcıların hisseye ilgisinin arttığını gösterir.

RSI 0-30 arasında ise fiyatın düşeceği, 70-100 arasında ise fiyatının artacağı tahmin edilmektedir [65].

BB (Bollinger Bantları) Göstergesi

1980'de John Bollinger tarafından piyasadaki fiyat değişimlerine göre aşırı alım veya aşırı satım gerekip gerekmediğini gösteren osilatör araçtır. Fiyatlardaki dalgalanmaları alt bant, orta bant (hareketli ortalama bandı) kullanılarak gösterilir.

Bollinger Bantları göstergesi kullanılan bant formülleri aşağıdaki gibidir:

- Alt bant: 20 günlük SMA - (20 günlük standart sapma x2)
- Orta çizgi: 20 günlük basit hareketli ortalama (SMA)
- Üst bant: 20 günlük SMA + (20 günlük standart sapma x2)

Fiyat arttıkça yanlardaki bantlar genişler (orta banttan uzaklaşır), azaldıkça yandaki bantlar daralır (orta banda yaklaşır) [66].

Teknik analiz varlıkların geçmiş fiyat performanslarına dayanarak tahminlerde bulunur. Bu tahminler için mum grafik düzenleri belirlenir ve temel göstergeler incelenir [63].

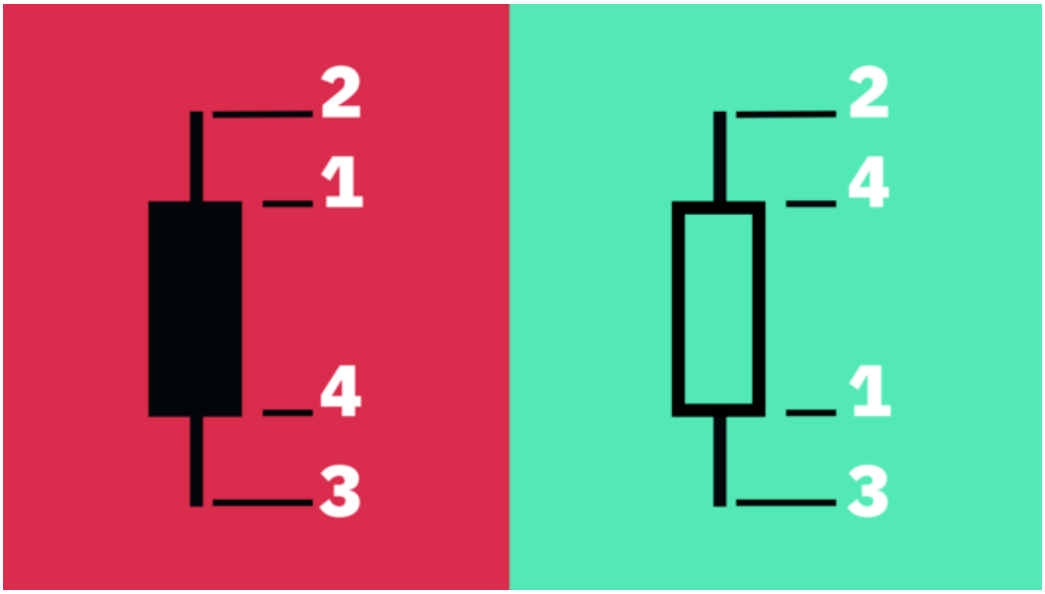
2.4.1.2. Mum Grafik

Mum grafik, bir kripto para veya varlığın belirli bir zaman aralığındaki fiyat hareketlerini temsil eden mumlardan oluşan grafiksel gösterimidir. Mumların zaman aralığı değişkenlik gösterir.

Mumları aşağıdaki fiyat noktaları- OHLC değerleri oluşturmaktadır:

1. Açılış(Opening): Varlığın belirli zaman aralığındaki ilk fiyatıdır.
2. En düşük(Lowest): Varlığın belirli zaman aralığındaki en düşük fiyattır.
3. En yüksek(Highest): Varlığın belirli zaman aralığındaki en yüksek fiyattır.
4. Kapanış(Closing): Varlığın belirli zaman aralığındaki son fiyatıdır.[67]

Açılış ve kapanış arasındaki bölgeye gövde, gövde ile en düşük ya da en yüksek değerler arasındaki bölgeye ise kuyruk veyahut gölge, en düşük ve en yüksek noktalar arasındaki bölgeye ise mum aralığı adı verilir.



Şekil 12. Mum fiyat noktaları- OHLC değerleri [67].

Grafiklerde genel olarak 2 renk kullanılır. Gövde yeşil ise fiyat artıyor, kırmızı ise fiyat düşüyor demektir. Gövde ne kadar uzunsa o kadar fiyat farkı fazla demektir ve alım veya satım baskısı da bir o kadar yoğundur. Eğer kuyruklar kısa ise açılış ve kapanış fiyatları birbirine yakın demektir.

2.4.1.3. Boğa Dönüş Formasyonları

Çekiç

Piyasanın dip seviyelere indikten sonra negatif değişim yaşayarak değer kazanıp potansiyel büyümeyi öngörmeye yarayan en popüler mum formasyonlarındandır [68].

Şekil 13. Çekiç(hammer) formasyonu [69].

Ters Çekiç

Piyasanın düşüş eğilimindeyken yükselişe geçtiği formasyondur. Çekiç formasyonun baş aşağı olduğu halidir [70]. Ters çekiç fiyatın aşağıya hareketini bitirip fiyatın açılış fiyatına yaklaşacağı ön görülür [69].

Şekil 14. Ters çekiç(inverted hammer) formasyonu [69].

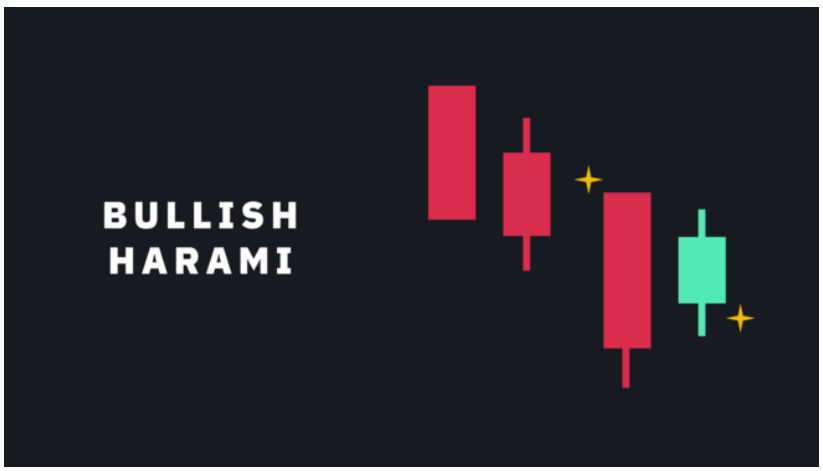
Üç Beyaz Asker

Üç beyaz asker**,** bir yükseliş trendinin başladığını belirten bir mum formasyonudur.

Şekil 15. Üç beyaz asker (three white soldiers) formasyonu [69].

Harami Boğa

Harami boğa, uzun kırmızı mumlar sonunda kısa yeşil mumdan oluşur. Yeşil mumun boyu öncesindeki yeşil mumun gövde aralığı içinde olur. Satış ivmesinin yavaşladığını hatta sona yaklaşmış olabileceğini gösterir.



Şekil 16. Harami boğa (bullish harami) formasyonu [69].

2.4.1.4. Ayı Dönüş Formasyonları

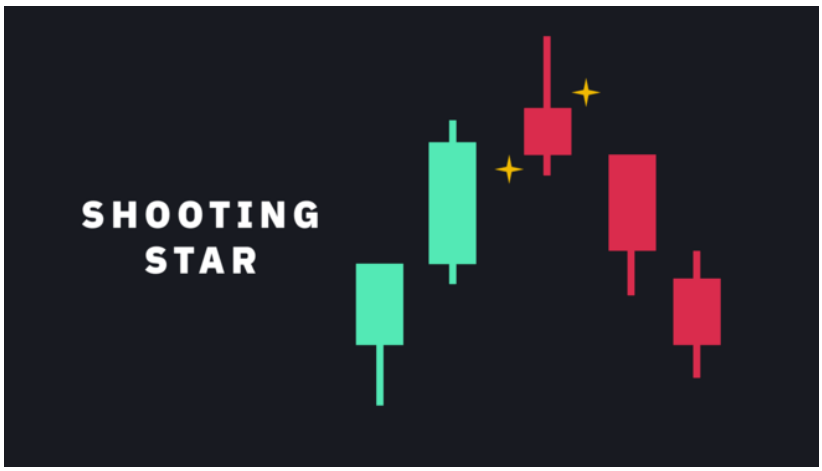
Asılı Adam

Asılı adam, boğa piyasasındaki çekicinin ayı piyasasındaki dengidir. Piyasanın yüksek seviyelere çıktıktan sonra negatif değişim yaşayarak değer kaybedip potansiyel küçülmeyi öngörmeye yarar.

Şekil 17. Asılı adam (hanging man) formasyonu [69].

Kayan Yıldız

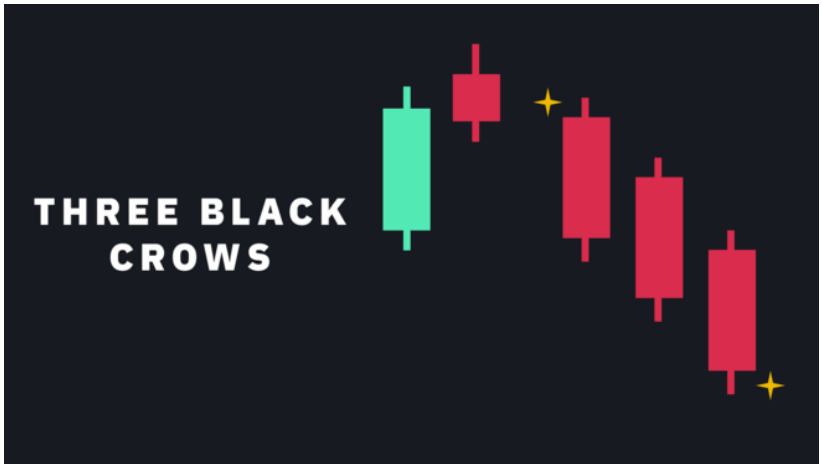
Kayan yıldızın şekli ters çekice benzerdir fakat bu formasyon yukarı trendin sonunda ortaya çıkar. Piyasanın yükseliş eğilimindeyken düşüşe geçtiği formasyondur. Kayan yıldız fiyatın yukarı hareketini bitirip fiyatın açılış fiyatına yaklaşacağı ön görülür.



Şekil 18. Kayan yıldız (shooting star) formasyonu [69].

Üç Siyah Karga

Üç beyaz askerin ayı piyasasındaki dengidir. Bir düşüş trendinin başladığını belirten bir mum formasyonudur.



Şekil 19. Üç siyah karga (three black crows) formasyonu [69].

Harami Ayı

Harami ayı, uzun yeşil mumlar sonunda kısa kırmızı mumdan oluşur. Kırmızı mumun boyu öncesindeki kırmızı mumun gövde aralığı içinde olur. Alış ivmesinin yavaşladığını hatta sona yaklaşmış olabileceğini gösterir.

Şekil 20. Harami ayı (bearish harami) formasyonu [69].

Kara Bulut Örtüsü

Kara bulut örtüsü kırmızı mumdan ve mumun açılış noktası kendisinden önceki yeşil mumun kapanışından yukarıdadır. Kapanışını ise önceki mumun orta noktasından aşağıda yapar.

Şekil 21. Kara bulut örtüsü (dark cloud cover) formasyonu [69].

2.4.1.5. Devamlılık Formasyonları

Yükselen Üç Metot

Yükseliş trendinde ortaya çıkar ve kısa kısa üç kırmızı mumdan sonra yukarı trendde devam eder. Sonrasında uzun gövdeli yeşil mumla devam edip boğalara geçtiğini belli eder.

Şekil 22. Yükselen üç metot (rising three methods) formasyonu [69].

Düşen Üç Metot

Yükselen üç metot formasyonunun tam tersidir. Düşüş trendinde ortaya çıkar ve kısa kısa üç yeşil mumdan sonra aşağı trendde devam eder. Sonrasında uzun gövdeli kırmızı mumla devam edip ayılara geçtiğini belli eder.

Şekil 23. Düşen üç metot (falling three methods) formasyonu [69].

Doji

Açılışa kapanış fiyatlarının aynı veyahut çok yakın olma durumlarına Doji oluşur. Fiyatlar açılış ve kapanış arasında değişkenlik gösterebilir. Ancak yine de alış satış işlemlerinde yatırımcılar kararsız kalırlar.

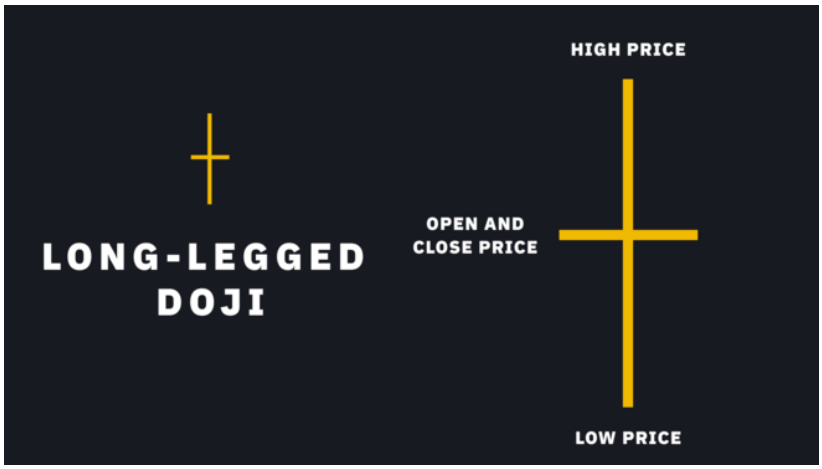
1. Mezartaşı Doji

Mezar taşı dojisi, açılış, en düşük ve kapanış fiyatlarının birbirine yakın olduğu uzun gölge şeklindeki ters şamdan formasyondur. Yükselişin ardından ayının başlayacağının habercisidir [71].

Şekil 24. Mezar taşı doji (gravestone doji) formasyonu [69].

2. Uzun Bacaklı Doji

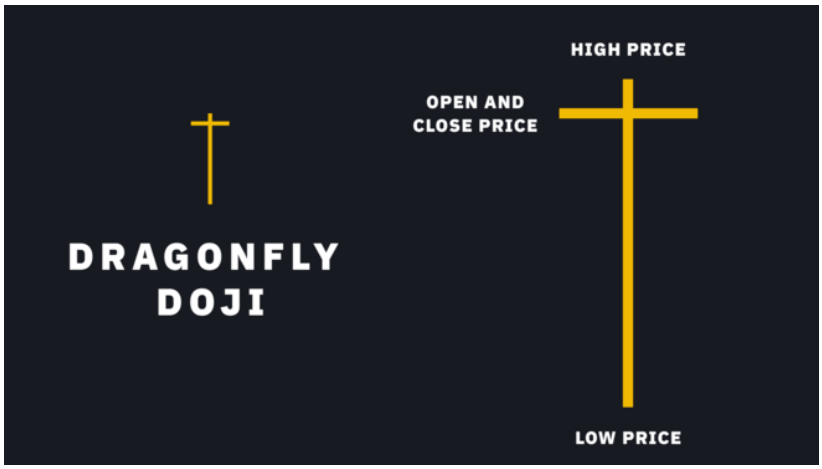
Uzun bacaklı doji, hemen hemen aynı açılış ve kapanış fiyatları olan, uzun alt ve üst gölgelerden oluşan ve kısa gövdeye sahip bir formasyondur. Yatırımcılar kararsızdır, güçlü yükselişin veyahut düşüşün ardından ortaya çıkar [72].



Şekil 25. Uzun bacaklı doji (long-legged doji) formasyonu [69].

3. Yusufcuk Dojisi

Yusufçuk dojisi, mezar taşı dojisinin tersidir. Açılış, en yüksek ve kapanış fiyatlarının birbirine yakın olduğu uzun gölge şeklindeki şamdan formasyondur. Düşüşlerin ardından boğanın başlayacağının habercisidir [73].



Şekil 26. Yusufcuk doji (dragonfly doji) formasyonu [69].

2.4.2. Temel Analiz

Temel Analiz (FA), yatırımcılar tarafından bir kripto paranın veyahut bir hissenin gerçek değerini belirlemek için kullanılır. Yatırımcılar alım- satım yapmak için temel analizden faydalanır. Kripto paranın geleceği hakkına tahmin yürütebilmeleri için o varlığa etki eden iç ve dış etmenleri ayrıntısıyla incelenmesi gerekmektedir. Temel analiz şirketleri değerlendirmede teknik analize oranla çok başarılıdır.

Elinde proje verileri olan herkes test edilmiş teknikler ile kolayca test yapabilir.

Bir şirketi ele aldığımızı varsayalım.

Aşağıdaki aşamaları uygulayarak projenin geleceği hakkında tahmin yürütebiliriz:

1. Şirketin bilançosu, nakit akışı, kazancı ve finansal tablolarını incelenebilir.
2. Şirketin faaliyet gösterdiği piyasa veya sektörü incelenebilir.
3. Rakipler ve müşteri kitlesi, büyüme potansiyeli incelenebilir.
4. Enflasyon, faiz oranları gibi ekonomik öğeleri incelenebilir.

2.4.2.1. Temel Analizdeki Popüler Göstergeler

Hisse Başına Kar (HBK)

Hisse başına kar, projenin her bir hissesinden ne kadar kar ettiğini gösterir [74]. Aşağıdaki gibi hesaplanır:

$$(Net\ gelir\ -\ Hisse\ senetlerindeki\ kar\ payı)\ /\ Toplam\ hisse\ sayısı$$

Fiyat Kazanç (F/K) Oranı

Fiyat kazanç oranı, o projenin hisse fiyatlarının HBK'siyle kıyaslanarak o şirketin değerini belirlenir. [74]. Aşağıdaki gibi hesaplanır:

$$Hisse\ fiyatı/\ Hisse\ başına\ kar$$

Piyasa Değeri Defter Değeri (PP/DD) Oranı

Piyasa değeri- defter değeri oranı yani piyasa değeri-öz kaynak PD/Ö olarak da bilinmektedir. Yatırımcıların şirketleri defter değerlerine göre değerlendirmelerini ele alır. Defter değeri de projenin finansal raporlarındaki değerlerdir [74]. Aşağıdaki gibi hesaplanır:

$$Hisse\ başına\ fiyat/\ Hisse\ başına\ defter\ değeri$$

Fiyat Kazanç/Beklenen Büyüme (PEG) Oranı

Fiyat kazanç/beklenen büyüme oranı, büyüme oranlarını dikkate alarak F/K'nin kapsamını genişleten fiyat kazanç oranının bir uzantısıdır [74]. Aşağıdaki gibi hesaplanır:

$$Fiyat\ kazanç\ oranı/\ Beklenen\ büyüme\ oranı$$

2.4.2.2. Kripto Paralarda Temel Analiz Göstergeleri

Ağ Değeri İşlem Hacmi (NVT) Oranı

Ağ değeri işlem hacmi oranı, genellikle P/E'nin kripto paralardaki hali olarak kabul edilir [74]. Aşağıdaki gibi hesaplanır:

$$Ağ\ değeri/\ Günlük\ işlem\ hacmi$$

Aktif Adresler

Bazı yatırımcılar, işlem yapacağı ağın ne kadar kullanıldığını bilmek ister ve bunun içinde aktif adreslerin sayısını inceler.

Fiyat Madencilik Başabaş Oranı

Fiyat madencilik başa baş oranı, madenciliği yapılan Proff of Work coinlerinin değerlendirildiği göstergedir. Madencilik maliyetli bir işlem olduğu için donanım ve elektrik masrafları da dikkate alınır [74]. Aşağıdaki gibi hesaplanır:

$$Coin\ piyasa\ fiyatı / Bir\ coin\ için\ madencilik\ masrafı$$

Whitepaper, Ekip Ve Yol Haritası

Token ve kripto paraların değerini belirlemede en eski usül proje incelemeleridir. Bu proje incelemeleri projeye ait whitepaperı okuyarak kullanım alanları, teknolojisi ve hedefleri, yürütücü ekip deneyimleri vb. araştırarak yapılır [73].

3. BLOKZİNCİR BİLEŞİMİ

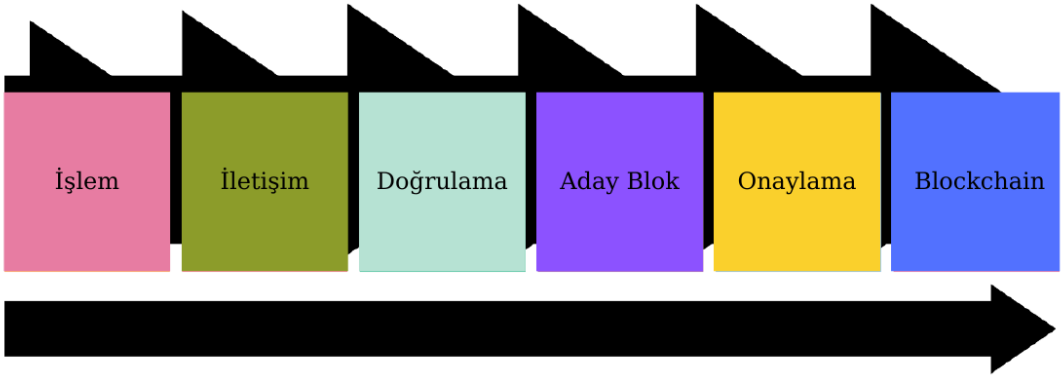
Blok zinciri, zaman serisi bloklarından oluşan bir veri yapısıdır. Blok, ilgili bilgi ve kayıtları içeren bir veri topluluğudur ve blok zincirinin temel birimidir. Blok zincirinin veri yapısı temel olarak bir blok başlığı ve bir blok gövdesinden oluşur. Blok başlığı, önceki bloğu bağlamak ve alttaki blok zincirinin bütünlüğünü sağlamak için kullanılan önceki bloğun karmasıdır. Blok gövdesi, bloğun ana bilgilerini (işlem bilgileri gibi) içerir. Bu bilgi, önceki bloğun hash yapısını ve rastgele sayı ile mevcut bloğun hash yapısını oluşturur [46].

3.1. Blokzincir ve Dijital Finansallaşma

Bitcoin veya Ethereum gibi kripto para birimlerinin hızlı yükselişinden bu yana Blokzincir konusu da ilgi odağı haline geldi. Çoğu zaman, Blokzinciri teknolojisinin işlevselliği ve özellikleri önemli ölçüde azaltıldı veya eksik olarak tanımlandı. Bu nedenle, bir blok zincirinin ne olmadığını anlamak da gereklidir. Farklı blok zincirlerinin birbirleriyle iletişim kuramaması, yani veri alışverişi yapamaması anlamına gelen blok zinciri sistemi, Bitcoin değildir ve Bitcoin blok zincirine eşit değildir. Bitcoin, teknolojiye dayalı blok zinciri kullanan bir kripto para birimidir. Bu nedenle, bir blok zinciri üzerindeki bir uygulamadır, ancak akla gelebilecek tek uygulama senaryosu değildir. Ek olarak, dünya çapında birçok kripto para birimi olduğu için Bitcoin tek kripto para birimi değildir. Ve bir blok zincirinin kesinlikle bir para birimine, özellikle de genel manada bir kripto para birimi kullanmayan özel blok zincirlere ihtiyacı yoktur. Bununla birlikte, halka açık blok zincirlerinde bu para birimleri daha fazla katılımcı çekmek için bir teşvik mekanizması olarak hizmet eder ve blok zinciri içindeki doğru davranış veya bilgi işlem gücü için "parasal" değerlerle ödüllendirilir. Bir blok zinciri sistemi, bir veritabanı ile aynı değildir [77].

3.1.1. Blokzincir Teknolojisi ve Kripto Para Piyasalarının Finansallaşma Bağlantıları

Şekil 26'da işlem, iletişim, doğrulama, blok adayı ve sürecin doğrulanması bir görsel ile ifade edilmektedir. Zincirin halkalarının iç içe geçmesiyle birlikte Blokzincir kavramını ortaya çıkarmaktadır [77].



Şekil 27. Blokzincir çalışması ve fonksiyon sıralaması [77].

Blokzincir yapısına ait teknoloji mimarisi oluşturulmak istendiğinde sırasıyla şunlardan oluşur:

- Veri katmanı,
- Ağ katmanı,
- Konsensüs katmanı,
- Teşvik katmanı,
- Sözleşme katmanı ve
- Uygulama katmanı [77]

Veri katmanı, temel veri bloklarını ve zaman damgalarını vb. içerir ve tüm işlem verilerini ve bilgi kayıtlarını blok zinciri formatında saklar. Ağ katmanı esas olarak eşler arası (P2P) ağ teknolojisini (noktadan noktaya iletim teknolojisi veya eşler arası ağ teknolojisi olarak da bilinir), yayılma mekanizmalarını ve kimlik doğrulama mekanizmalarını içerir. Konsensüs algoritmalarını, şifreli imzaları ve veri depolamayı tamamlayacaktır. Konsensüs katmanı, temel olarak, karar gücünün yüksek oranda dağıtıldığı merkezi olmayan bir sistemde düğümlerin blok verilerinin etkinliği üzerinde anlaşmaya varmasına izin veren bir fikir birliği mekanizması içerir. Teşvik katmanı, esas

olarak ekonomik teşvik verme mekanizmaları ve dağıtım mekanizması dahil olmak üzere ekonomik faktörleri blok zincir teknolojisi ile bütünleştirir. Teşviklerin amacı, katılımcıları bilgi işlem güçlerine katkıda bulunmaya çekmektir. Sözleşme katmanı temel olarak çeşitli komut dosyası kodlarını, algoritmik mekanizmaları ve akıllı sözleşmeleri içerir ayrıyeten düzenlenmiş ve denetlenebilir sözleşme özelliklerini belirler. Uygulama katmanı ise mevcut tüm verilerin programlanmasına katkıda bulunur [77, 78].

Konsensüs Algoritması: Bu algoritma, bilgisayar bilimlerinde dağıtılmış süreçler veya sistemler arasında tek bir veri değeri üzerinde anlaşmaya varmak için kullanılan bir süreçtir. Bu nedenle, blok zincirindeki konsensüs mekanizmalarının önemi, dağıtılmış bir kümenin kendi kuralları altında durum geçişlerini gerçekleştirdiği bir işlemin veya bir durumun güncellenmesinin basitleştirilmesi ve sağlanmasıdır [79].

3.1.2. Blokzincir Teknolojisi ve Dijital İmza

Dijital imza, kayıtlı bir işlemdeki belge ve belgeyi imzalayanı güvenli bir biçimde ilişkilendiren elektronik kimlik doğrulamasıdır. El yazısı imza gibi, belgeyi imzalayan kişiyi tanımlayan dijital imzayı kısaca bir mesaja ya da belgeye eklenmiş bir kod gibi de düşünülebilir [80]. Basite indirgendiğinde dijital imza, bir dokümana ya da mesaja eklenmiş bir kod olarak açıklanabilir. Kod, oluşturulmasının sonrasında, göndericiden alıcıya giderken mesajın değiştirilmediğinin bir kanıtıdır.

Eski tarihlerde kriptografi kullanarak iletişimi güvenli hale getirmek, Açık Anahtar Kriptografisinin (PKC) dijital imza yapıları 1970 yılında geliştirilmesiyle ancak mümkün hale getirilmiştir. Bu sebeple, dijital imzaların çalışma yapılarını öğrenmek için ilk olarak hash fonksiyonlarının ve açık anahtar kriptografisinin yapısını öğrenmek gerekir. Dijital imza belirli bir teknik alt yapıya ihtiyaç duymaktadır. Örneğin kullanıcının bilgisayarı ve dijital imzayı oluşturabileceği yazılımının olması gerekmektedir. Kullanıcının bunlar vasıtasıyla kendi dijital şifresini oluşturabilir [81].

Dijital imza, elektronik belgeyi şifreleyerek değiştirilmesini önlemekte ve birden fazla kişinin şifrenin anahtarını öğrenmeden elektronik olarak haberleşmesini sağlamaktadır. Teknik açıdan dijital imza, anahtar denilen bir çift şifreden oluşmaktadır. Anahtarların birincisi göndericide, diğeri ise alıcıda bulunur. Bu anahtarlardan göndericideki gizli

anahtarla dijital imza oluşturulup açık anahtar denilen diğeri ise, alıcıya bildirilir ve yalnızca dijital imzanın doğrulanmasında kullanılmaktadır [82].

3.1.2.1. Hash (Öz değer) Fonksiyonları

Dijital imza sistemlerinin temel ögelerinden biri de hashing işlemidir. Hashing süreci, herhangi büyüklükteki veriyi sabit büyüklükte çıktı haline getirmeyle ilgilidir. Yapılan bu işlem, özel algoritma olarak bilinen hash fonksiyonları ile yapılır. Hash fonksiyonu tarafından oluşturulan bu çıktı hash değeri (mesaj özeti) olarak isimlendirilir. Hash fonksiyonları ile kriptografi birleştirildiğinde, kriptografik hash fonksiyonları ismini alan bu işlemler benzeri olmayan dijital parmak izi olarak ilerleyen bir hash değeri(özet) yapmak için kullanılabilir. Bu da girdi verisindeki (mesaj) yapılan rastgele bir değişikliğin tamamen farklı bir çıktı (hash değeri) yapacağını göstermektedir. Kriptografik hash fonksiyonlarının dijital verilerin yapılarını, orijinalliğini kanıtlamak için sıkça kullanılmasının gerekçesi budur.

Sistem, imzalama aşamasında karmaşık işlemler olmasına rağmen kullanıcı için bir hayli kolay işlemektedir. Gönderilecek veri kendisine has bir şekilde kısaltılır bu işleme "hash" (öz değer) denmektedir. Sonrasında gizli anahtarlarla bu hash kodlanır. Sonuç olarak dijital imza, kodlanmış hash bileşenlerinden oluşmaktadır. Dijital imza, hash işlemine sokulmuş iletiye eklenir ve alıcıya gönderilir. Alıcı açık anahtarlarla şifreyi çözer. Deşifre olmuş gönderici hash değeri, alıcı hash değerine eşit ise ileti doğru bir şekilde iletilmiş anlamına gelmektedir [83].

3.1.2.2. Açık Anahtar Kriptografisi (PKC)

Açık anahtar kriptografisi (PKC), Asimetrik kriptografi olarak da bilinen açık anahtar kriptografisi (PKC), tek anahtarın kullanıldığı simetrik kriptografinin aksine hem açık hem de özel anahtarların kullanıldığı bir altyapıdır [84]. İki anahtar matematiksel olarak bağlantılı olup hem dijital imzalar için hem de veri şifreleme kullanılabilir.

PKC bir şifreleme aracı olarak, diğer simetrik şifrelemelere göre daha güvenlidir. Bundan önceki sistemlerde bilginin şifrelenmesi ve şifresinin açılması için aynı anahtar kullanılırken, PKC'de veri şifrelemesi açık anahtarla ve şifre çözümü de karşılık gelen

özel anahtarla yapılmaktadır. Bu yapılanların dışında PKC yapıları dijital imzaların yapılması aşamasında da uygulanabilir. Bu yapılan süreç basitçe, bir mesajın (ya da dijital verinin) imzalayan kişilerin özel anahtarı ile hashlenme işleminden oluşmaktadır. Bu işlemden sonra mesajı alacak olan kişi, imzalayan kişi tarafından temin edilen açık anahtarı kullanarak imzanın geçerli olup olmadığını kontrol edebilir. Belli başlı durumlarda, dijital imzalar şifreleme de içerebilir. Ancak bu her zaman değildir. Örneğin; dijital para birimi olan Bitcoin, Blokzincir'i PKC'den ve dijital imzalardan faydalanır fakat birçok insanın düşündüğünün tam tersine bu süreçte şifreleme yapılmaz. Teknik olarak dijital para birimi Bitcoin işlemleri doğrulamak için Eliptik Eğri Dijital İmza Algoritmasını (ECDSA) kullanır. Gönderici orijinal iletiyi gizli anahtarıyla şifreler ve bu belgeyi alıcıya hem şifresiz hem de şifreli olarak iletir. Alıcı şifreli belgeyi göndericinin açık anahtarını kullanarak açar ve şifresiz gelen belge ile karşılaştırıp iki belge birbirine uyuyor ise belge orijinal olarak kabul edilir [85].

3.1.2.3. Dijital İmzaların Çalışma Mimarisi

Dijital paralar bağlamında, bir dijital imza sistemi çoğunlukla üç temel adımdan oluşur: *İmzalama, hash etme, doğrulama.*

- **Veriyi hash etme**
  İlk olarak dijital veriyi ya da mesajı hash etmektir. Bu işlemleri yapabilmek için veri bir hashing algoritmasından geçirilerek bir hash değeri yaratılır. Örneğin: mesaj özeti.

Hash fonksiyonunun en temel özelliği: Mesaj büyüklüğü geniş çapta farklılık gösterebilir ancak girdiler hash edildiğinde ortaya çıkan tüm hash değerleri aynı uzunlukta olur.

Veriyi hash etmek dijital imza yapmak için zorunlu değildir. Bunun nedeni ise bir kişi özel anahtarını kullanarak hiç hash edilmemiş bir mesajı imzalayabilir. Dijital paralar için veri her zaman hash edilebilir. Çünkü sabit uzunlukta özetlerle çalışmak yapılan tüm süreç için çok önemlidir [86].

- **İmzalama**

Bilgi hash edilince, mesajın göndereninin bunu imzalaması gerekir. Açık anahtar kriptografisinin devreye girdiği yer burasıdır. Her birinin farklı özelliği olan kendine has

özel mekanizmalara sahip birkaç farklı dijital imza algoritması türü vardır. Bunların en önemlisi, hash edilmiş mesaj özel anahtarla imzalanır ve mesajın alıcısı bunlara karşılık olarak gelen açık anahtarı (imza atan tarafından sağlanır) kullanarak mesajın geçerliliğini kontrol eder. Başka bir söylemle, imza yapılırken özel anahtar dahil edilmezse alıcı mesajın geçerliliğini doğrulamak için karşılık gelen açık anahtarı kullanamaz.

Mesajın göndereni hem açık hem de özel anahtarları oluşturur. Ancak yalnızca açık anahtar alıcı ile paylaşılır. Dijital imzaları, her bir mesajın içeriği ile direkt olarak ilişkili olduğunu belirtmek de oldukça önemlidir. Gönderilen mesajdan bağımsız olarak genellikle hep aynı olan el ile atılan imzaların aksine her biri dijital olarak imzalanmış mesaj farklı bir dijital imzaya sahip olacaktır [86].

- **Doğrulama**

  Son doğrulama adımına kadar oluşan tüm süreç açıklanmak istendiğinde;

Matt'in Chris'e bir mesaj yazdığını, bunu detaylıca inceledikten sonra hash ettiğini ve daha sonrasında hash değerini kendisine özel anahtarıyla birleştirerek bir dijital imza yarattığını düşünelim. İmza, gönderilen mesaj için benzeri olmayan bir dijital parmak izi olarak çalışacaktır. Chris'e mesaj ulaştığında, dijital imzanın geçerliliğini Matt tarafından sağlanan açık anahtarı kullanarak kontrol edebilir. Bu şekilde Chris, imzanın Matt tarafından yaratıldığına emin olabilir. Çünkü açık anahtara karşılık gelen özel anahtar yalnızca Matt'te olması beklenir.

Matt'in özel anahtarını gizli tutması çok önemlidir. Eğer Matt'in özel anahtarı başka birinin eline geçerse bu kişiler dijital imzalar yaratabilir ve Matt gibi davranabilir. Dijital para bağlamında bu kişinin Matt'in özel anahtarını kullanarak ona ait Dijital paraları izni olmadan taşıması ya da harcaması anlamına gelir [86].

3.1.2.4. Dijital İmzaların Önemi ve Kullanım Alanları

Dijital imzalar genellikle üç amaç için kullanılır: *Doğrulama, inkâr edememe ve veri bütünlüğü.*

- *Veri bütünlüğü*: Chris, Matt'e ulaştırılan mesajın kendisine gelene kadar başka kişiler tarafından değiştirilmediğini doğrulayabilir. Mesajda yapılan en ufak bir değişiklik tamamıyla bambaşka bir imza yaratacaktır.

- *Doğrulama*: Matt kendisine ait anahtarlarını gizli tuttuğu müddetçe Chris, Matt'in açık anahtarını kullanarak dijital imzaların başka biri tarafından değil Matt tarafından yaratıldığını onaylayabilir.
- *İnkâr edememe*: İmza bir kere oluşturulduğunda, özel anahtarlar başkasının eline geçmediği takdirde Matt imza attığını gelecekte reddedemez.

Dijital imzalar çeşitli sertifikalarda ve dijital belgelerde kullanılabilir. Dolayısıyla, çeşitli uygulamalara da sahiptir. En yaygın kullanım alanlarından bazıları şunlardır:

- *Blokzincir*: Dijital imza yapıları, kripto paraların yalnızca gerçek (özel anahtarları başkaları tarafından ele geçirilmediği müddetçe) sahiplerinin kullanmasına izin vermektedir.
- *Bilgi Teknolojisi*: İnternet iletişim sistemlerinin güvenliğini güçlendirmek.
- *Sağlık*: Dijital imzalar sağlık kayıtlarındaki ve reçetelerdeki sahtecilikleri engelleyebilir.
- *Finans*: Dijital imzalar denetimlere, masraf raporlarına, kredi anlaşmalarına ve daha pek çok şeye uygulanabilir.
- *Hukuk*: Resmi evraklar ve iş anlaşmalarında yasal olarak imzalamalarını sağlamaktadır.

Dijital imza yapılarının karşı karşıya kaldığı başlıca zorluklar en az üç gerekliliğe dayanır:

- *Uygulama*: Eğer algoritmalar iyi fakat uygulama kötü olursa dijital imza sistemlerinde sorunların görülmesi olasıdır.
- *Algoritma*: Dijital imza yapılarında kullanılan algoritmaların kalitesi önemlidir. Buna güvenilir hash fonksiyonları ve kriptografik sistemlerin seçilmesi de dahildir.
- *Özel Anahtar*: Eğer özel anahtarlar açığa çıkarsa ya da bir başkasının eline geçerse orijinallik ve reddedilememe özellikleri geçersiz hale gelir. Kripto para kullanıcılarının anahtarlarını kaybetmeleri ciddi finansal kayıplara yol açabilir [86].

3.1.2.5. Elektronik İmzalar ve Dijital İmzalar

Basitçe ifade etmek gerekirse dijital imzayı bir belgeye veyahut bir mesaja eklenen kod olarak anlatabiliriz. Dijital imza kodu, iletilen mesajın veya belgenin alıcıya bozulmadan iletildiğine dair güven sağlar [86]. Dijital imzalar; hash fonksiyonları, açık anahtar kriptografisi ve şifreleme teknikleri gibi kriptografik sistemleri kullanır. Günümüzde hash fonksiyonları ve açık anahtar kriptografisi artık pek çok farklı kullanım alanına uygulanan dijital imza sistemlerinin tabanında yer alır. Dijital imzalar; eğer sağlıklı bir şekilde uygulamaya alınırsa güvenliği arttırmayı başarabilir, bütünlüğü garanti edebilir ve tüm dijital verilerin doğrulanmasına destek olabilir.

Yıllardır hem elektronik hem de dijital imzaları kullanıyor olsak da hala daha her ikisi için de büyüme fırsatları bulunuyor. Günümüzde sistemlerin büyük çoğunluğu hala evrak işlerine dayanıyor. Ancak dijital sistemlere geçtikçe dijital imza yapılarının daha fazla kullanılması çok olasıdır. Blokzincir dünyasında dijital imzalar, dijital para işlemlerini imzalamak ve onaylamak için kullanılır. Bitcoin için özel bir öneme sahiptir. Çünkü Coin bileşenlerinin yalnızca karşılık gelen özel anahtarlara sahip kişiler tarafından harcanabilmesini garanti altına alır.

3.2. Blokzincir Teknolojisi ve Kullanım Alanları

Blokzincir teknolojisi, karşılıklı taraflar arasındaki işlemleri efektif ve geçici olmayan bir şekilde kaydeden açık, dağıtılmış bir defterdir. Bir Blokzincir, belirli bir sırayla birbirine bağlanmış bir dizi ilgili işlemi içeren ayrı veri bloklarından oluşur. Alakalı bütün taraflar, merkezi bir otoriteye veya aracılara ihtiyaç duymadan bir bilgisayar ağında dijital bir defteri paylaşabilir. Bu nedenle işlemlerin blok zinciri aracılığıyla işlenmesi daha hızlıdır [5].

3.2.1. Blokzincir Teknolojisi ve Geleceğe Yönelik Teknoloji Uygulamaları

Blokzincir teknolojisi birçok alana yenilikler getirmiştir. Bunlardan biri de enerji sektörüdür. Enerji üretimi ve satışında kullanılan Blokzincir tabanlı ödeme sistemi, sektöre ödeme, güvenlik ve sadakat girişimlerini getirdi. Ülkemizdeki mevzuata göre üreticiler lisans almadan doğrudan nihai tüketiciye enerji satamazlar. Blokzincir tabanlı bir ödeme altyapısı kullanılırsa üreticiler arasında ve üreticiler ile tüketiciler arasında

ödemeler aracısız yapılabilir, ucuzken enerji satın alabilirler. Üretici olmadıkları halde geçmişte aldıkları enerjiyi kullanabilirler, hatta daha pahalı bir kazanç için başkasına satabilirler. Akıllı sayaçlara ödeme sistemi kurularak yaygınlığı artırılacaktır.

Geliştirilen ödeme sistemi, evde elektrik üreten bir komşuya fazla enerji satma veya yenilenebilir enerji kaynakları ile bütünleşmiş şarjlı otomatlarla satış yapma gibi senaryolarda kullanılabilir. Kullanıcının enerjisini alıp daha önce satın aldığı kripto para ile ödeme yapabileceği ve ödeme miktarına göre sistemden puan kazanabileceği ve puanlarını tekrar enerjiye çevirebileceği şekilde tasarlanabilir [11]. Bu sistem ile enerji üreticilerinin kayıp ve kaçak maliyet, faturalama, kredi-borç ilişkisi gibi sorunları her iki taraf için de düzenlenecek ve bu konularda yaşanan sorunlar ortadan kalkacaktır. Elektrikli araç sayısındaki artışla birlikte kapasite sıkıntısının da artacağı tahmin edilmektedir. Bu sorunu aşmak için yapılacak yatırımlar ülkemize ekonomik bir yük getirecektir. Kapasite yatırımına gerek kalmadan gerçekleştirilecek projeler, ekonomik kazanç sağlamakta ve yenilenebilir enerji kaynaklarına yönelerek çevrenin korunmasına katkıda bulunmaktadır [87].

Dördüncü sanayi devriminin bir parçası olarak Blokzincir teknolojisi bu dünya için yenidir. Konu, kripto para borsalarının tanıtılması ve kripto para birimlerinin dünyanın bazı büyük ekonomilerinde bir dijital ödeme modu olarak kabul edilmesinden sonra 2016 sonrasında araştırmacılar arasında dikkat çekmeye başlamıştır [88]. Teknoloji, eğitim, Nesnelerin İnterneti, bankacılık, tedarik zinciri, sağlık hizmetleri, savunma, yönetişim vb. dahil olmak üzere tüm önemli araştırma alanlarında yaygın olarak uygulanmaktadır [89, 90]. Bununla birlikte, araştırmalar ayrıca, blok zinciri uygulamasının son derece olgunlaşmamış olduğunu ve kamu bilgisinden yoksun olduğunu ve bunun da gerçek gelecek potansiyeline dair net bir stratejik vizyona sahip olmayı zorlaştırdığını bulmuştur. Şu anda ölçeklenebilirlik, akıllı sözleşmelerin güvenliği ve kullanıcı kabulü ile ilgili sorunlar mevcuttur [91]. Blokzincir teknolojisinin okullar, kolejler, üniversiteler arasındaki bağlantılarda ve dolayısıyla toplumla ilişkilerinde önemli değişiklikler getirebileceğine inanılmaktadır.

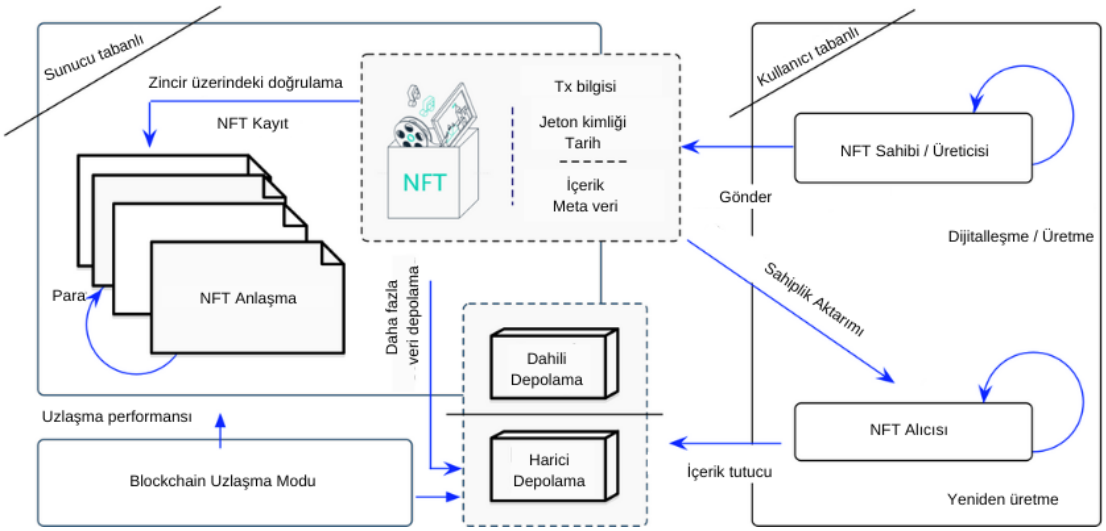
Birçok teknolojik yenilik alanında olduğu gibi, akademik çalışmalar da teknolojilerin pratikte uygulanmasında gecikme eğilimindedir. Yalnızca dergi yayınlarına güvenmek, literatüre oldukça dar bir bakış açısı sağlayacaktır. Bu nedenle mevcut uygulamanın durumunu gözden geçirmek, blok zinciri teknolojisinin pratikte

nasıl kullanıldığını anlamak için sağlam bir zemin sağlamak için çok önemlidir. Mevcut endüstriyel sömürü ve blok zincirinin gelişiminin trendini belirlemek için çok çeşitli kaynaklara danışılmıştır [92]. Bu bölümde Blokzincir bileşiminin ve geleceğe yönelik çalışmalarından kısaca bahsedilmiştir. Ayrıca, Blokzincir teknolojisinin günümüzde kullanım alanlarına aşağıda yer verilmiştir.

3.2.1.1. Değiştirilemez Belirteç (NFT)

Değiştirilemez Belirteç (Non-Fungible Token, NFT), Ethereum'un akıllı sözleşmeleri tarafından türetilen bir tür kripto para birimidir [93]. NFT ilk olarak Ethereum İyileştirme Önerilerinde (EIP)-721 [94] önerildi ve daha sonra EIP-1155'te [95] geliştirildi. NFT, özünde Bitcoin [96] gibi klasik kripto para birimlerinden farklıdır [97]. Bitcoin, tüm madeni paraların eşdeğer ve ayırt edilemez olduğu standart bir madeni paradır. Buna karşılık, NFT benzersizdir ve benzeriyle değiştirilemez (eşdeğeri, değiştirilemez), bu da onu bir şeyi veya birini benzersiz bir şekilde tanımlamaya uygun hale getirir. Spesifik olmak gerekirse akıllı sözleşmelerde (Ethereum'da [98]) NFT'leri kullanarak bir içerik oluşturucu, dijital varlıkların varlığını ve sahipliğini videolar, resimler, sanatlar [99], etkinlik biletleri [100], vb. Ayrıca, içerik oluşturucu ayrıca herhangi bir NFT pazarında başarılı bir ticaretin her seferinde veya eşler arası değişim yoluyla telif ücreti kazanabilir. Tam geçmişe dayalı ticaret, derin likidite ve uygun birlikte çalışabilirlik, NFT'nin gelecek vaat eden bir fikri mülkiyet (Intellectual Property,IP) koruma çözümü olmasını sağlar. Her ne kadar özünde, NFT'ler koddan biraz daha fazlasını temsil etse de bir alıcıya verilen kodlar, dijital bir nesne olarak karşılaştırmalı kıtlığı düşünüldüğünde değer atfetmiştir. Bu, fikri mülkiyetle ilgili ürünlerin, takası mümkün olmayan sanal varlıklar için düşünülemez gibi görünen satış fiyatlarını iyi bir şekilde güvence altına alır [93].

NFT'nin kurulması, eşler arası ağda ticaret için değiştirilebilir işlemlerle birlikte kayıtlar için temel bir dağıtılmış defter gerektirir. Bu rapor, öncelikle dağıtılmış defteri, NFT verilerini depolamak için özel bir veri tabanı türü olarak ele alır. Özellikle, defterin temel güvenlik tutarlılığı, eksiksizliği ve kullanılabilirlik özelliklerine sahip olduğu varsayılmaktadır [93].



Şekil 28. Nft sistemlerin çalışma yapısı [93].

Şekil 28 incelendiğinde NFT sistemlerin adım adım sunucu ve kullanıcı tabanlı olmak üzere çalışma mimarisine yer verilmiştir. Aşağıda sırasıyla depolama, işaretleme, ticaret ve onaylama işlemleri yer almaktadır.

- NFT Depolama: Bir NFT sahibi, ham verileri blok zincirinin dışındaki harici bir veritabanında saklar. Bu işlemin gaz tüketmesine rağmen, ham verileri bir blok zincirinde saklamasına da izin verildiğini unutmayın.
- NFT İşareti: NFT sahibi, NFT verilerinin karması dahil bir işlemi imzalar ve ardından işlemi akıllı bir sözleşmeye gönderir.
- NFT Darphane ve Ticaret: Akıllı sözleşme, NFT verileriyle işlemi aldıktan sonra para basma ve ticaret süreci başlar.
- NFT Onayı: İşlem onaylandıktan sonra, para basma işlemi tamamlanır. Bu yaklaşımla, NFT'ler kalıcı kanıtları olarak sonsuza kadar benzersiz bir blok zinciri adresine bağlanacaktır [93].

NFT'lerin çeşitli kullanım durumları için potansiyeli vardır. Örneğin, gayrimenkul ve sanat eseri gibi fiziksel varlıkları dijital olarak temsil etmek için ideal bir araçtır. NFT'ler blok zincirlere dayandıkları için aracıları kaldırmak ve sanatçıları izleyicilerle veya kimlik yönetimi için bağlamak için de çalışabilir. NFT'ler aracıları kaldırabilir, işlemleri basitleştirebilir ve yeni pazarlar yaratabilir. NFT'ler için mevcut pazarın çoğu, dijital sanat eserleri, spor kartları ve nadir ürünler gibi koleksiyon ürünleri etrafında toplanmıştır [101].

3.2.1.2. Kuantum Bilgisayarlar

Günümüzde verilerin iletilmesi kadar güvenli iletilmesi için iletim sürecinin gizliliği de çok önemlidir. İletilmek istenen verilere başkalarının erişememesi için şifreleme yöntemleri kullanılmaktadır. Söz konusu olan şifreleme yöntemleri kriptoloji olarak isimlendirilmektedir. Kriptoloji, cruptos(gizli) ve logos(bilim) kelimelerinden oluşmaktadır ve anlamı gizleme bilimidir. Kriptoloji, hem kriptografiyi (şifre bilimini) hem de kripto analizini (şifre analizini) kapsayan matematiksel tekniklerle ortaya konulan bilim dalıdır. Kriptografinin temel gayesi ise veri güvenliği için açık iletileri gizli iletilere dönüştürme işlemlerini yapmaktır. Kimlik doğrulama, gizlilik, bütünlük, güvenilirlik vb. bilgi güvenliğinin üst düzey olması gereken konular kriptografinin üzerinde çalıştığı konulardır [102, 103]. Özetle kriptografi; anlaşılır bir metni anlaşılmaz duruma getirme, anlaşılmaz bir metni de anlaşılır duruma getirme işlemidir.

Kriptolojide düz metin (plaintext), orijinal metne, şifreli metin (ciphertext): şifrelenmiş metne anlamlarına gelmektedir. Düz metni muhafaza etmek için şifreleme (encryption) işlemi yapılmalıdır. Şifrelenmiş metni okuyabilmek için alıcıda şifreyi çözebilecek anahtar bulunmalıdır. Bu sayede şifre çözme (decryption) işlemi gerçekleştirilebilir [104, 105]. Şifre çözme ve şifreleme işlemlerinde kullanılmak üzere birçok algoritma bulunmaktadır. Bunlar kriptografik algoritmalardır. Kriptografik algoritmalar, şifre çözme ve şifreleme işlemlerini anahtar ile yapmaktadır. Şifreli ileti sadece iletinin şifrelenmesinde kullanılan anahtar ile çözülebilmektedir [105, 106]. Anahtarlı şifreleme algoritmaları asimetrik şifreleme (açık anahtar) ve simetrik şifreleme (gizli anahtar) olarak ikiye ayrılmaktadır.

Asimetrik yani açık anahtarlı şifreleme yönteminde simetrik şifrelemeden farklı olarak 2 farklı anahtar bulunmaktadır: açık ve özel anahtar [106]. Şifreleme işleminde kullanılan anahtar: açık anahtar, şifre çözme işlemlerinde kullanılan anahtara ise özel anahtar denilmektedir [105]. Şifre anahtarının genele açık olmasından dolayı bu algoritmalar açık anahtarlı algoritmalar adlandırılmıştır. Kullanıcının açık anahtarıyla şifrelenen iletisi yalnızca o kullanıcının özel anahtarı ile ileti şifresi çözülebilmektedir.

Simetrik anahtar kriptografisi veri şifreleme ve şifreyi çözme işlemi için sadece tek 1 anahtar kullanır. Asimetrik kriptografi, kripto para ekosisteminin ve birçok internet altyapısının kritik öğelerindendir. Asimetrik kriptografinin en önemli avantajlarından biri güvenilirsiz kanal vasıtasıyla ortak anahtar paylaşmaksızın bilginin iletilmesine

olanak sağlar. Bu özelliksiz internette temel bilgi güvenliğinin sağlanması imkânsızdır. Asimetrik kriptografinin güvenliğinde açık anahtar kullanarak özel anahtarı hesaplamanın bir hayli zor, özel anahtar kullanarak açık anahtar oluşturmanın ise kolay olduğu varsayılır. Matematikte bu varsayıma "*tuzak kapısı fonksiyonu*" denir.

Günümüzde kriptolama işlemi için bu fonksiyondan yararlanılarak anahtar çifti oluşturulmaktadır. Tuzak kapısı fonksiyonu ile oluşturulan anahtarlar normal makineler ile ölçülebilir bir zamanda çözülemeyeceği bilinmektedir. Bu hesaplamalar için çok güçlü makineler için bile çok uzun zaman alır.

Günümüzde kullanmakta olduğumuz bilgisayarlar klasik bilgisayarlardır. Bilgisayarların karmaşık yapılı hesaplamaları daha hızlı yapabilmesi için çeşitli yazılım ve donanımlar vardır. Ama mantık hep aynıdır. Hesaplamalar sırayla kuyruk mantığıyla ilerler ve biri bitince diğeri başlar. Bu bilgisayarların hafıza yapısı bitlerden oluşmaktadır. Her bit 0 veyahut 1 değerini alır. Kuantum bilgisayarlarda ise seri qubit(kübit)lerden oluşur. Bir qubit 0 veyahut 1 veya 0-1 arasındaki bir değeri alabilir. Sonuç olarak n qubit sayısına sahip bir kuantum bilgisayarı tek seferde 2^n çakışmanın herhangi birinde olabilir [107]. Bir bilgisayardan 4 bitlik bir anahtarı çözmesini yani tahmin etmesi örneğini düşündüğümüzde, bu bitlerin her biri 1 veya 0 olabilir.

Klasik bilgisayarlar bu kombinasyonların her birini ayrı ayrı tahmin etmektedirler. Bu durumda anahtar uzunluğu arttıkça kombinasyon sayıları da 2^n kuralına bağlı olarak artmaktadır. Örneğin 5 bitlik anahtar için 32, 6 bit için 64 olası kombinasyon oluşmaktadır. Dolayısı ile tahmin etme süreside doğru orantıda artmaktadır. Klasik hesaplama sistemlerinin 55 bitlik bir anahtarı çözümlemesi tahmin etmesi yaklaşık 1000 yıl alır. Bitcoin'de 128 bitlik bir anahtar kullanılması önerilmektedir ve çoğu cüzdan uygulamaları 256 bitlik anahtarlar kullanırlar. Klasik bilgisayarların kripto paralar ve internet altyapısında kullanılan asimetrik şifrelemeyi çözme konusunda bir tehdit oluşturmadığı aşikardır.

RSA: Birçok akıllı karta gömülü en iyi olduğu varsayılan ve kullanılan açık anahtar algoritmasıdır [108]. RSA, kredi kartlarını, e-postaları ve diğer birçok elektronik sistemi güvenli hale getirmekte kullanılır [109].

Henüz gelişim aşamasında olan ve bir problemi çözmede hiç zorlanmayacak olan bu bilgisayarlar kuantum mekaniği teorisinin atom altı parçacıkların nasıl davrandığını açıklayan temel prensiplerine dayanır. Kuantum bilgisayarlar veri üzerinde

işlem yapmak için dolaşma ve bindirme vb. kuantum-mekanik fenomenin doğrudan kullanımını sağlayan teorik hesaplama sistemlerini kullanan bilgisayarlardır [110].

Klasik bilgisayarlar 2^n durumun sadece birinde bulunurken, kuantum bilgisayarı bu durumların bir kısmında veyahut hepsinde bulunabilir. Kuantum bilgisayarları kübitleri (qubit) belirli kuantum mantık kapıları ile düzenleyebilir. Bu kapı serilerine kuantum algoritması denilmektedir [106]. Kuantum ile klasik bilgisayarların farkı; klasik bilgisayarlar transistörlü elektriksel devre kullanır. Bu işlem süresi hayli uzundur. Fakat Kuantum bilgisayarlarda fiber optik bağlantılardaki gibi ışık hızında işlemler mevcuttur. Kuantum bilgisayarların bu hızı araştırma ve geliştirme alanlarında çalışan özel şirketleri ve üniversiteleri çok heyecanlandırmış ve ciddi yatırımlar almalarına sebep olmuştur. 4 bitlik anahtarı çözme tahmin etme örneğine geri dönecek olursak, 4-qubitlik bir bilgisayar teorik olarak tek bir hesaplama yaparken tek seferde 16 kombinasyonun yani durumun tamamında olabilir. Bu durumda anahtarı doğru bulma olasılığı %100 olur.

Kuantum hesaplama teknolojisiyle kripto paralar da dahil modern dijital altyapının çoğunluğunun altında yatan kriptografi kolay çözülebilir ve anlamsız olabilir. Bu durumda tüm dünyanın hükümetlerin bile iletişimini, operasyonlarını ve güvenliğinin risk altında olduğu anlamına gelmektedir. Bu teknolojiye karşı önlem geliştirmeleri araştırılmadır. Kuantum bilgisayarlarının tehdidine karşı güvenli kabul edilen kriptografik algoritmalara kuantuma dayanıklı algoritmalar denilmedir. Kuantum teknolojisi saldırılarını engellemek için büyük veri boyutları oluşturmak için hashing vb. basit teknikler ve kafes tabanlı kriptografi benzeri yöntemler geliştirilmektedir. Yakın gelecekte güçlü kuantum bilgisayarlar, Ethereum ve Bitcoin vb. dayanan tüm Blokzincir yapıları için bir tehdit oluşturacağa benzemektedir [111].

Kuantum kriptografi, kuantum ışınlanma, kuantum ölçümleri ve kuantum hesaplama içeren kuantum bilgi işlemenin dalıdır. Kuantum mekanik sistemler, kuantum bilgisi ve kuantum hesaplama kullanılarak gerçekleştirilen bilgi işleme görevlerinin incelenmesidir [112]. Kuantum Algoritma, her adımı bilgisayarda gerçekleştirilen bir hesaplama veya bir sorunun adım adım çözümlerini içeren bir prosedürdür. Bu algoritma kuantum bir bilgisayarda gerçekleştirildiğinde kuantum algoritması olmaktadır. Şu an için güçlü kuantum bilgisayarlar mevcut değilse de kuantum algoritmaları teorisi 20 yıldan fazla süredir üzerinde çalışılan bir alandır [113]. Kuantum bilgisayar Shor ve

Grover algoritmaları sayesinde zor problemleri polinom zamanda çözmesi amaçlanmıştır.

Son zamanlarda zor matematiksel problemleri çözmek için gerek klasik bilgisayarlarla gerekse kuantum mekaniğiyle birçok araştırmalar yapılmıştır. Bu araştırmalar sonucunda güçlü kuantum bilgisayarlar şu ana kadar üretilmiş olsaydı, günümüzde kullanılan açık anahtarlı şifreleme sistemleri çoktan kırılmış olacaktı. Şifreleme sistemlerinin çözülmesi, dijital iletişim ve internet bütünlüğünü ve güvenliğini yüksek ölçüde tehlikeye sokacaktır. Kuantum sonrası kriptografinin amacı hem klasik bilgisayarlara hem de kuantum bilgisayarlara karşı güvenli çalışan kriptografik sistemler geliştirmektir [114]. Kuantum kriptografi tekniği çok güvenli protokollere sahipse de şu an için maliyeti bir hayli yüksektir. Bu sebepten ötürü günümüzde yalnızca askeri amaçlarla kullanılmaktadır. Uçtan uca şifrelemenin tanınmış mesajlaşma uygulamaları ve tarayıcılar aracılığıyla kullanılması gibi kuantuma dayanıklı standartlar da genel kitle kullanıma açılabilir. Bu standartlar geliştirildiğinde kripto para ekosistemi de saldırı vektörlerine karşı en güçlü savunmayı basit bir şekilde entegre edebilir.

Zaman ilerledikçe madencilikte blok bulmak ve o blokta işlem yapmak bir hayli zorlaşmıştır. Dolaysıyla madenciler için block bulmak oldukça zor bir duruma gelmiştir. Madencilik havuzları, birçok madencilik ile ilgilenen tarafları bir araya getirip birlikte daha yüksek seviyede madencilik yapmalarını sağlayan bir sistemdir.

Madencilik havuzları potansiyeli olan madencilere ulaşıp bağlantılar toplayıp sonrasında hash oranlarını birleştirir. Böylelikle havuzdaki her bir madenci daha yüksek seviyelerde madencilik yapmaya ve blokları işlemelerine olanak sağlar. Bir diğer güzel olanak ise blok ödülleridir. Blok ödülleri, madencinin sağladığı katkıya oranla madenciler arasında dağıtılmaktadır. Madencilik havuzlarının açılması kripto para madenciliğinde adeta bir devrimdir. Havuzlar, sabit ve daha istikrarlı gelir akışı garantiler ve bu yönüyle madenciler için bir hayli faydalıdırlar. Madencilerin havuzdaki ödeme planlarında kendilerine en uygun olanı seçmeleri gerekmektedir.

Bitcoin madenciliğinde merkeziyetsiz oluşu madenci için daha karlıdır. Tek bir havuzun çoğunluk hash oranını ele geçirmesi kimse için kazançlı olmayacağından muhtemelen diğer kullanıcılar tarafından engellenir. Bu sebeple madencilik havuzları merkeziyetsiz yapısına bir tehdit değildir. Bitcoin kullanıcılar tarafından yönetilir, madenciler tarafından yönetilmemektedir [115].

3.2.1.3. Spot Piyasa ve Spot Alım Satımı

Spot piyasa, herkese açık varlıklarını anında işleme sokabildiği finansal piyasadır. Bu piyasada alıcı satın alma işlemini itibari para veyahut diğer takas araçlarıyla yapabilir. Satın alınan varlık genelde anında teslim edilir, bu durum varlığa göre değişiklik gösterebilir. Başka bir ifadeyle spot piyasalar, satıcı ve alıcının buluştuğu ya da daha teknik açıklamak gerekirse varlığı talep ve arz edenlerin ilgili varlığın ödemesini ve teslimini eş zamanlı gerçekleştirdiği piyasalardır [116]. Spot piyasaların bir diğer adı da nakit piyasalardır. Bu isim işlemlerin nakit gerçekleşmesinden gelmektedir. Spot piyasaların birçok farklı türü vardır. Borsalar, 3. taraf olarak işlemlere yalnızca aracılık yapar. Borsa dışı yani OTC işlemler aracılığıyla farklı kişilerle direkt alışveriş yapılabilir. Spot piyasalardaki işlemlere Spot işlemler denilmektedir. Spot işlemlerde satıcı ve alıcılar sadece ellerindeki varlıklarla işlem yapabilirler. Marjin ya da kaldıraç işlemleri kullanılmaz [117].

Kripto spot işlemleri, kripto para birimleri kullanılarak yapılan alım satımları ifade eder. Kripto borsalarının tümünde olan bu yatırım, Türk lirası ya da dolar gibi birimlerle Ethereum veya Bitcoin alım satım anlamına gelir [118]. Spot piyasada, emtialar, para birimleri, hisse senetleri gibi finansal menkul kıymetler anında alınır ve satılır [119]. Spot piyasaların avantajlarından bahsedilecek olunursa;

- Bir varlığın fiyatı piyasadaki arz ve talebe göre şekillenir ve fiyatlar şeffaf olarak kullanıcılarla paylaşılır. Bu durum birden çok referans fiyat barındıran vadeli işlem piyasalarında farklıdır. Örneğin, bazı geleneksel piyasalardaki fiyatlar faiz oranlarından etkilenir.
- Kuralları basit, düşük riskli ve ödüllü olması nedenleriyle spot piyasada işlem yapmak çok daha kolaydır.
- Spot piyasada marjin ve türevlerindeki gibi likide edilme veyahut marjin çağrısı alma durumları söz konusu değildir. İstediğiniz an işleme girilebilir veyahut işlem sonlandırılabilir. Uzun vadeli yatırımlar için idealdir [120].

Spot piyasaların avantajlarının yanı sıra beraberinde getirdiği birçok dezavantajı da bulunmaktadır. Bu dezavantajlardan birkaç tanesine aşağıda yer verilmektedir;

- Alım satımı yapılan varlığa göre o varlığı elden çıkarılmasında güçlük çekilebilir.

- Spot piyasada kar edilebilmesi için o varlıkta, kullanıcılarda ve şirketler istikrar önemlidir. Varlığı sunan şirketin güven sağlıyor olması gerekir aksi takdirde varlık değerini kaybedecek ve kullanıcılarını zarar ettirecektir.
- Spot işlemlerde elde edilen kazançlar diğer işlemlere göre yani marjin veya vadeli işlemlere oranla çok daha düşüktür [120].

Spot satış yani spot işlem temelde bir yatırımdır. Spot işlemlerde kripto paralardan istediklerinizi alabilir, yükselişi bekler ve Spot satışı alınan fiyatın üzerine çıkınca satıp kar edebilirsiniz. Kullanıcıların aldığı kripto paralar direkt olarak kullanıcının sanal cüzdanına yansıtılmaktadır. Bu cüzdandaki para istenilen anca paraya çevrilebilir veyahut Takas ya da Stake gibi işlemlerde kullanılabilir. Spot, gerçek ya da dijital piyasalarda takas işlemlerine karşılık gelmektedir. En fazla 2 gün süren alım ve satımlarda, kullanıcılar bu sürede değişiklik olmaması risksiz işlemler için spot işlemleri daha fazla cazip kılar. Spot işlemler, ticaretin farklı alanlarında da kullanılan bir işlem türü olması kaynaklı kullanım alanı oldukça fazladır [121]. Spot alım satım işlemleri tek bir platformla sınırlı değildir. Çoğu kişi spot işlemlerini borsalarda yapıyor olsa dahi 3. taraf olmadan da kullanıcılar alışveriş yapabilirler. Borsa dışı, aracı kurumlar yani borsalar alışveriş fiyatlarını kullanıcılara belirtmek zorundadırlar. Fakat borsa dışı işlemlerinde emir defteri kullanma zorunluluğu yoktur. Bu durumun avantajlarından biride düşük fiyatlı coin bileşeni düşük likiditeye sahip varlıklar olduklarından büyük fiyatlı bir emir slipaja sebep olabilir. Bu sayede piyasa bir anda yükselişe geçebilir [120]. Spot piyasalarda işlemler anında gerçekleşir öte yandan Vadeli işlemler piyasasında işlemler ileri tarihte gerçekleşmek üzere sözleşmeler içerir. İşlemdeki varlığın toplam fiyatının küçük bir kısmı kadar başlangıç teminatı (marjin) ile yatırıma başlanabilir [122]. Spot alım satımlarda kullanıcı kendi bütçesine göre işlem yapabilir. Fakat marjin alım satım, borsalardan faizle borç alıp daha fazla parayla daha büyük pozisyonlara girmeyi sağlar. Marjin daha fazla kar etmeye imkân sağladığı gibi ters pozisyonda kalınca da daha fazla zarar edilmesine neden olabilir. Marjin spot alım satıma göre daha risklidir. Borsalar tarafından ödünç verilen bu paralar ters pozisyonda kalan diğer kullanıcılardan sağlanmaktadır [123].

SONUÇLAR VE ÖNERİLER

Bu çalışmada, literatürde finans ve bankacılık alanında Blokzincir kavramı üzerine geliştirilen birçok akademik çalışma ve lisansüstü eğitim enstitüsü tezlerine yönelik gösterilebilecek temel Blokzincir teknolojilerinin araştırılması gerçekleştirilmiştir. Günümüzde gelişen teknoloji ile dijitalleşen finans sektöründe yer alan blok zincir, kripto para birimleri ve merkeziyetsiz finans konuları geliştirilen yüksek lisans tezi ile ortaya konmuştur. Blokzincir ve kripto para ilişkisi ele alınırken aynı zamanda literatürde en sık kullanılan kripto paralardan birkaçı detaylıca ele alınmıştır. Bununla birlikte, merkeziyetsiz finans yani DeFi sistemlerin avantajları ve dezavantajları objektif bir şekilde değerlendirilerek tezde yer verilmiştir. Ayrıca, Blokzincir bileşeninin yapısal olarak incelenmesi ile dijital imza ve elektronik imza karşılaştırılmış; teknolojinin verimli kullanımı sayesinde günümüzde ve geleceğe yönelik Blokzincir teknolojilerinin kullanımına yer verilmiştir.

Gelecek çalışmalar için finans, bankacılık ve işletme alanlarında literatürde yer verilen Blokzincir temelli ilgili akademik çalışmalarda bu tez çalışmasında detaylıca incelenen temel teknolojiler göz önünde bulundurularak akademik literatüre katkı verilmesi sağlanmıştır. Sonuç olarak ekonomi, bankacılık, finans ve medya platformları gibi bireylerin ihtiyaç duyduğu birçok platformda yer alan Blokzincir teknolojisi detaylı bir şekilde incelenmiştir.

KAYNAKLAR

1. Nofer, M., Gomber, P., Hinz, O., and Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, 59.3, 183-187.

2. *What is blockchain technology a comprehensive guide for beginners?*. (2021). Binance Academy. https://academy.binance.com/tr/articles/what-is-blockchain-technology-a-comprehensive-guide-for-beginners

3. Aslan, M., Kasapbaşı, M. C. (2022). Blok Zinciri Platformları, Fikir Birliği Mekanizmaları ve Ağın Güvenlik Analizi. *Haliç Üniversitesi Fen Bilimleri Dergisi*, 5/1.

4. Yaşa, A. A. (2022). Kamu Sektöründe Blok Zincir Teknolojisi Kullanımı: Türkiye'de Mevcut Durum Analizi. *Yaşar Üniversitesi E-Dergisi* 17(66), 615-633.

5. Ezgin, B. (2021). *Blockchain Teknolojisinin Bankacılık ve Finans Sektöründeki Kullanım Alanları.* Yüksek Lisans Tezi, Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 134.

6. *What is the blockchain*. Bitpin. https://bitpin.ir/academy/what-is-the-blockchain/

7. Radziwill, N., and Benton, M. (2017). Quality and innovation with blockchain technology. *Software Quality Professional Magazine*, 20(1).

8. Miller, A. Juels, E. Shi, B. Parno, and J. Katz. (2014). Permacoin: Repurposing bitcoin work for data preservation. *IEEE Symposium on Security and Privacy*, 475–490.

9. Akleylek, S., ve Seyhan, K. (2018). *Blok Zinciri Bileşenleri ve Uygulamaları Üzerine Bir Derleme.* İnformasiya Təhlükəsizliyinin Aktual Multidissiplinar Elmi-Praktiki Problemləri, IV Respublika Konfransı Bildiri Kitabı

10. Tanrıverdi, M., Uysal, M., Üstündağ, M. T. (2019) Blokzinciri teknolojisi nedir? ne değildir?. *Bilişim Teknolojileri Dergisi,* 12(3), 203-217.

11. Yalvaç, M.F. (2021). *Blockchain Technology: Its Impact on Energy Efficiency and Trade.* Yüksek Lisans Tezi, İzmir Kâtip Çelebi Üniversitesi Fen Bilimler Enstitüsü, İzmir.

12. Mukherjee, P., and Pradhan, C. (2021). *Blockchain 1.0 to blockchain 4.0-The evolutionary transformation of blockchain technology.* Blockchain technology: applications and challenges (29-49), Springer, Cham.

13. *Smart contract*. (2022). Wikipedia. https://en.wikipedia.org/wiki/Smart_contract

14. Macrinici, D., Cartofeanu, and C., Gao, S. (2018). Smart contract applications within blockchain technology: a systematic mapping study. *Telematics Inform.* 35(8), 2337–2354.

15. *Cryptocurrency Market Capitalizations*. (2018). CoinMarketCap. https://coinmarketcap.com/

16. Bouoiyour, J., Refk S. (2017). *Ether: Bitcoin's competitor or ally?*. arXiv preprint arXiv:1707.07977.

17. Frankenfield, J. (2022). *Decentralized Applications (dApps)*. Investopedia. https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp

18. EdChain. (2018). *Blockchain FAQ #3: What is Sharding in the Blockchain?*. Medium. https://medium.com/edchain/what-is-sharding-in-blockchain-8afd9ed4cff0#

19. De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., and Sassone, V. (2018). *PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain*. Research Center of Cyber Intelligence and Information Security, Sapienza University of Rome.

20. Frankenfield, J. (2022). *What Is Proof of Work (PoW)?*. Investopedia. https://www.investopedia.com/terms/p/proof-work.asp#

21. Sarıkaya Yaylamış, G. (2022). *Blok zincir teknolojisinin öğrenimi için bir simülatör tasarımı.* Yüksek Lisans Tezi, Maltepe Üniversitesi, Lisansüstü Eğitim Enstitüsü, İstanbul.

22. *What's a Blockchain Bridge?*. (2022). Binance Academy. https://academy.binance.com/en/articles/what-s-a-blockchain-bridge

23. *What Are Blockchain Bridges, and Why are they Important for DeFi?*. (2021) Maker Blog. https://blog.makerdao.com/what-are-blockchain-bridges-and-why-are-they-important-for-defi/

24. Yuan, Y., and Wang, F. Y. (2018). Blockchain and cryptocurrencies: Model, techniques and applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 48(9), 1421-1428.

25. Yadav, S. P., Agrawal, K. K., Bhati, B. S., Al-Turjman, F., and Mostarda, L. (2020). Blockchain-based cryptocurrency regulation: An overview. *Computational Economics* 1-17.

26. *Blockchain Monitoring*. (2016). https://blockchain.info/

27. *Cryptocurrency Monitoring.* (2015). http://coinmarketcap.com/

28. Yuan, Y., and Wang, F. Y. (2018). Blockchain and cryptocurrencies: Model, techniques and applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* 48(9), 1421-1428.

29. *Conference in Metaverse Lane One Live Updates, Metaverse*. (2022). CoinMarketCap. https://coinmarketcap.com/alexandria/article/coinmarketcap-the-capital-conference-in-metaverse-lane-one-live-updates.

30. Vujičić, D., Jagodić, D., and Ranđić, S. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview.

31. Chen, H., Pendleton, M., Njilla, L., and Xu, S. (2020). A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. *ACM Computing Surveys (CSUR).* 53(3), 1-43.

32. Buterin, V. (2014). *A next-generation smart contract and decentralized application platform*. Ethereum white paper, 3(37), 2-1.

33. Koning, J. P. (2016). *Fedcoin: A central bank-issued cryptocurrency*. R3 Report, 15.

34. Marszałek, P. (2019). Kryptowaluty–pojęcie, cechy, kontrowersje. *Studia BAS,* (1), 105-125.

35. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* Decentralized Business Review, 21260.

36. Kołodziejczyk, H., and Jarno, K. (2020). Stablecoin–the stable cryptocurrency. *Studia BAS,* 3(63), 155-170.

37. Hoang, L. T., and Baur, D. G. (2021). How stable are stablecoins?. *The European Journal of Finance*, 1-17.

38. Mallick, S. K. (2020). Causal relationship between Crypto currencies: An Analytical Study between Bitcoin and Binance Coin. *Journal of Contemporary Issues in Business and Government Vol,* 26(2), 2172.

39. *BNB'nin Evrimi: İşlem Ücretlerinden Global DeFi Altyapısına. (2021)*. Binance. https://www.binance.com/tr/blog/ecosystem/bnbnin-evrimi-işlem-ücretlerinden-global-defi-altyapısına-4214998246849019 25.

40.*NBGlossary*. (2022). Binance Academy. https://academy.binance.com/en/glossary/bnb

41. *Decentralized Finance (DeFi) Definition*. (2022). Investopedia. https://www.investopedia.com/decentralized-finance-defi-5113835

42. Schär, F. (2021). *Decentralized finance: On blockchain-and smart contract-based financial markets*. FRB of St. Louis Review.

43. İmamoğlu, D. A. (2021). *Kripto para birimleri ve Türk hukukunda düzenlenmesi.* Seçkin.

44. Dizinler, T. (2014). Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi.

45. *DeFi Nedir?*. (2022). Bitlo. https://www.bitlo.com/rehber/defi-nedir

46. DeFi piyasasında kredi verme ve kredi çekme. (2021). CoinTelegraph. https://tr.cointelegraph.com/news/what-is-lending-and-borrowing-in-defi

47. Yeni Başlayanlar İçin Merkeziyetsiz Finans (DeFi) Rehberi. (2022). Binance Academy. https://academy.binance.com/tr/articles/the-complete-beginners-guide-to-decentralized-finance-defi#decentralized-marketplaces

48. İnternetin geleceği: Web 3.0 nedir?. (2021). Shift Delete. https://shiftdelete.net/internetin-gelecegi-web-3-0-nedir

49. Johnson, Steven (2018). Beyond the Bitcoin Bubble. The New York Times, ISSN 0362-4331. 21 11.

50. Schroeder, S. (2020). *Crypto wallet MetaMask finally launches on iOS and Android, and it supports Apple Pay*. Mashable. https://mashable.com/article/metamask-ios-android

51. *ConsenSys funding round would value crypto start-up at $3bn*. (2021). FT Magazine.

52. Schroeder, Stan (2021). *Crypto wallet MetaMask now lets you swap tokens on your phone.* Mashable. https://mashable.com/article/metamask-swaps

53. *What is a Bull Market in Cryptocurrency?*. Liquid. https://blog.liquid.com/what-is-a-bull-market-in-cryptocurrency

54. Ritter, J. R., Warr, R. S. (2022). *The Decline of Inflation and the Bull Market of 1982-1999*. Warrington College of Business. Journal of Financial and Quantitative Analysis Vol. 37, No. 1.

55.*Nasdaq Composite (^IXIC).* (2022). Yahoo Finance. https://finance.yahoo.com/quote/%5EIXIC/history?period1=788918400&period2=978134400&interval=1mo&filter=history&frequency=1mo&includeAdjust

edClose=true&guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuaW52ZXN0b3BlZGlhLmNvbS90ZXJtcy9iL2J1bGxtYXJrZXQuYXNw&guce_referrer_sig=AQAAANdKbv-c4_z_U4RxS1dQOdaxS92WUD2knxKldk_ZVb0o0F2Tu7zo7ifQv7ZkO05DTi-sBIFo7SL_FDeiqZMv_9RbfTjTkiFsGod8jnNxI6JsrpZTkoQ0HNsy_xxWRuSt7xLre85NE0HMN-GI6jj4rIkkDkg_04Slk66lZ6uetJL4

56. *Dow Jones Industrial Average - 1900-Present*. (2022). StockChart. https://stockcharts.com/freecharts/historical/marketindexes.html

57. *The Great Recession and Its Aftermath*. (2007). Federal Reserve History. https://www.federalreservehistory.org/essays/great-recession-and-its-aftermath

58. *Federal Reserve Bank of St. Louis. S&P 500*. (2022). Fred Economic Data. https://fred.stlouisfed.org/series/SP500

59. *Yıllara göre Bitcoin'in değeri: Son 10 senede ne oldu?.* (2021). Shift Delete. https://shiftdelete.net/yillara-gore-bitcoinin-degeri-son-10-yil.

60. *Ayı Piyasası Nedir?*. QNB Finansinverst. https://www.qnbfi.com/forex/forex-terimler-sozlugu/ayi-piyasasi-nedir

61. *Ayı Piyasası Nedir? Kripto Para ve Bitcoin Ayı Piyasası*. (2020). Coin Bilgi https://www.coinbilgi.net/ayi-piyasasi-nedir-kripto-para-ve-bitcoin-ayi-piyasasi/

62. *2022 ayı piyasası tarihin en kötüsüne dönüştü – Glassnode*. (2022). Coin telegraph. https://tr.cointelegraph.com/news/2022-bear-market-has-been-the-worst-on-record-glassnode

63. *Kripto Para Temel Analiz Rehberi*. (2022). Binance Academy. https://academy.binance.com/tr/articles/a-guide-to-cryptocurrency-fundamental-analysis

64. MACD Göstergesi Nedir?. (2022). Binance Academy. https://academy.binance.com/tr/articles/macd-indicator-explained

65. Göreceli Güç Endeksi Göstergesi Nedir?. (2022). Binance Academy. https://academy.binance.com/tr/articles/what-is-the-rsi-indicator

66. *Bollinger Bantları*. (2022). Binance Academy. https://academy.binance.com/tr/articles/bollinger-bands-explained

67. *Yeni Başlayanlar İçin Mum Grafik Rehberi*. (2022). Binance Academy. https://academy.binance.com/tr/articles/a-beginners-guide-to-candlestick-charts

68. *Çekiç Formasyonu Ne Demektir?*. Xtb Online Trading. https://www.xtb.com/tr/education/cekic-formasyonu-nedir.

69. *Teknik Analizde Kullanılan 12 Popüler Mum Grafik Formasyonu*. (2022). Binance Academy. https://academy.binance.com/tr/articles/beginners-candlestick-patterns

70. *Ters Çekiç-Boğalar*. Tradingview. https://tr.tradingview.com/support/solutions/43000583780/

71. *Mezar Taşı Doji.* (2021). Finansal Ansiklopedi. https://tr.nesrakonk.ru/gravestone-doji/

72. *Uzun Bacaklı Doji.* (2021). Finansal Ansiklopedi. https://tr.nesrakonk.ru/long-legged-doji/

73. *Yusufcuk Doji* . (2021). Finansal Ansiklopedi. https://tr.nesrakonk.ru/dragonfly-doji/

74. *Temel Analiz (FA) Nedir?*. (2020). Binance Academy**.** https://academy.binance.com/tr/articles/what-is-fundamental-analysis-fa

75. *Muhabbit Özel, "DEX nedir?"*. (2021)**.** Muhabbit. https://muhabbit.com/dex-nedir/

76. Meraklı, S. (2021). Merkeziyetsiz Finans (Defi) Faaliyetlerinin İzinsiz Bankacılık Faaliyetinde Bulunma Suçu Bakımından Değerlendirilmesi. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 27(2), 1156-1190.

77. Khatoon, A., Verma, P., Southernwood, J., Massey, B., and Corcoran, P. (2019). Blockchain in energy efficiency: Potential applications and benefits. *Energies,* 12(17), 3317.

78. Wu, J., and Tran, N. K. (2018). Application of blockchain technology in sustainable energy systems: An overview. *Sustainability*, 10(9), 3067 (2018).

79. Alabadı, M. A. A. A. (2019). *Blockchain as a solution to access control in IOT systems*. Yüksek Lisans Tezi, Altınbaş Üniversitesi, İstanbul.

80. *Dijital İmza nedir, nasıl kullanılır?*. (2021). İnnova E-bülten. https://www.innova.com.tr/tr/blog/dijital-donusum-blog/dijital-imza-nedir-nasil-kullanilir

81. Arıkan, S. (2000). *Modern İletişim Araçları ve Özel Hukuk (İnternette Sözleşme Akdi)*, Hukuk Kurultayı 2000 Bildiriler Kitabı, 312.

82. Erdotain, J.E. (1999). *Encryption Technnologies and Digital Signatures*. 27 IBL, 275.

83. *Dijital İmza Nedir ve Özellikleri Nelerdir?*. (2000). NTV Arşiv Teknoloji. www.ntvmsnbc.com/news/11740.asp

84. Açık Anahtar Kriptografisi Nedir?. (2022). Binance Academy https://academy.binance.com/tr/articles/what-is-public-key-cryptography

85. Berber, L. K. (2000). İmzalıyorum O Halde Varım Dijital İmza, Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Elektronik Belgelerin Hukuki Değeri. *Türkiye Barolar Birliği Dergisi* 514-525.

86. *Dijital İmza Nedir?* . (2021). Binance Academy. https://academy.binance.com/tr/articles/what-is-a-digital-signature

87. Kula, Ö. (2019). *Application to the energy sector by developing a system payment based on customer loyalty and blockchain.* Yayımlanmamış Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi, Malatya.

88. Bhaskar, P., Tiwari, C. K., & Joshi, A. (2020). Blockchain in education management: present and future applications. *Interactive Technology and Smart Education.*

89. Yaqoob, S., Khan, M. M., Talib, R., Butt, A. D., Saleem, S., Arif, F., and Nadeem, A. (2019). Use of blockchain in healthcare: a systematic literature review. *International Journal of Advanced Computer Science and Applications*, 10(5).

90. Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., and Faxvaag, A. (2020). Blockchain in healthcare and health sciences—A scoping review. *International Journal of Medical Informatics*, 134, 104040.

91. Radanović, I., and Likić, R. (2018). Opportunities for use of blockchain technology in medicine. *Applied health economics and health policy*, 16(5), 583-590.

92. Wang, Y., Han, J. H., and Beynon-Davies, P. (2018). Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. *Supply Chain Management: An International Journal*.

93. Wang, Q., Li, R., Wang, Q., and Chen, S. (2021). *Non-fungible token (NFT): Overview, evaluation, opportunities and challenges*. arXiv preprint arXiv:2105.07447.

94. William, E., Dieter, S., Jacob, E., Nastassia, S. (2018). *Erc-721 non-fungible token standard*. Ethereum Improvement Protocol, EIP-721, Accessible: https://eips.ethereum.org/EIPS/eip-721.

95. Witek, R., Andrew, C., Philippe, C., James, T., Eric, B., Ronan, S. (2018). *Eip-1155: Erc-1155 multi token standard.* Ethereum Improvement Protocol, EIP-1155.

96. Nakamoto, S. (2019). *Bitcoin:Apeer-to-peerelectroniccashsystem*. Accessible: https://bitcoin.org

97. Shirole, M., Darisi, M., Bhirud, S. (2020). *Cryptocurrency token: An overview*. IC-BCT 2019, 133–140.

98. Wood, G. (2014). *Ethereum: A secure decentralised generalised transaction ledger*. Ethereum project yellow paper 151.

99. Franceschet, M., Colavizza, G., Smith, T. (2020). Crypto art: A decentralizedview. *Leonardo* 1-8.

100. Regner, F., Urbach, N., Schweizer, A. (2019). *Nfts in practice non-fungible tokens as core component of a blockchain-based event ticketing application.*

101. *What Is a Non-Fungible Token (NFT)?*. (2022). Investopedia. https://www.investopedia.com/non-fungible-tokens-nft-5115211

102. Yerlikaya, T. (2006). *Yeni şifreleme algoritmalarının analizi*. Doktora Tezi, Trakya Üniversitesi Fen Bilimler Enstitüsü, Trakya

103. Yeşilbaş, E. (2016). Cebirsel Kriptoloji Yöntemleri ve Bazı Uygulamaları, Yüksek Lisans Tezi, Recep Tayip Erdoğan Üniversitesi Fen Bilimler Enstitüsü, Rize.

104. Kodaz, H., and Botsali, F. M. (2010). Simetrik ve asimetrik şifreleme algoritmalarının karşılaştırılması. *Selçuk Teknik Dergisi*, 9(1), 10- 23.

105. Fındık, O. (2004). *Şifrelemede kaotik sistemin kullanılması*. Yüksek Lisans Tezi, Selçuk Üniversitesi Fen Bilimleri Enstitüsü.

106. Okumuş, İ. (2012). *RSA Kriptosisteminin hızını etkileyen faktörler / The factors affecting speed of the RSA cryptosystem*. Doktora Tezi, Atatürk Üniversitesi Fen Bilimleri Enstitüsü.

107. *Kuantum bilgisayarı*. (2022). Vikipedi. https://tr.wikipedia.org/wiki/Kuantum_bilgisayarı

108. Atkins, W. (2004). *Market Trends and Output 2003-2006*. The Smart Card Report, 3.

109. FIlali, K., *Shor's algorithm in C++*. (2020). https://medium.com/@kfila1/shors-algorithm-in-c-52920e8f4f1c

110. Gershenfeld, N., Chuang, I. L. (2017). Quantum Computing with Molecules. *Scientific American*.

111. *How the Crypto World Is Preparing for Quantum Computing, Explained.* (2020). https://cointelegraph.com/explained/how-the-crypto-world-ispreparing-for-quantum-computing-explained

112. Tan, X. Q. (2013). *Introduction to quantum cryptography. Theory and Practice of Cryptography and Network Security Protocols and Technologies*

113. Montanaro, A. (2016). *Quantum algorithms: an overview*. Quantum Information, 2(1), 1-8.

114. *Post-quantum cryptography*. (2020). Computer Security Resource Center. https://csrc.nist.gov/Projects/post-quantum-cryptography

115. *Madencilik havuzu nedir?*. Web Kripto Madencilik. (2022). https://webkripto.com/madencilik-havuzu-nedir/

116. Korkmaz, T., Çevik, E. İ., Uygurtürk, H. (2017). Spot ve Vadeli Piyasalar Arasında Risk Durumunda Nedensellik İlişkisi, *Hitit Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 737-756.

117. *Spot Piyasa Nedir?*. (2022). BTC Turk. https://www.btcturk.com/bilgi-platformu/spot-piyasa-nedir

118. *Spot İşlemler Ne Demek?*. (2022). İltem. https://iltem.gen.tr/spot-işlemler-ne-demek/

119. *Spot Market Nedir?*. (2022). Spot Pazar. https://tr.know-base.net/7578485-spot-market

120. *Spot Piyasa Nedir ve Spot Alım Satım Nasıl Yapılır?*. (2021). Binance Academy. https://academy.binance.com/tr/articles/what-is-a-spot-market-and-how-to-do-spot-trading

121. *Spot Satış Nedir, Nasıl Yapılır?*. (2021). Favorim Teknoloji Haberleri. https://favorim.net/spot-satis-nedir-nasil-yapilir/

122.Kayalıdere K., Aracı H., Aktaş H. (2012). Türev ve Spot Piyasalar Arasındaki Etkileşim: VOB Üzerine Bir İnceleme. *Muhasebe ve Finansman Dergisi*.

123. Kripto Spot Alım Satım vs. Marj Alım Satım- Fark nedir?. (2021). Binance Trader. https://binantrader.com/tr/kripto-spot-alim-satim-vs-marj-alim-satim-fark-nedir-05131938

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

ÖZGEÇMİŞ

Nurlan HUSEYNLİ, orta öğrenimini Azerbaycan'ın Bakü Şehri Sabunçu Rayonu Rixard Zorge adına 90 numaralı tam orta okulda tamamladı. 2015 yılında Karabük Üniversitesi İktisadi ve İdari Bilimler Fakültesi İşletme Bölümünde öğrenime başlayıp 2019 yılında mezun oldu. Yüksek lisans eğitimine ise 2019 yılında Karabük Üniversitesi Lisansüstü Eğitim Enstitüsünde Finans ve Katılım Bankacılığı anabilim dalında görmektedir. 2018 yılından itibaren bölümü ile entegre olmak üzere Blokzin ve kripto paralar üzerine çeşitli araştırmalar gerçekleştirdi. 2020 yılında Karabük'te çalıştığı mali müşavirlik bürosunda muhasebe ve finans alanlarında staj eğitimini görürken 2021 yılında ise Nur Demir Çelik Şirketinde finans alanında tamamladı.