ATOMİK TAKAS YÖNTEMİ İLE MERKEZİ OLMAYAN KRİPTO-PARA MODELİ VE BORSASI

Hüseyin Ergün
151450201

DOKTORA TEZİ
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Doktora Programı
Danışman: Prof. Dr. Mesut Razbonyalı

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Aralık, 2021

ATOMİK TAKAS YÖNTEMİ İLE MERKEZİ OLMAYAN KRİPTO-PARA MODELİ VE BORSASI

Hüseyin Ergün
151450201
Orcid: 0000-0003-1203-8308

DOKTORA TEZİ
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Doktora Programı
Danışman: Prof. Dr. Mesut Razbonyalı

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Aralık, 2021



JÜRİ VE ENSTİTÜ ONAYI

Bu belge, Yükseköğretim Kurulu tarafından 19.01.2021 tarihli *"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"* ile bildirilen 6689 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

ETİK İLKE VE KURALLARA UYUM BEYANI

Bu belge, Yükseköğretim Kurulu tarafından 19.01.2021 tarihli *"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"* ile bildirilen 6689 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

TEŞEKKÜR

Her türlü bilgi birikimini benimle paylaşan ve akademik çalışmalarımda değerli katkıları ile her zaman kılavuz olan saygı değer danışmanım; Sayın Prof. Dr. Mesut Razbonyalı'ya teşekkürlerimi sunarım. Çalışmam sırasında önerileriyle bana her zaman destek olan, tez izleme komitesi üyeleri; Sayın Dr. Öğr. Üyesi Erdal Güvenoğlu ve Sayın Dr. Öğr. Üyesi Can Razbonyalı'ya çok teşekkür ederim. Ayrıca tez savunma jürisi üyeleri; Sayın Dr. Öğr. Üyesi Fatih Yücalar ve Sayın Dr. Öğr. Üyesi Emin Borandağ'a teşekkür ederim.

Lisans eğitimimde Bilgisayar Mühendisliği Bölümü'ne ilgi duymamı sağlayan, beni bu bölümü seçmeye teşvik eden ve bu alanda gelişimime destek olan hocalarım Sayın Kemal Oflazer, Sayın Hüsnü Yenigün, Sayın Erkay Savaş, Sayın Yücel Saygın, Sayın Berrin Yanıkoğlu ve Sayın Kemal İnan'a teşekkürü borç bilirim.

Son olarak, doktora çalışmam sürecinde göstermiş oldukları destek için kıymetli aileme en içten teşekkürümü sunarım.

Look Mama! I'm on TV!

Hüseyin Ergün

Aralık, 2021

ÖZ

ATOMİK TAKAS YÖNTEMİ İLE MERKEZİ OLMAYAN KRİPTO-PARA MODELİ VE BORSASI

Hüseyin Ergün
Doktora Tezi
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Doktora Programı
Danışman: Prof. Dr. Mesut Razbonyalı
Maltepe Üniversitesi Lisansüstü Eğitim Enstitüsü, 2021

Elindeki bir malı başka bir şeyle takas yapmak isteyen herkes üç şeyi arzular: en uygun orandan takas yapmak, en az masrafla takas yapmak, takas sırasında hırsızlık ve dolandırıcılığa maruz kalmamak. Kripto-paralar arası takas da herhangi iki varlığın takasından farksızdır. Borsalarının 7 / 24 açık ve programlanabilir para olması sebebiyle kripto-paralar gün geçtikçe ilgi çekmektedir. Kullanım sırasında karşılaşılan zorluklar ve alınan riskler değerlendirildiğinde, dünyadaki tüm kripto-para çevrelerinde bizim beklentilerimize benzer beklentiler olmasına rağmen; piyasalarda bu beklentileri karşılayan bir borsanın olmaması araştırmanın problemi olarak tanımlanmıştır.

Tezin amacı, özel blok-zincir teknolojisi, atomik takas yöntemi ve ödeme kanalları teknolojisini kullanarak piyasadaki büyük merkezi borsalar kadar iyi oranların olduğu; kripto-para kullanıcılarının mevcut borsalardaki risklere girmeden en az masraf ödediği; hileye maruz kalma, hırsızlık ve dolandırıcılığın mümkün olmadığı; mevcut borsaların sağladığı tüm imkanlardan faydalanabildiği, merkezi olmayan bir kripto-para borsası modeli tasarlamaktır.

Merkezi borsalarda kullanıcılar takas yapabilmek için önce sahip oldukları kripto-paraları borsanın kendi hesabına gönderirler. Bu da tüm kullanıcıların kripto-paralarının tek bir havuzda toplanması sonucunu doğurur. Bu tez kapsamında üretilecek olan model ile kullanıcıların kripto-paraları takas gerçekleşene kadar kendi sahip olduğu cüzdanlarda beklemesi sağlanacak ve merkezi hileye maruz kalma tehlikesi ortadan kalkacaktır. Bu tez çalışmasının özgünlüğü Atomik Takas ve Ödeme Kanalları teknolojilerini birleştirerek merkezi borsalar kadar likit merkezi olmayan borsa modeli oluşturmaktır.

Anahtar Sözcükler: Blok zincir; Kripto-para; Merkezi Olmayan Kripto-para Borsası; Kripto-paralar Arası Atomik Takas; Kripto para Ödeme Kanalları.

ABSTRACT

DISTRIBUTED CRYPTO CURRENCY EXCHANGE MARKET MODEL WITH ATOMIC SWAP

Hüseyin Ergün
PhD Thesis
Department of Computer Engineering
Computer Engineering Programme
Thesis Advisor: Prof. Dr. Mesut Razbonyalı
Maltepe University Graduate School, 2021

Anyone who wants to trade something in his possession with something else desires three things: To trade at the most appropriate rate, to trade at the least cost, not to be exposed to theft and fraud during the clearing. The cryptocurrency swap is also no different from swapping of any two entities. Crypto-currencies are getting more and more attractive day by day because their stock exchanges are open 24/7. Although all crypto-money markets in the world have similar expectations, existing market models have difficulties and risks while operating on them. The problem of this research is centralized exchange markets and risks while operating on them.

The study aims to develop a distributed exchange model on blockchain using smart contracts for atomic swap method, and payment channels technology for liquidity. With this model, users will pay less without taking risks of centralized exchange markets, like hacking, theft and fraud.

In central exchanges, users first send their cryptocurrencies to the stock exchange's account to trade. This results in collection of all cryptocurrencies of users in a single pool. With this model, users will be allowed to wait in their wallets until the cryptocurrency is exchanged, and the risk of central hacking will be eliminated. Original contribution of this study to the literature is to combine Atomic Swap and Payment Channels technologies to create a liquid decentralized stock market model as much as central exchanges.

Keywords: Block-Chain; Crypto currency; Distributed Cryptocurrency Market; Atomic Swap Between Cryptocurrencies, Cryptocurrency Payment Gateway.

İÇİNDEKİLER

JÜRİ VE ENSTİTÜ ONAYI ii
TEŞEKKÜR iv
ÖZ v
ABSTRACT vi
İÇİNDEKİLER vii
TABLOLAR LİSTESİ ix
ŞEKİLLER LİSTESİ x
KISALTMALAR xi
ÖZGEÇMİŞ xii
BÖLÜM 1. GİRİŞ 1
1.1. Problem 2
1.2. Amaç 2
1.3. Önem 3
1.4. Varsayımlar 4
1.4.1. Kişilerin Riskleri Finans Sektöründe 3. Kişilerin Devreden Çıkarılması 4
1.4.2. Teknik Başarısızlık 4
1.4.3. Güven Boşluklarını Doldurma 5
1.4.4. Kağıt Sistemi 6
1.4.5. Teknoloji Güven Kozu 6
1.5. Sınırlıklar 7
BÖLÜM 2. LİTERATÜR ARAŞTIRMASI 8
2.1. Kripto Paralar 8
2.2. Kripto Paralar'ın Tarihçesi 10
2.3. Kripto Para Piyasası 11
2.4. Bitcoin ve Bitcoin Blok Zinciri Tarihçesi 13
2.5. Bitcoin Teknolojileri 16
2.6. Blok Zincir Uygulamaları 19
2.7. Kriptografik Hash Fonksiyonları 21
2.8. Uçtan Uca İletişim 27
2.9. Cüzdan 28
2.10. İşlemler 31

2.11. İşlem Zamanlayıcıları ve İşlem Geçmişleri 34
2.12. Bölüm sonucu 38
BÖLÜM 3. YÖNTEM 39
3.1. Araştırma Modeli 39
3.2. Atomik Takas Örnek Senaryo 40
3.3. Bulgular 42
BÖLÜM 4. SONUÇ 50
EKLER 52
Ek 1. Uygulama Ekran Görüntüleri 52
KAYNAKÇA 56

TABLOLAR LİSTESİ

Tablo 2.1.: Dağıtık ve Merkezi Zincir Kıyaslaması..... 9

Tablo 2.2.: Blok- zincir teknolojilerinin karakteristik özellikleri..... 10

Tablo 2.3.: Blok- zincir Teknoloji Uygulamaları..... 20

Tablo 2.4.: İşlemlerin ACID özellikleri..... 33

Tablo 3.5.: Ödeme Kanallarında Kullanılan Atomik Takas Yapısı Formülü……. 47

Tablo 3.2.: Piyasa Yapıcı, Normal Kullanıcı ve Kanal Sağlayıcı arasındaki takas ilişkisi formülü……... 49

ŞEKİLLER LİSTESİ

Şekil 1.1 Merkezi ve Dağıtık Sistemlerin Farkı…..... 6

Şekil 2.1. Blok zincir çalışma modeli …..... 18

Şekil 2.2. Blok zincir teknolojilerinin geniş kullanımı …..... 21

Şekil 2.3. Kriptografik hash fonksiyonu çalışma modeli…..... 22

Şekil 2.4. Açık anahtar şifreleme çalışma modeli …..... 23

Şekil 2.5. Dijital imza ile imzalanmış dokümanın kontrol ve onay süreci …..... 24

Şekil 2.6. İlgili teknolojiler bağlamında fonksiyonlar ve kazanımlar …..... 24

Şekil 2.7. İş ispatı algoritmasında hash hesaplamaları …..... 27

Şekil 2.8. Bitcoin ağı ile işlem oluşturma süreci …..... 32

Şekil 2.9. Çift işlem doğrulama Sistemi …..... 37

Şekil 3.1. Atomik Takas Senaryo …..... 41

Şekil 3.2. Atomik Takas Senaryo …..... 42

KISALTMALAR

API : Application Programming Interface

FX : Forex

FOREX : Foreign Exchange – Kambiyo

ECDSA : Elliptic Curve Digital Signature Algorithm

RDBMS : Relational Database Management System – İlişkisel Veritabanı Yönetim Sistemi

SQL : Structured Query Language – Yapılandırılmış Sorgu Dili

ACID : Atomicity, Consistency, Isolation, and Durability – Atomiklik, Tutarlılık, İzolasyon, Devamlılık

BTC : Bitcoin

P2P : Peer to Peer – Uçtan uca

ANSI : American National Standards Institute – Amerikan Ulusal Standartlar Enstitüsü

TCP : Transmission Control Protocol – İletim Kontrolü Protokolü

ÖZGEÇMİŞ

Hüseyin Ergün

Bilgisayar Mühendisliği Anabilim Dalı

Eğitim

Derece Yıl	*Üniversite, Enstitü, Anabilim / Anasanat Dalı*
Y.Ls.	2008 Işık Üniversitesi, Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı
Ls.	2004 Sabancı Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi Bilgisayar Mühendisliği Bölümü
Lise	1999 Ümraniye Anadolu Lisesi

İş/İstihdam

Yıl	*Görev*
2020 - ……	SSH Bilgi Teknolojileri, Kurucu Ortak.
2016 - ……	Finartz Bilgi Teknolojileri, Kurucu Ortak.
2015 - ……	FBT Finansal Bilgi Teknolojileri, Kurucu.
2013 - ……	Infonal Bilgi Teknolojileri, Kurucu Ortak.
2004 - 2012	OBSS Teknoloji, Kurucu Ortak.

Mesleki Birlik/Dernek Üyelikleri

Yıl	*Kurum*
2004 -	Linux Kullanıcıları Derneği
2007 -	Türkiye Bilişim Derneği

Alınan Burs ve Ödüller

Yıl	*Burs/Ödül*
1999	Sabancı Üniversitesi Eğitim Bursu

Yayınlar ve Diğer Bilimsel/Sanatsal Faaliyetler

"Atomik Takas Yöntemi ile Merkezi Olmayan Kripto-Para Modeli ve Borsasi" Int. Journal of Engineering Research and Application. 11(4), 2020.

BÖLÜM 1. GİRİŞ

Merkezi borsalarda kullanıcılar takas yapabilmek için önce sahip oldukları kripto-paraları borsanın kendi hesabına göndermektedirler. Bu da tüm kullanıcıların kripto-paralarının tek bir havuzda toplanması sonucunu doğurmaktadır (Raval, 2016) ve söz konusu durum hilekarlar için bir ilgi odağı haline gelmektedir. Tarihte neredeyse tüm merkezi borsalar çeşitli büyüklüklerde hile yapma vakalarıyla karşılaşmışlardır (Street vd., 2010). Sürekli yeni borsa açılması nedeniyle tam bir oran vermek mümkün olmamakla birlikte, tarihteki en büyük hile yapma olayı, 2014 yılında daha önce de birçok kez hileye maruz kalan MtGox adlı borsada yaşanmıştır. Bu hileye yapma olayı kapsamında o gün için piyasa değeri 473 milyon dolar (wikipedia.org/wiki/Mt._Gox) olan 750 bin bitcoin (tüm bitcoinlerin %7'si) hileye maruz kalmıştır. Bu olay MtGox borsasının iflasına yol açmıştır. Bu tür dolandırıcılık olaylarının oluşturduğu riskten yola çıkarak, tez çalışmasının ortaya koyduğu modelde kullanıcıların kripto-paraları takas gerçekleşene kadar kendi sahip olduğu cüzdanlarda bekletmesi önerilmektedir. Böylece merkezi hileye maruz kalma tehlikesinin olmayacağı öngörülmektedir (Hoben, 2018).

Merkezi olmayan borsalarda, kripto-paralar takas anına kadar kullanıcının kendi cüzdanında olduğundan dolayı bu süreçte hileye maruz kalma, kurum içi ya da dışı hırsızlık ve dolandırıcılık gibi olayların gerçekleşmesi mümkün değildir (Goodman, 2014). Bunun yanı sıra mevcut merkezi olmayan borsalarda likidite problemi vardır. Likidite problemi, belirli bir miktar kripto-para almak istenildiğinde yüksek fiyat, satmak istenildiğinde düşük fiyattan işlem görmesi olarak tanımlanır ve bu durum fazla alıcı-satıcı olmamasından kaynaklanmaktadır. Merkezi olmayan borsalarda tüm takas işlemleri gerçek kripto-para transferi işlemidir. Bu sebeple her takas yapıldığında borsa komisyonu hariç blok zincirdeki komisyonu da ödemek zorunda kalınmaktadır. Bu durum piyasa yapıcı ve kısa vadeli hareketlerden kar etmeyi amaçlayan ve borsalara likidite sağlayan kullanıcı tipi olarak tanımlanan yatırımcıların bu tip borsalardan uzak durmasına sebep olmaktadır (Greene, 2018).

Bu tez çalışması ile ödeme kanalları teknolojisi ve kanal sağlayıcı yatırımcılar vasıtasıyla likidite probleminin çözülmesi amaçlanmaktadır. Proje aşamasındaki merkezi olmayan borsalarda ise şimdiye kadar paylaştıkları bilgiler ışığında likidite problemini

merkezi borsalar kadar iyi çözemeyecekleri öngörülmektedir. Bu tez çalışmasının özgünlüğü; Atomik Takas ve Ödeme Kanalları teknolojilerini birleştirerek merkezi borsalar kadar likit merkezi olmayan borsa modeli ortaya koyuyor olmasıdır.

1.1. Problem

Merkezi kripto-para borsalarında komisyon oranı ortalama olarak yapılan takasın %0,2'si kadardır. Merkezi borsalar kullanıcıların kripto-paralarını da kendi bünyelerinde tuttuklarından bunların transferleri ve güvenli saklanması konusunda birçok masraf ortaya çıkmaktadır.

Kripto-paralar üzerinde stratejiler geliştirilmekte ve kripto-para borsalarının API'leri kullanılarak bu borsalarda algoritmik alım satım yapılmaktadır. Kullanım sırasında karşılaşılan zorluklar ve alınan riskler değerlendirildiğinde, dünyadaki tüm kripto-para çevrelerinde beklentilerimize benzer beklentiler olmasına rağmen; piyasalarda bu beklentileri karşılayan bir borsanın olmaması bu çalışmanın problemi olarak tanımlanmaktadır.

1.2. Amaç

Proje aşamasındaki merkezi olmayan borsalarda ise şimdiye kadar paylaştıkları bilgiler ışığında likidite problemini merkezi borsalar kadar iyi çözemeyecekleri öngörülmektedir. Daha önceki süreçte Hoben (2018) ve Greene (2018) tarafından tanımlanan likidite probleminin, ödeme kanalları teknolojisi ve kanal sağlayıcı yatırımcılar vasıtasıyla bu tez çalışmasında sunulan modelle çözülmesi amaçlanmaktadır.

Borsaların verileri açık olarak paylaşmadıkları için tam bir oran vermek mümkün olmamakla birlikte, masrafların yaklaşık olarak %90'ının hileye maruz kalma ve dolandırıcılık gibi sebepten kaynaklandığı söylenebilir. Özel blok zincir temelli merkezi olmayan bir borsada, masraf sadece blok zincirin erişilebilir tutulması ve yeni veri eklenmesi işinin sürdürülebilmesi kadardır. Özel blok zincir temelli merkezi olmayan bir borsada çok daha düşük, tahmini %0,02 gibi komisyonla çalışılması ve böylece daha çok kullanıcının sistemi kullanması öngörülmektedir. Toplam pazar payı 200 milyar dolar olan kripto-paralarda günlük takas hacmi 10 milyar dolarları bulabilmekte ve bu hacim kripto-paralar

yaygınlaştıkça artmaktadır. Bu takaslardan alınan komisyonların bir kısmının ülkemize çekilmesi ise tez çalışmasının hedefleri arasındadır.

Bu tezin amacı, özel blok zincir teknolojisi, atomik takas yöntemi ve ödeme kanalları teknolojisini kullanarak piyasadaki büyük merkezi borsalar kadar iyi oranların olduğu; kripto-para kullanıcılarının mevcut borsalardaki risklere girmeden en az masraf ödediği; hileye maruz kalma, hırsızlık ve dolandırıcılığın mümkün olmadığı; mevcut borsaların sağladığı tüm imkanlardan yararlandığı, merkezi olmayan bir kripto-para borsası modeli ortaya koymaktır.

1.3. Önem

Bu tez çalışması kapsamında ortaya konulan model ile sağlanacak ulusal kazanımlar;

a. Ülkemizdeki teknolojinin ve Türkçe dilindeki blok zincir alanındaki bilgi birikiminin artırılması,

b. Sanayi işbirliği ile ürüne dönüşme potansiyelinin olması ve bu teknoloji alanında Ar-Ge projesi yapma imkanı,

c. Hali hazırda patent için hazırlıkların yapılmış olup patent ve faydalı model başvurusu yapılma imkânı,

d. Çıkacak olan ürün sayesinde girişimci firmaların kurulmasına imkan vermesi ve istihdam artırma potansiyeli,

e. Bilişim, kriptoloji, blok zincir gibi sektörlere katkısının bulunması,

f. Projenin ve çıktılarının sosyo-kültürel hayata etkisi, eğitim, sağlık, bölgeler arası gelişmişlik farkını azaltma gibi konularda iyileşme sağlama potansiyeli,

g. Projenin sonuçlarının maliyet düşürücü etkisinden dolayı sosyo-kültürel hayata olumlu etkilerinin olması,

h. Kullanıcıların kripto-paraları takas gerçekleşene kadar kendi sahip olduğu cüzdanlarda bekletilmesi sağlanacak ve merkezi hileye maruz kalma tehlikesinin ortadan kalkması olarak sıralanabilir.

Ayrıca, atomik takas ve ödeme kanalları teknolojilerini birleştirerek merkezi borsalar kadar likit merkezi olmayan borsa modeli oluşturulması tez çalışmasının özgünlüğü olarak düşünülebilir.

1.4. Varsayımlar

Tez çalışması kapsamında bazı varsayımlar ile hareket edilmiştir. Bunlar "Kişilerin Riskleri- Finans Sektöründe Üçüncü Kişilerin Devreden Çıkarılması, Teknik Başarısızlık, Güven Boşluklarını Doldurma, Kağıt Sistemi ve Teknoloji Güven Kozu" olmak üzere 5 başlık altında sunulmuştur.

1.4.1. Kişilerin Riskleri Finans Sektöründe 3. Kişilerin Devreden Çıkarılması

Finans sektörü yoğun olarak güvenilir üçüncü kişilere dayanmaktadır. Takas evleri, merkezi karşı taraflar, hisse senedi ve vadeli işlem borsaları gibi varlıklar, birbirlerine tam olarak güvenmeyen ancak birlikte çalışması gereken finansal kurumlar arasındaki riski azaltmak için konumlanmışlardır. Bu gibi üçüncü kişilerin sürece eklenmesi ise yeni sorunlara sebep olmaktadır (Radivojak & Grujic, 2019).

1.4.2. Teknik Başarısızlık

Bazı durumlarda üçüncü kişiler, tek bir potansiyel başarısızlık noktası haline gelebilmektedir. Teknik arızalar oluşabilmekte ya da merkezi etkiler söz konusu olabilmektedir. Örneğin; Ekim 2014'te, İngiltere'de günde 275 milyar sterlin değerinde yüz binlerce ödeme işlemini temizlemekten sorumlu "Gerçek Zamanlı Brüt Uzlaşma" ödeme sistemi 10 saat boyunca çalışmadığında, önemli ödemeler gecikmiş ve büyük sorunlar ortaya çıkmıştır. Yaşanılan bu durum ise bağımsız bir gözden geçirme mekanizması gereksinimini ortaya çıkarmıştır. Alıcının ve satıcıların buluştuğu merkezi varlıklar olan borsalarda buna benzer sorunların meydana gelmesi olasıdır. Bu süreç müşterileri risk altında bırakırken, yapılan işlemlerin durumu hakkında geçici olarak güvenilmeyen durumların ortaya çıkmasına neden olmaktadır. Böyle bir duruma verilebilecek bir diğer örnek de 2015 yılının Temmuz ayında New York Borsası'nın bir yazılım hatası nedeniyle 3 saatten daha uzun bir süre çalışmaması ve bu sürecin neden olduğu kayıplardır (Popper, 2015).

Değerli verilerin yoğunluğu, üçüncü kişileri hem verileri yeniden satmaya hem de sistemlere zarar vermeye yönelik çekici bir hedef haline getirmiştir. Şirket içi çalışanlar, veri ve sistemlere ayrıcalıklı erişim hakkına sahip oldukları için dış hilekarlar gibi şirket içi çalışanlar da üçüncü kişiler için risk oluşturmaktadır. Bu güvenlik eksiğinin oluşturduğu risk, teknik bir başarısızlık sayılmaktadır (Musonera & Vincent, 2008).

Çoğu zaman takas sektörünün üçüncü kişileri tekelleşmiş ve alternatifi olmayan katılımcılardır. Bu nedenle, köklü sanayi kuruluşlarının rekabetçi fiyatlar sunmak ve üstün müşteri deneyimi üretmek için gerçek bir nedenleri yoktur ve uygulamalı yeniliğe yönelik çaba göstermeye ihtiyaç duymamaktadırlar. Örneğin, ödemeler ile ilgili mesajlar göndermek için kullanılan bir bankalar arası mesajlaşma ağı ve standartlaşma şeması olan SWIFT, bankacılık sektöründe gerçek bir rekabetin olmadığının kanıtıdır. Benzer şekilde, CLS (uzman bir ABD finans kurumu) FX (Forex) işlemlerinde fiili takas mekanizması olup ve birçok ülke hisse senedi işlemleri için takasbank kullanmaktadır. Bu gibi güvenilen üçüncü kişilerin her biri, işlevleri için yarı-tekel olarak hareket etmektedir (Destais, 2014).

Uluslararası üçüncü kişiler, her bir tarafın bir işlemin bulunduğu yargı alanlarından farklı olabilecek bir yargı yetkisine sahip olduklarından, bu durum yeni bir yasal risk unsuru olarak ortaya çıkmaktadır. Üçüncü kişilere güven, güç ve denetimin verilmek istenmemesinin bu gibi risk unsurları vardır. Bu risk durumlarından ayrı olarak dağıtılmış defterlerin (distributed ledger) uzlaşma potansiyeli, üçüncü kişilerin sistemden çıkarılabilme olasılığına fırsat sunmaktadır. Dağıtılmış defterler sayesinde üçüncü kişiler sistemden çıkarıldığında dahi katılımcıların verimli sonuçlara ulaştığı görülmektedir (Locher vd., 2018).

1.4.3. Güven Boşluklarını Doldurma

Bir önceki başlıkta belirtilen böyle bir güven sorunu ortamında blok zincirler, birbirlerine tam olarak güvenmeyen ve tek bir olay üzerinde anlaşmaya ya da manipülasyona karşı korumalı bir veri kaynağına gereksinim duyan nesnel varlıklar için ideal çözümlerdir (Gervais vd., 2016).

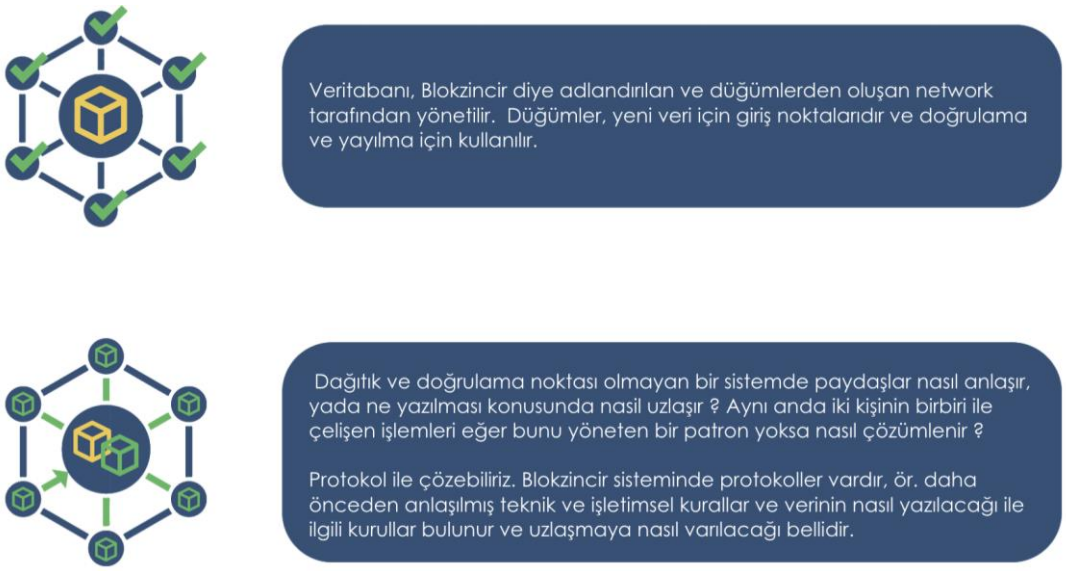
1.4.4. Kağıt Sistemi

Kâğıt belgeler tarih boyunca güven sağlanması gereken ortamlarda güvenin yerine kullanılmıştır. Örneğin, geçmişte tüccarın sözüne güvenmek yerine, tüccarın verdiği orijinallik sertifikasına güvenilmekteydi. Ancak zaman içinde teknolojinin gelişmesiyle birlikte, kopyalama ve çoğaltma imkanları artmış ve kağıt belgelerin çoğaltılması ya da kopyalanması riski ortaya çıkmıştır. Islak imzalı kağıt belgelerin kopya ve çoğaltma riskine karşı dijital imza geliştirilmiş ve dijital imzalı belgeler kullanılmaya başlanmıştır. Blok zincirler, özgünlüğü temsil eden ve gizliliği koruyan orijinallik kayıtlarını dijital ortamda oluşturabilme fırsatı sunmaktadır (Lemieux, 2017).

1.4.5. Teknoloji Güven Kozu

Dijital kayıtların tek bir varlık tarafından merkezi olarak saklandığı durumlarda varlığa olan güven düşükse ya da üçüncü tarafın kayıtlara müdahale edilemez olduğunu ispatlaması gerekiyorsa blok zincirler bu durumlarda çözüm aracı olarak kullanılabilir. Eğer bir blok zincir üzerinde veriye sahip olunuyorsa, bu bir önceki zincirdeki matematiksel güvenin kabul edilerek doğruladığının göstergesidir (Meijer, 2017).

Genel olarak tüm bu varsayımlar blok zincir desteği ile dağıtık bir sistemin kurulması üzerine tasarlanmıştır. Şekil 1.1'de bu çalışmanın da odak noktası olan merkezi ve dağıtık sistemlerin farkı sunulmuştur.



Şekil 1.1. Merkezi ve Dağıtık Sistemlerin Farkı

1.5. Sınırlıklar

Atomik takas modeli sürecinde kullanılan bazı teknolojiler alternatifleri ile karşılaştırıldığında avantajların yanında bazı sınırlılıkları da yanında getirmektedir. Merkezi olmayan sistemler, birden çok sunucu sistemin haberleşmesine dayalı bir altyapıya sahip olmalarından dolayı, ağ gecikmesine sahiptirler. Bu sebeple merkezi olmayan sistemler merkezi ve tek işlemci içerisinde çalışan sistemlere göre daha yavaş hareket etmektedirler. Bunun yanı sıra sistemlerin bağlı bulundukları blok zincir teknolojilerinin kriptoloji standartlarını uygulamaları gerekmektedir. Yaygın kullanılan farklı kriptoloji teknolojileri arasında seçim yapıldığı için güvenlik konusunda olumsuz bir etkisi olmasa dahi, kullanılan sistemlerin dışına çıkılamamaktadır.

BÖLÜM 2. LİTERATÜR ARAŞTIRMASI

Bu bölümde, dağıtık atomik takas sisteminin temel kavramları olan teknolojiler ve güncel durumları açıklanmıştır. Dağıtık takas sisteminin temelini oluşturan kripto para yapıları, bu sistemlerin tarihsel gelişimi, kripto paranın alt yapısını oluşturan blok zincir ve açık anahtar şifreleme, hash fonksiyonları gibi kriptoloji teknolojileri anlatılmıştır. Bu bölümde sözü edilen teknolojilerin uygulama alanı bulduğu, kriptolojik para cüzdanı ve bu cüzdanlar üzerinde işlemlerin (transaction) tanımlandığı alt yapılar ile ilgili literatür bilgisi verilmiştir.

2.1. Kripto Paralar

Kripto para birimi, işlemleri güvenceye almak ve para birimine ilişkin ek birimlerin oluşturulmasını kontrol etmek için kriptografi kullanan bir değişim aracı olarak çalışır. Kripto paralar dijital varlıklardır. Kripto para birimleri; dijital para birimleri, alternatif para birimleri ve sanal para birimlerinin bir alt kümesi olarak sınıflandırılabilir (And Greenberg, 20 Nisan 2011; “Kripto Para Birimi”. Forbes.com 8 Ağustos 2014).

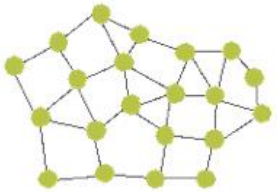
En popüler kripto para olarak kabul edilen Bitcoin, 2009 yılında ilk merkezi olmayan kripto para olarak piyasaya sunulmuştur (bitguru.co.uk, 2017). O zamandan günümüze, çok sayıda kripto para sistemi oluşturulmuştur (Tasca, 2015). Bu alternatif para birimleri genellikle “altcoins” olarak adlandırılmakta ve bitcoinin alternatif türevleri olarak işlem görmektedir (Wilmoth, 2014). Kripto paralar, merkezi bankacılık sistemlerinin tam tersine dağıtılmış bir sistemde kullanılırlar. Bu durumun sebebi ise kripto paraların blok zincir işlem veri tabanını kullanmasıdır (Allison, 2015).

Merkezi olmayan kripto para birimi; kripto para birimi sistemi tarafından, sistem oluşturulduğunda ve herkes tarafından bilinen bir zamanda, tanımlanan bir oranda, toplu olarak üretilmektedir. Merkez Bankası ve Federal Rezerv Sistemi gibi merkezi ekonomik sistemlerde; şirket yönetim kurulları ya da hükümetler, yeni para basmak ya da basılmasını talep etmek durumundadırlar. Merkezi olmayan kripto para birimlerinde; şirket yönetim kurulları ya da hükümetler, yeni paralar üretemezler ve o sırada mevcut paraya sahip olan firmaların, bankaların ya da kurumsal kuruluşların desteklenmesini sağlarlar. Dağıtılmış

kripto para birimlerinin temel aldığı teknik sistem, Satoshi Nakamoto olarak bilinen grup ya da birey tarafından oluşturulmuştur (theeconomist.com, 2016; Nakamoto, 2009).

Dağıtık ve merkezi zincirlerin bakım maliyeti, doğrulama maliyeti, şeffaflık ve güvenlik bağlamında kıyaslanması Tablo 2.1'de verilmiştir.

Tablo 2.1. Dağıtık ve Merkezi Zincir Kıyaslaması

	 Dağıtık Zincir	 Merkezi Zincir
Bakım Maliyeti: Blok zincir'in bakım ve işletim maliyeti, işlemlerin doğrulanması ve zincire eklenmesi dahil	$$$	$
Doğrulama Maliyeti: Üçüncü güvenilir kişiye sahip olma maliyeti	$	$$$
Şeffaflık: Tüm paydaşların işlemleri görme şeffaflığı	✓ ✓ ✓	✓
Güvenlik: Doğru olmayan bir işlem gerçekleştirme zorluğu	✓ ✓	✓

Dağıtık sistemlerin dayandığı blok zincir teknolojisinin karakteristik özelliği Zhu ve Zhou (2016) tarafından ortaya konulmuştur. Tablo 2.2'de blok zincir teknolojilerinin karakteristik özellikleri verilmiştir.

Tablo 2.2. Blok zincir teknolojilerinin karakteristik özellikleri

Karakteristiği	Açıklama
Dağıtık zincir ve şeffaflık	Açık ve şeffaf işlem listesi ağdaki her paydaşın işlemlere erişimini ve sistemin şeffaflığını sağlamaktadır.
Merkezi olmayan veri yönetimi	Sistemdeki her paydaşın zincire yeni bir halka ekleme, bir diğer ifadeyle işlem gerçekleştirme yetkisi bulunmaktadır. Her paydaş sistem üzerinde diğerleri kadar hak sahibidir.
Veri güvenliği, dayanıklılık	Blok zincir sistemi bölünemez ve bütünlüğünü koruyan bir veri yapısına sahiptir. Sistemin merkezi olmayan yapısı, kötü niyetli insanlar tarafından değiştirilmesini ve bozulmasını engellemektedir.
Yüksek verimlilik	Bakiyelerin sorgulanması ve işlemin sonuçlandırılması, teorik olarak anlık gerçekleşebilir.
Merkezi çökme riski olmaması	Merkezi bir sistemin olmaması, veri kaybını, göçen bir merkezi sistemin oluşturacağı hasarları engeller.
Esnek ve güvenilir	Blok zincir sisteminin programlanabilir altyapısı farklı senaryoların gerçekleştirilmesine izin verir.

2.2. Kripto Paralar'ın Tarihçesi

İlk olarak Wei Dai, 1998'de "b-money"i dağıtılmış bir elektronik para sistemi olarak; bundan kısa bir süre sonra ise, Nick Szabo "BitGold"u oluşturmuştur. Bitcoin ve onu takip eden diğer kripto paralar gibi, BitGold da, kriptografik olarak bir araya getirilen ve yayınlanmış olan çözümlerle birlikte kullanıcıların çalışma fonksiyonunun bir kanıtını tamamlamalarını gerektiren elektronik para sistemi olarak tanımlanmaktadır. Daha sonra yeniden kullanılabilir bir iş ispatına dayanan bir para birimi, Dai ve Szabo'nun çalışmalarını takip eden Hal Finney tarafından piyasaya sunulmuştur (theeconomist, 2016).

İlk dağıtılmış kripto para olan Bitcoin, 2009 yılında Satoshi Nakamoto takma adlı yazılım geliştiricisi tarafından oluşturulmuştur (Nian & Chuen, 2015). İş ispatı olarak bir kriptografik özet sistemi (cryptographic hash system) olan SHA-256 kullanılmıştır (Brito & Castillo, 2013). "Bitcoin: A Primer for Policymakers" Nisan 2011'de Namecoin, internet

sansürünü çok zorlaştıran merkezi olmayan bir Alan Adı Sunucusu (Domain Name Server - DNS) oluşturma girişiminde bulunmuştur (Mercatus Merkezi, George Mason Üniversitesi, 2013). Kısa bir süre sonra, Ekim 2011'de, Litecoin yayınlanmış ve Bitcoin'in kullandığı SHA-256 yerine karma işlem dosyasını ilk başarılı kullanan kripto para olarak tarihe geçmiştir. Bir diğer önemli kripto para birimi olan Peercoin, kavram ispatı (proof of concept) ve ispat belgesini (certificate of proof) hibrit olarak kullanan ilk kripto para olma özelliği taşımaktadır. IOTA (MIOTA) para birimi, veri tabanı blok zincire dayanmayan ilk kripto paradır ve bunun yerine daha hızlı ve verimli olduğu düşünülerek Tangle kullanmaktadır (Sonstebo, 2016). Bu süreçte ortaya çıkan birçok kripto para birimi, yenilik getirmediği için başarısız olmuş ancak yine de pek çoğu piyasada talep görmüştür (Nian & Chuen, 2015). 2009 - 2018 arasında 720 adet kripto para oluşturulmuştur. Bitcoin, halen toplam kripto para piyasasının %81'ini temsil eden en büyük ve en popüler para birimidir (coinmarketcap.com, 2018). Tüm kripto para birimlerinin kombine piyasa değeri Mayıs 2018 itibariyle yaklaşık 330 milyar ABD dolarıdır. En popüler olan ilk 15 para birimi pazarın %97'sini temsil etmektedir. Bunun yanı sıra popüler kripto paraların ilk yedisi toplam piyasa kapitalizasyonunun % 90'ını oluşturmaktadır (Chan vd., 2017).

İngiltere hükümeti, Ağustos 2014'te kripto paralarla ilgili bir çalışma yapmak için hazinenin görevlendirildiğini ve İngiltere ekonomisinde hangi rolü oynayabileceğini araştıracaklarını açıklamıştır (theuknews, 2014). Bu açıklama kripto para borsalarının ve blok zincir teknolojilerinin devletlerin resmi olarak gündeminde olduğunun ifadesidir.

2.3. Kripto Para Piyasası

Piyasadaki aşırı tepkilere ve beraberinde getirdiği dalgalanmalara ilişkin çok sayıda çalışma olmasına karşın (De Bondt & Thaler, 1985; Brown vd., 1988; Atkins & Dyl, 1990; Bremer & Sweeney, 1991; Ferri & Min, 1996; Choi & Jayaraman, 2009; Mynhardt & Plastun 2013; Caporale vd., 2017) finansal piyasalar arasında kripto para piyasasına odaklanan herhangi bir çalışma bulunmamaktadır. Kripto para piyasasındaki ortalama günlük fiyat dalgalanması FOREX'e göre 10 kat, Amerikan borsasına göre 7 kat ve emtia piyasalarına göre 5 kat daha fazladır. Bu özellik kripto para piyasasını (çok genç bir pazar olduğu gerçeği ile birleştiğinde) olası aşırı tepkileri ve beraberinde gelişen dalgalanmaları

incelemek için özellikle çekici hale getirmektedir (Dwyer, 2014; Cheung vd., 2015; Carrick, 2016; Bartos, 2015).

Farklı kripto paralar için piyasa kapitalizasyon değerleri oldukça değişkendir. Bitcoin'in ardından ikinci sırada yer alan ve en büyük piyasa değeri, toplam dijital para piyasası kapitalizasyonunun yaklaşık %18'ine sahip olan Ethereum'dur. Ripple, üçüncü en büyük piyasa değeri olan dijital paradır ve toplam piyasa kapitalizasyonunun %7'sine sahiptir. Son zamanlarda kripto para piyasasına artan ilgi ile çok sayıda yeni kripto para piyasaya girmiştir (Alpago, 2018).

Altcoinlerin çoğu özellikle de Litecoin ve Peercoin gibi daha yeni olanlar-geliştiricilerinin Bitcoin'de görülen eksiklikleri düzeltmek için geliştirilmişlerdir. Bazı değişiklikler sadece çok dar bir kullanıcı grubunun ilgisini çekerken (örneğin, Namecoin, Bitcoin'den daha fazla anonimleştirmeyi hedefler), bazıları ise Bitcoin'e alternatif olarak daha çok ilgi görmektedir. Bununla birlikte, son zamanlarda dijital paralara olan ilginin ve dijital para piyasasına girişlerin artmasıyla birlikte piyasaya girişin nispeten maliyetli hale gelmesi ve madeni paraların kurucularının önemli karlar elde etmesi durumları ortaya çıkmıştır (Neil & Hanna, 2014).

Yeni kripto paraların (Bitcoin'in eksikliklerinin giderilmesi ve potansiyel popülerlikten faydalanılması) meydana getirilmesinde kripto paraya olan talebi yönlendiren şeylerin anlaşılamadığını gözler önüne sermek ve insanların potansiyelleri nedeniyle mi yoksa spekülatif amaçlar için mi dijital para satın aldıklarını ortaya çıkarmayı (ör. finansal varlık olarak) hedefleyen 2 temel motivasyon vardır (Vejacka, 2014). Bunlar takviye ve ikame etkisi olarak adlandırılmaktadır (Zhao, 2014). Takviye etkisi, para birimi benimseme sürecinde mevcut olan tek taraflı ağ etkilerinin bir sonucudur. Bitcoin daha popüler hale geldikçe, daha fazla insan "al-kazan" yarışında diğer kripto paralara yapacağı yatırıma oranla daha fazla kazanacağına inanacaktır. Bu beklenti ile talep daha da artacaktır. İkame etkisi ise spekülatif dinamiklerin bir sonucudur. Kripto para birimlerinin finansal varlıklar olarak ele alınması gerekliliği bulunmaktadır. Bitcoin daha popüler ve daha değerli hale geldikçe, insanlar aşırı değerli ya da çok değişken olabileceğinden ve alternatif bir kripto para birimi yatırımı arandığından korkmaktadırlar.

2.4. Bitcoin ve Bitcoin Blok Zinciri Tarihçesi

Satoshi Nakamoto “Bitcoin: A Peer-to-Peer Electronic Cash System,” başlıklı tezinde Bitcoin'i; güvenilir üçüncü şahıslara olan ihtiyacı ortadan kaldırarak doğrudan ve geri dönüşü olmayan işlemleri etkinleştiren, küçük rahat işlemlerde kredi maliyetini ve işlem ücretlerini azaltan, çift harcamaları önleyen özellikleri ile tanımlamıştır (Nakamoto, 2009).

İlk blok zincir Ocak 2009'da oluşturulmuş ve Bitcoin ile blok zincirinin çalışması başlatılmıştır. O zamandan beri, Bitcoin sistemi hiçbir zaman kesintiye uğramamış ve blok zincir sisteminin kullanıcıları sadece Amerika Birleşik Devletleri'nde değil, dünya çapında gün geçtikçe artmıştır. Japonya'da 2014'ün başlarında bir alım satım platformunun hileye maruz kalması kullanıcıların dikkatini çekmiş olsa da 2015 yılında FinTech için artan ivmeyle birlikte blok zincirlere olan ilgi giderek artmaktadır (Nassiry, 2018).

İlk merkezi olmayan kripto para birimi olan Bitcoin, 2009 yılındaki kuruluşundan bu yana medya, akademisyenler ve finans sektöründe önemli bir yer elde etmiş ve bu çevrelerde oluşan tartışmalarda sıklıkla yer almıştır. Bitcoin, blok zincir teknolojisine dayanarak, kripto paralar arasında liderliğini korumuş ve yavaşlama belirtisi göstermemiştir. Bitcoin, geleneksel güvene dayanmak yerine, kriptografik ispatlara dayanmaktadır. Geleneksel ödeme yöntemleri (Visa ve Mastercard gibi) para birimi, yüksek likidite, daha düşük işlem maliyetleri ve anonimlik gibi araçlara ihtiyaç duyarken kriptografik ispatlar geleneksel ödeme yöntemlerine göre pek çok avantaj sağlamaktadır (Chan vd., 2017).

BTC kısaltması ile ifade edilen Bitcoin'in çeşitli sembol ve logoları bulunmaktadır. Bitcoin, 8 basamağa kadar bölünebilir olmasından dolayı 0,00000001 Bitcoin'lik bir işlem yapmak dahi mümkündür. 0,00000001 Bitcoin'lik bu en küçük birime Satoshi denilmektedir. Başka bir deyişle, 100 Milyon Satoshi 1 BTC’e karşılık gelmektedir (Lansky, 2017).

Bir kripto para birimi olan Bitcoin’in popüler olmasının nedeni döviz kurları ile ilişkisi üzerine yapılmış çok fazla çalışma olmasıdır. Hencic ve Gourieroux (2014) modeli ve Cauchy hataları ile nedensel olmayan otoregresif bir süreci kullanarak ABD doları karşısında Bitcoin döviz kuru tahmininde bulunmuştur. Elde edilen sonuçlar, günlük Bitcoin/USD döviz kurunun, çevrimiçi işlemlerden spekülatif davranış dönemlerini gösteren yerel eğilimleri ifade ettiğini ortaya çıkarmıştır.

Sapuric ve Kokkinaki (2014), Temmuz 2010'dan Nisan 2014'e olan verilerle, büyük küresel para birimlerinin döviz kuru dalgalanması ile Bitcoin'i karşılaştırarak, Bitcoin'in dalgalanmasını araştırmıştır. Sapuric ve Kokkinaki'nin analizleri, Bitcoin'in döviz kurundan daha yüksek yıllık dalgalanmaya sahip olduğunu göstermekte ancak işlem hacmi dikkate alındığında daha istikrarlı sayılabileceğini ortaya koymaktadır.

Briere vd. (2015), çeşitli yatırım portföylerini analiz etmek ve bu süreçte Bitcoin'in aşırı derecede dalgalı olduğunu, önemli kazanç fırsatları sunduğunu ortaya çıkarmak amacıyla 2010 yılından 2013'e kadarki haftalık verileri kullanmıştır. Sonuçlar yatırım portföylerini çeşitlendirmeye yardımcı olsa da Bitcoin'in diğer varlıklar ile çok az ilintili olduğu çıktısına ulaşılmıştır.

Kristoufek (2015) Bitcoin'in fiyatını etkileyen faktörleri araştırmış ve Çin Bitcoin pazarına uygulamıştır. Kısa ve uzun vadeli bağlantılar keşfeden araştırmada Bitcoin'in hem standart finansal varlıkların özelliklerini hem de spekülatif varlıkları gösterdiği belirtilmiştir. Bu durum, Bitcoin'in bir para birimi, varlık ya da bir yatırım aracı olarak sınıflandırılıp sınıflandırılmayacağı hakkında daha fazla tartışmaya yol açmıştır.

Chu vd. (2015) çalışmalarında 2011'den 2014'e kadar olan veriler kullanılarak Bitcoin döviz kurunun ilk istatistiksel analizini yapmışlardır. ABD doları karşısında Bitcoin, döviz kuruna göre alınan logaritmik getirilere, finansmanda kullanılan en yaygın dağıtımların 15'ini sığdırmıştır. Söz konusu çalışmada, genel hiperbolik dağılımın en uygun olanı verdiği saptanmıştır.

Corlu ve Corlu 2015 yılındaki çalışmalarında döviz kurunun getirilerinin çarpıklık ve zirvelerini yakalamada genelleştirilmiş lambda dağılımının çarpık *t* dağılımı, sınırsız Johnson dağılımları ve normal ters Gauss dağılımı gibi diğer esnek dağılımlara göre karşılaştırmasını yapmıştır. Bu çalışmada Riske Maruz Değer ve Beklenen Eksiklik için, genelleştirilmiş lambda dağılımının benzer bir performans gösterdiği ve genel olarak, finansal verilerdeki ağır kuyruğun davranışının yerine getirilmesi için bir alternatif olarak kullanılabileceği sonucuna varmışlardır.

Nadarajah vd. (2015) ile Corlu ve Corlu (2015) döviz kuru iadeleri çalışmasını gözden geçirerek, *t* dağılımının test edilen dağılımlara benzer bir performans

gösterebileceğini ortaya koymuşlardır. Bruneau ve Moran (2017), Kanada imalat sanayilerindeki döviz kuru dalgalanmalarının işgücü piyasası düzenlemeleri üzerindeki etkisini araştırmıştır. Dai vd. (2017), Doğu Asya ülkelerinde döviz kurlarının ekonomik büyüme üzerindeki rolünü incelemiştir. Parlapiano vd. (2017), döviz kuru riskini Avrupalı firmaların değerine göre ortaya koymuşlardır. Schroeder (2017), gelişmekte olan ülkelerdeki döviz kurları ile ilgili makro ekonomik performansı araştırmıştır. Seyyedi (2017), altın fiyatları, petrol fiyatları ve Hindistan'daki döviz kuru arasındaki etkileşimli bağlantıların bir analizini sunmuştur.

Literatürde araştırılan bir diğer konu da kripto paraların fiyatlarındaki büyük dalgalanmalardır (volatilite). Çeşitli araştırmalarda bu büyük dalgalanmaların hesaplanması için çok sayıda tanım ve yöntem ortaya konulmuştur (Chan vd., 2017; Sapuric ve Kokkinaki, 2014; Briere vd., 2015). Sapuric ve Kokkinaki (2014) çalışmalarında, volalitelilik kavramını döviz kuru günlük dalgalanmalarını temsil eden yıllık dalgalanma (ya da standart sapma) olarak tanımlamıştır. Araştırmacılar bu çalışmada döviz kurunun standart sapmasını, yıllık işlem gün sayısının karekökü ile çarpılmasıyla hesaplamışlardır. Briere vd. (2015), analizlerinde yıllık getirileri kullanmaktadır ve ayrıca yıllık volatiliteyi hesaplamaktadır.

Literatürdeki diğer volatilite türleri, gelecekteki, tarihsel, tahmin ve ima edilen volatilite olarak geniş bir şekilde kategorize edilebilmektedir (Natenberg 2007). Literatürdeki çoğu çalışmada temel hipotez, blok zincirin dijital çevrimiçi dünyada dağıtılmış bir fikir birliği oluşturma sistemi kurmasıdır. Bu dijital sistem, katılımcı kurumların kamu muhasebesinde reddedilemez bir kayıt oluşturarak dijital bir olayın gerçekleştiğinin kesin olarak bilinmesini sağlamaktadır. Söz konusu dijital sistem merkezi bir sisteme göre daha demokratik ve açık, ölçeklenebilir bir dijital ekonomi geliştirmeyi amaçlamaktadır (Pimentel vd., 2020). Halka açık defterdeki her işlem için sistemdeki katılımcıların çoğunluğu ile mutabakat sağlanmakta ve bir kez sisteme girilen bilgi asla silinememektedir. Blok zinciri, yapılan her bir işlemin kesin ve doğrulanabilir bir kaydını dijital ortamda bulundurmaktadır (Zhang vd., 2019).

Bu bilgiler ışığında, bir blok zinciri; katılımcı taraflar arasında icra edilmiş ve paylaşılmış olan tüm işlemlerin, dijital olayların kayıtlarının, halka açık defterlerinin dağıtılmış bir veri tabanı (distributed database) olarak belirlenmektedir. Bu noktada günümüzde sıklıkla kullanılan Bitcoin teknolojilerini ele almakta fayda vardır.

2.5. Bitcoin Teknolojileri

Bitcoin, blok zinciri teknolojisine içsel olarak bağlı olan en popüler ve en tartışmalı örnektir. Bitcoin'in mevcut teknolojileri birleştirerek yeni fonksiyonlar yarattığı söylenebilir. Herhangi bir merkezi otorite olmaksızın, elektronik para ile çalışılan bir sistem gibi çalışabilmek, verilerin tahrif edilmesini ve ödemelerin çoğalmasını önlemek için önlemlerin alınması ve sistemin kötü niyetli kullanıcıların saldırılarına karşı korunması için bitcoin çok uygun bir sistemdir (Cermeno, 2016). Hükümet kontrolü olmaksızın çok büyük hacimdeki anonim işlem pazarını mümkün kılmasından dolayı ulusal hükümetler ve finansal kurumlarını kapsayan bir dizi düzenleyici konuyla ilgilenmek zorundadır.

Blok zincir teknolojisi yıllardır kusursuz bir şekilde çalışmakta, finansal ve finansal olmayan piyasa uygulamalarına başarıyla entegre edilmektedir. 2019 yılında Silikon Vadisin'de çalışan, tarayıcı geliştiren bir şirket sahibi olan Marc Andreessen, blok zincirin dağıtık tasarlanmış modelinin internetin kendisinden bu yana en önemli buluş olarak gördüğünü açıklamıştır. BNP Paribas'dan Johann Palychata, Quintessence dergisinde, Bitcoin'in, blok zincirin ve dijital paranın işlev görmesine izin veren yazılımın, finans dünyasını önemli oranda dönüştürme potansiyeline sahip olan ve buhar ya da yanmalı motor gibi tarihsel bir buluş olarak ele alınması gereken bir buluş olduğunu belirtmiştir (Joshi vd., 2019).

Mevcut dijital ekonomi, belirli bir merkezi otoriteye güvenmeye dayanmaktadır. Tüm çevrim içi işlemleri bize doğruyu söyleyecek birine duyulan güven üzerinden çalışmaktadır. Buna örnek olarak,

- e-posta hizmet sağlayıcısının e-postanın teslim edildiğini bildirmesi,
- Belli bir dijital sertifikanın güvenilir olduğunu bildiren bir sertifika yetkilisi olması,
- Facebook gibi bir sosyal iletişim ağı, hayatımızdaki olaylarla ilgili yazılarımızın sadece arkadaşlarımızla paylaşıldığını garantilemesi,
- Paramızın uzak ülkedeki sevdiklerimize güvenilir bir şekilde teslim edildiğini söyleyen bir banka işlevini yerine getirmesi verilebilir.

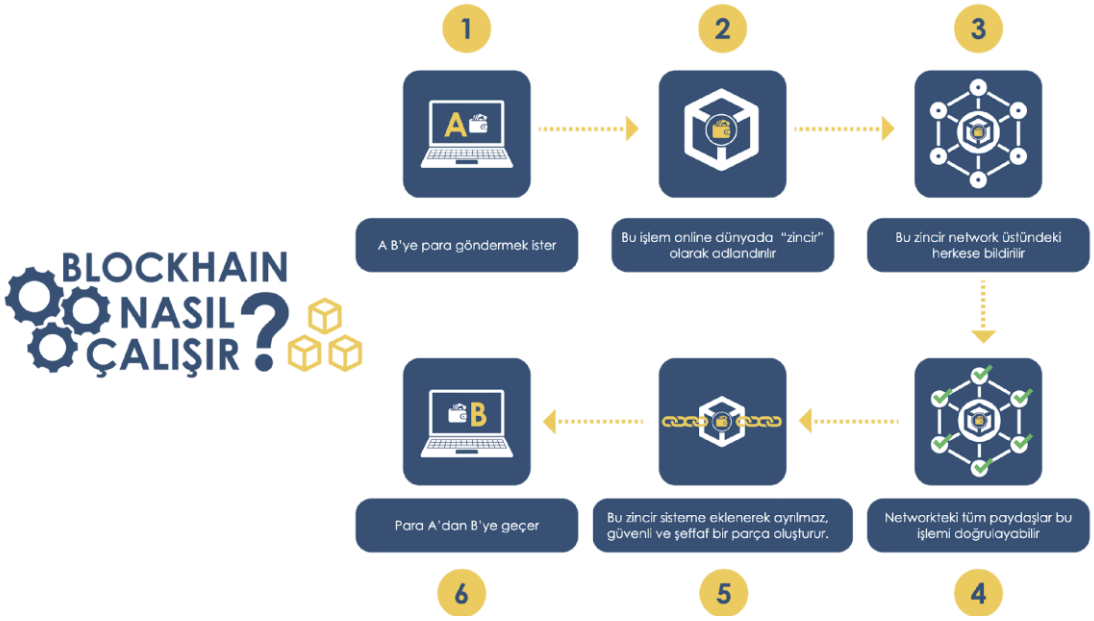
Blok zinciri teknolojisinin farkı bu noktada ortaya çıkmaktadır. Blok zincir dijital dünyayı içeren geçmiş ve şimdiki her çevrimiçi işlemin, gelecekte herhangi bir zamanda doğrulanabileceği dağıtılmış bir mutabakat sağlayabilmesi ile dijital dünyada devrim potansiyeline sahiptir. Bu potansiyel, dijital varlıkların ve ilgili tarafların gizliliğinden taviz verilmesini gerektirmemektedir. Dağıtılmış fikir birliği ve anonimlik, blok zinciri teknolojisinin iki önemli özelliğidir.

Blok zincir teknolojisinin avantajları, düzenleyici sorunları ve teknik zorlukları kolayca aşabilme olarak sıralanabilir. Gelişmekte olan bir anahtar kullanım bloğu teknolojisi, "akıllı sözleşmeler" içeren ve temel olarak sözleşmenin şartlarını otomatik olarak yerine getirebilen bilgisayar programlarıdır. Katılımcı kuruluşlar arasında akıllı bir sözleşme ile önceden yapılandırılmış bir koşul sağlandığında, sözleşme anlaşmasına dahil olan taraflar, sözleşmeye göre otomatik olarak şeffaf bir şekilde ödeme yapabilmektedirler (Sitonio & Nucciarelli, 2018).

Akıllı Mülkiyet (Smart Property) bir mülkiyetin ya da varlığın mülkiyetinin, Akıllı Sözleşmeler kullanılarak blok zincirleme yoluyla kontrol edilmesine ilişkin bir diğer ilgili kavramdır. Blok zinciri teknolojisinin, hem finansal hem de finansal olmayan alanlarda geniş uygulama ortamı bulması nedeniyle finansal kurumlar ve bankalar artık blok zinciri teknolojisini geleneksel iş modellerine tehdit olarak görmeyerek, bu alanda yenilikçi blok zinciri uygulamaları üzerinde araştırma yapmakta ve gerçek anlamda fırsatlar aramaktadırlar. Yakın zamanda yapılan bir röportajda Estonya'daki LHV Bankası'ndan Rain Lohmus, bazı bankacılık ve finansla ilgili uygulamalar için Blok zincirinin en çok test edilen ve en güvenli sistem olduğunu ifade etmiştir. Blok zincirin finansal olmayan uygulama fırsatları da giderek yaygınlık kazanmaktadır. Müzik endüstrisi, noter, özel menkul kıymetler ve evlilik cüzdanlarındaki tüm yasal belgeler, sağlık kayıtları ve diğer ödemelerin varlığını doğrulayan dijital ispatlar blok zincirle oluşturulabilmektedir (Sitonio & Nucciarelli, 2018).

Dijital varlığın kendisini saklamak yerine dijital varlığın parmak izini depolayarak, anonimlik ya da gizlilik hedefi kolayca elde edilebilmektedir. Blok zincir teknolojisi, dijital ticareti yürütmek, kişisel verilerimizi ve yaşam olaylarımızı paylaşmak için gittikçe artan bir dijital ekonomideki yeni büyüme motoru olma potansiyeline sahiptir (Allessie vd., 2019). "Blok Zincir Teknolojisini" bir teknoloji topluluğu ya da bir Lego kümesi olarak düşünmek

mümkündür. Kümeden farklı elemanlar seçerek, farklı şekillerde bir araya getirebilir ve böylece farklı sonuçlar elde edilebilmektedir (Alamri vd., 2019). Blok zincir modelinde en son değere sahip olan blok, bir diğer sisteme yaptığı transfer miktarını zincirin halkaları şeklinde ana sisteme ekler. Her bir işlem bir sonrakinin devamı niteliğindedir ve peş peşe doğrulanabilir bir ana sistemi oluşturur. Blok zincirin çalışma modeli Şekil 2.1'de sunulmuştur.



Şekil 2.1. Blok zincir çalışma modeli

İnternet ticareti, herhangi bir elektronik işlemi gerçekleştiren ve aracılık eden güvenilir üçüncü taraf olarak hizmet veren finansal kurumların varlığı üzerine kurulu bir sistemdir. Güvenilir üçüncü kişilerin rolü, işlemleri doğrulamak ve kayıtları korumaktır. Çevrimiçi işlemlerde belli bir dolandırıcılık yüzdesi kaçınılmazdır ve bu durum finansal işlemlerle yüksek işlem maliyetli arabuluculuk gerektirmektedir (Dai vd., 2013). Böyle bir ortamda bitcoin, üçüncü kişilerin internet üzerinden çevrimiçi bir işlem yürütmesi için iki tarafa güven veriyor olması yerine şifreleme kullanıyor olmasıyla farklılaşmaktadır. Bitcoin ile her işlem dijital imza ile korunarak, gönderenin "özel anahtarı" ile dijital olarak imzalanmış alıcının "ortak anahtarına" gönderilmektedir. Para harcamak için, kripto para birimi sahibinin "özel anahtar"ın sahipliğini ispatlanması gerekir. Dijital para birimi alan varlık, dijital imzayı ilgili "özel anahtar"ın sahipliğini, gönderenin "açık anahtarı"nı kullanarak işlem üzerinde doğrulamaktadır. Her işlem, Bitcoin ağındaki her düğüme

yayınlanmakta ve daha sonra doğrulama işleminden sonra bir açık deftere kaydedilmektedir. Ayrıca her bir işlemin geçerlilik için doğrulanması gerekmektedir (Houben ve Snyers, 2018).

Bitcoin'in yarattığı bu değerin yanı sıra, eşler arası ağdaki diğer düğümlere yayınlanan bu işlemlerin sırasını korumada sorun yaşanabilmektedir. İşlemler, üretildikleri sıraya gelmediklerinde, kripto para biriminin çift harcamalarının gerçekleşmediğinden emin olmak için bir sisteme ihtiyaç duyulmaktadır. İşlemlerin, düğümün Bitcoin ağı üzerinden geçtiği göz önünde bulundurulduğunda, bir düğümde alınan siparişlerin, bu işlemlerin oluşturulduğu sırayla gelmesi konusunda garanti yoktur (Çarkacıoğlu, 2016).

Bitcoin bu sorunu blok zinciri teknolojisi ile çözmüştür. Bitcoin sistemi, işlemleri blok olarak adlandırılan gruplara yerleştirmektedir. Daha sonra bu blokları blok zinciri adı verilen bir yöntemle birleştirerek sipariş etmektedir. Bir bloktaki işlemlerin aynı zamanda gerçekleştiği kabul edilmektedir. Bu bloklar, her bir bloğa, bir önceki bloğun hash fonksiyonunu içeren uygun bir lineer ve kronolojik sırayla (bir zincir gibi) bağlanmaktadır.

2017 yılının Ekim ayı itibariyle, 1000 adet farklı kripto para birimi üzerinde şartname mevcuttur ve tam olarak uygulanan ilkleştirilmiş kripto para birimleri, Bitcoin'den türetilmişlerdir. Kripto para sistemlerinde güvenlik, dürüstlük ve kefalet dengesi, madenciler olarak adlandırılan karşılıklı şüphe eden taraflardan oluşan bir topluluk tarafından korunmaktadır. Madenciler yani genel topluluk üyeleri, bilgisayarlarını kullanarak belirli bir zaman damgasına göre onları sıraya eklenen işlemlerin doğrulanmasına ve zaman damgasını vurmaya yardımcı olmaktadırlar. Madencilerin kripto para birimi defterinin güvenliğini korumak için mali teşvikler bulunmaktadır (Adedoyin vd., 2017).

2.6. Blok Zincir Uygulamaları

Blok zincir teknoloji uygulamaları finans, gayrimenkul, hukuk, kimlik gibi farklı alanlarda uygulanabilmektedir. Tablo 2.3'te farklı uygulama alanları bağlamında blok zincir teknoloji uygulamaları sunulmuştur.

Tablo 2.3. Blok zincir Teknoloji Uygulamaları (Deloitte, 2018).

Uygulama Alanı	Paydaşlar	Açıklama
Finans	Dağıtık zincir ve finansal servisler	Blok zincir teknolojisinin ilk odaklandığı çalışmalardan birisi, finansal kurumların kendi geliştirdikleri özel blok zincirler olmuştur.
Gayrimenkul	Akıllı, Otonom Özellikler	Akıllı özellikler fiziksel olan ve fiziksel olmayan varlıkların işlem görmesine olanak tanır. Fiziksel ürünlere örnek olarak, araçlar, telefonlar, evler gösterilebilir.
Hukuk	Programlanabilir Kontratlar	Dağıtık Otonom Organizasyonlar, Dağıtık Otonom Kurumlar, kayıtların saklanması ve kaydedilmesi konusunda yenilikçi bir mimari sunmaktadır.
Kimlik	Güvenli Kimlik Doğrulama	Blok zincir ile geliştirilen kimlik uygulamaları verimliliği artırmak ve dolandırıcılık işlemlerini en aza indirmektedir.

Blok zinciri teknolojilerinin kayıt ve değişim kapsamının genişletilmesi ve bu teknolojilerin daha yaygın bir şekilde kullanılması blok zinciri üzerinde çalışan uygulamalar ile mümkündür. Bu uygulamalar ile çeşitli malların mülkiyet devrinin, ispatlanmasının ve hizmetlerin alınması haklarının (mülkiyet, kullanım hakkı, vb.) blok zinciri teknolojileri ile daha yaygın bir şekilde uygulanabilir olması ve teknolojinin yaygınlaşması sağlanabilir.

Fikir birliği algoritmaları, sistemi kullanan paydaşların nasıl işlediğine karar verdiği sistemlerdir. Bu sistemlerin performansının revizyonu ve iyileştirilmesi ya da Bitcoin'deki İş İspatı'nın (Proof of Work) sorunlarına cevap olarak yeni fikir birliği algoritmaları benimsenebilir.

Katılımcıların ağa katılımını sınırlandırarak, bir uzlaşı sağlamada verimliliği arttırmayı ve çok sayıda tanımlanmamış kişilerin katılımına izin vermek yerine belirli sınırlamalar getirerek işlemlerin işlenmesini hızlandırmayı hedefleyen güvenilirliğin artırılması olarak belirlenen başlıca üç eksen üzerinde odaklanarak geliştirilmiştir (Matthieu Quiniou, 2019). Blok zincir teknolojilerinin kullanım alanları Şekil 2.2'de sunulmuştur.



Şekil 2.2. Blok zincir teknolojilerinin geniş kullanımı

2.7. Kriptografik Hash Fonksiyonları

Kriptografik hash fonksiyonu (hash function) çeşitli güvenlik özelliklerini sağlayan bir hash fonksiyonudur. İdeal bir kriptografik hash fonksiyonu; herhangi bir mesaj için özet hesaplamanın, bir özete karşılık gelecek mesajı oluşturmanın, özeti değişmeyecek şekilde mesajı değiştirmenin, aynı özete sahip iki farklı mesaj bulmanın kolay olması olmak üzere dört özelliği sağlamalıdır (Brito & Castillo, 2013).

Kriptografik hash fonksiyonları, bilgi güvenliği konuları olan sayısal imza, mesaj doğrulama kodu ve diğer doğrulama yöntemlerinde yaygın olarak kullanılmaktadır. Sıradan hash fonksiyonları gibi veriyi komut çizelgesine eşlemede, eşdeğer veri bulmada, dosyaları tekil olarak tanımlamada ve veri bütünlüğü sağlamasında da kullanılır. Bilgi güvenliği

konularında kriptografik hash fonksiyonları, terim anlamları farklı olsa da sayısal parmak izi sağlama ya da özet değeri ile benzer anlamlarda kullanılır (Brito & Castillo, 2013).

Verileri bir hash fonksiyonuna girmek, belirli bir sayı ile bir karma değerin çıktısına neden olmaktadır. Bu mekanizma, aynı sonuç değerinin aynı girdilerden elde edilmesi gerçeğiyle karakterize edilir. Ancak orijinal verilerde sadece küçük bir farklılık tamamen farklı bir karma değerle sonuçlanabilmektedir. Orijinal verileri bir karma değere dayanarak çıkarmak son derece zordur. Bu özelliklerden faydalanarak, bu mekanizma ile verilerin bozulmasının tespiti için Bitcoin sistemi kullanılır. Blok zinciri verilerinin sürekliliğinin doğrulanması, garanti edilmesi ve karma değerlerin hesaplanmasından yararlanarak İş İspatları blok zincirlerin oluşturulması için kullanılmaktadır (Caradonna, 2020).

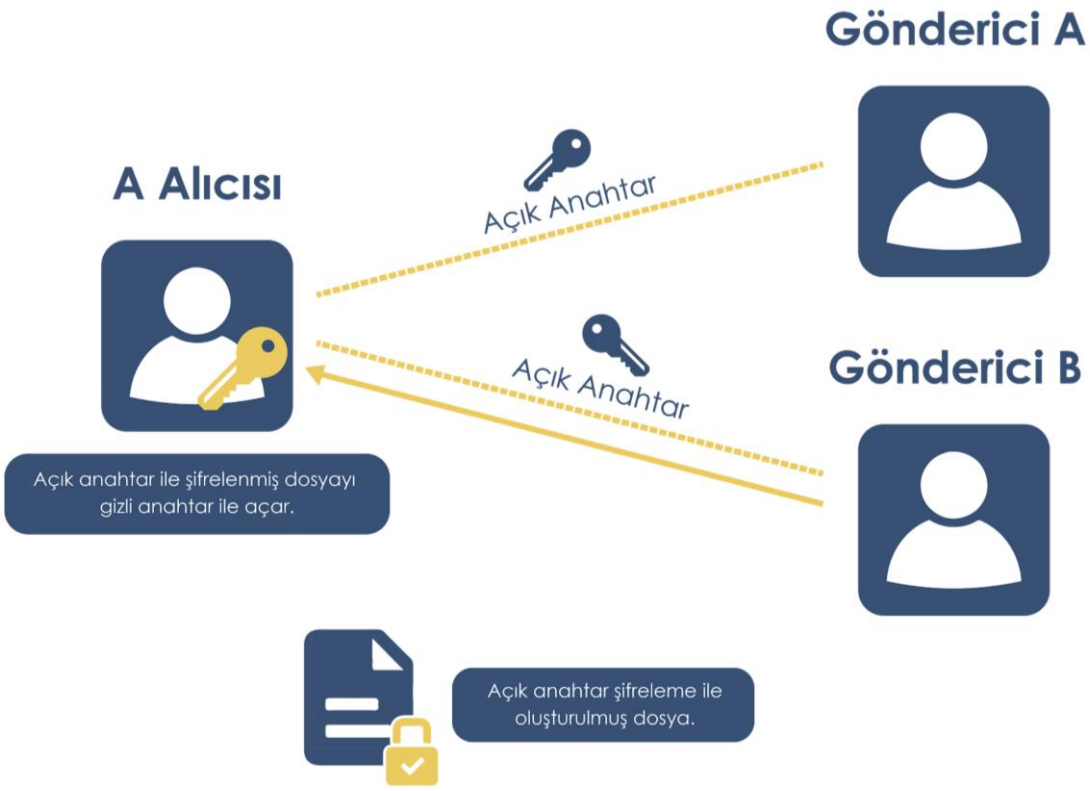
Kriptografik hash fonksiyonunda girdi olarak kullanılan veriler harmanlanıp bir sonuç değer üretilir, daha sonra bu sonuç bir başka harmanlamaya girdi teşkil eder. Bu olay defalarca tekrar edilir. Böylelikle, ilk girdide yapılan ufak değişiklikler, sonuç değerinde büyük farklılıkların oluşmasına yol açar. Kriptografik hash fonksiyonu çalışma modeli Şekil 2.3'te sunulmuştur.



Şekil 2.3. Kriptografik hash fonksiyonu çalışma modeli

Bu işlemler sırasında döküman formatları ve boyutları farklılık gösterebileceği için tüm dökümanın özeti şeklinde olan özet kodu imzalanarak bir standart oluşturulur. Bu süreçte dijital imzalar kullanılarak imzalama işlemi gerçekleştirilir. Dijital imzayı kullanmak için açık anahtar şifrelemesi yapılmaktadır. Açık anahtar şifrelemesi, şifreleme ve şifre çözme için farklı anahtarlar kullanan bir şifreleme yöntemidir. Şifreleme ve şifre çözme için

aynı anahtarı kullanan simetrik anahtar şifreleme durumunda, anahtarı yalnızca ilgili tarafa teslim etmek için çeşitli güvenlik önlemleri gereklidir. Buna karşılık, açık anahtar şifrelemesi, bir alıcının bir çift özel anahtar ve bir ortak anahtar hazırlaması ve açık anahtarın göndericiye önceden teslim edilmesi durumunda dosyaların güvenli bir şekilde teslim edilmesini sağlamaktadır. Alıcının özel anahtarını düzgün bir şekilde yönetmesi koşuluyla, diğer kişiler açık anahtarını kullanmasına rağmen güvenlik korunabilir risk bileşeni ortadan kalkar (Fang vd., 2020). Açık anahtarın bu şifreleme modeli Şekil 2.4'te verilmiştir.



Şekil 2.4. Açık anahtar şifreleme çalışma modeli

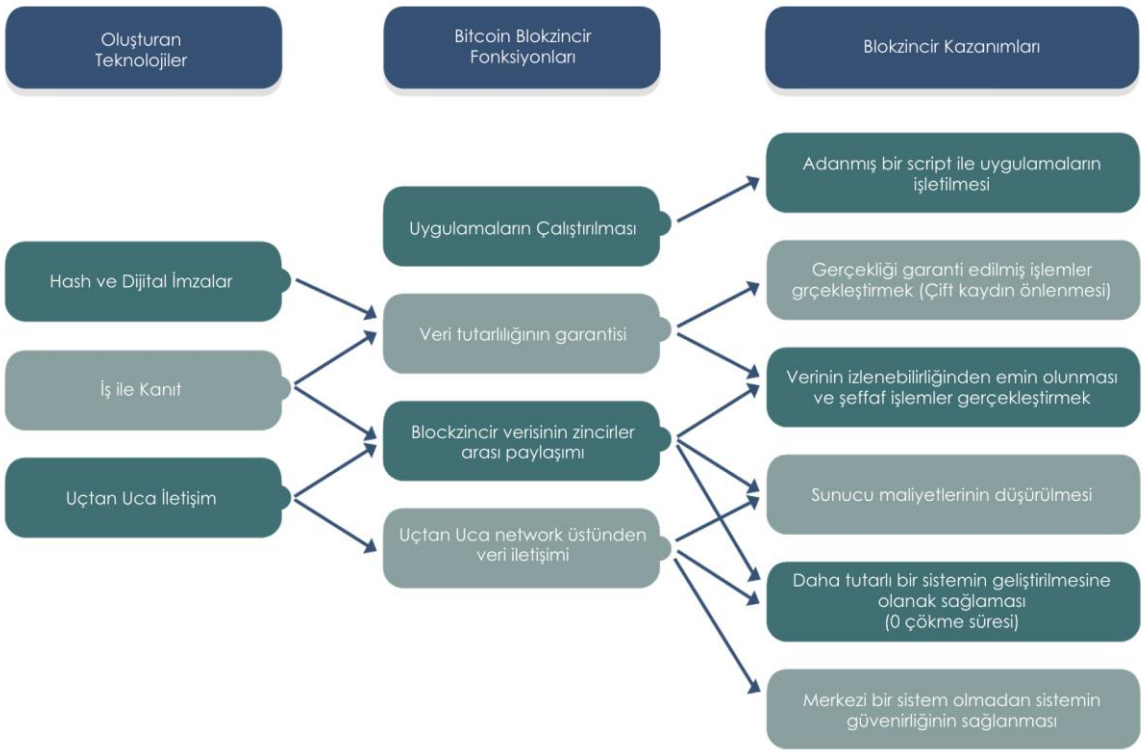
Dijital imza, bir ağ üzerinden gönderilen verilerin doğruluğunu ispatlamak için bir mekanizmaya atıfta bulunmakta ve açık anahtar şifrelemede yer alan bir çift anahtar da burada kullanılmaktadır. Genel olarak, gönderenin özel anahtarı ile bir alıcıya gönderilecek bir dosyanın karma değerini şifrelemek suretiyle yapılan dijital imza, söz konusu dosya ile birlikte alıcıya gönderilir. Alıcı, dosyanın özet değerini kendi başına oluşturması için gönderici ile aynı kriptografik hash işlevini kullanır ve göndericinin dijital imzasını alıcının açık anahtarı ile şifresini çözmek suretiyle elde edilen karma değerini çapraz olarak kontrol eder. Gönderenin dijital imzası doğru ise onaylama işlemi gerçekleşir. Bitcoin sisteminde, işlem verilerinin yaratıcısı (bitcoin işleminin verileri) ve bitcoin cüzdanının adresini

tanımlamak için ortak anahtar şifrelemesi ve dijital imza kullanılmaktadır (Aydar vd., 2019). Burada sözü edilen dijital imza ile imzalanmış dokümanın kontrol ve onay süreci Şekil 2.5'te ilgili fonksiyonlar bağlamında bitcoin blok zincir fonksiyonları sunulmuştur.



Şekil 2.5. Dijital imza ile imzalanmış dokümanın kontrol ve onay süreci

Bu süreçler sonunda elde edilen kazanımlar ise Şekil 2.6'da verilmiştir.



Şekil 2.6. İlgili teknolojiler bağlamında fonksiyonlar ve kazanımlar

Bitcoin blok zincirinde, her bir düğüm, bir istemci-sunucu sisteminden daha yüksek hata toleransı sağlamak için çalışan Peer to Peer (P2P) olarak adlandırılan Uçtan Uca ağa

bağlanmaktadır. P2P ağına bağlı bu düğümlerin her biri, İş İspatı (Proof of Work) aracılığıyla oluşturulan fikir birliği, blok zinciri verilerini tutmaktadır. Bitcoin blok zincirinde, bloklar (ve her bir bloktaki veriler), devam eden özet hesaplamaları ve dijital imzalar yoluyla birbiriyle ilişkilidir. Ayrıca, İş İspatı aracılığıyla her bir blok için fikir birliği oluşturma, Bitcoin blok zincirindeki verilerin takibini ve doğrulanmasını sağlamaktadır (Monrat vd., 2019). Bu fonksiyonlar sayesinde, Bitcoin blok zinciri ekosistemi merkezi bir otorite olmaksızın, kötü niyetli kullanıcılar tarafından herhangi bir saldırıya karşı istikrarlı bir şekilde korunabilmekte ve istikrarlı bir sistemin gelişimini ve çalışmasını gerçekleştirebilmektedir. Sonuç olarak, sisteme bağlı olmakla birlikte, geliştirme ve işletme için kullanılan sunucu maliyetlerinin genel olarak azaldığı söylenebilmektedir. Bunun yanı sıra, bu işlevler doğruluğu garanti edilen ve daha sonra doğrulanabilecek son derece şeffaf olan işlemlere olanak sağlamaktadır (Sultan vd., 2018).

Bitcoin blok zincirinde, özel bir betik çeşitli işleme prosedürlerinin yürütülmesini sağlamaktadır. Colourful Coins, bilgisayarlı hak talepleri, dijital içerikler ve bilgisayarlı gerçek varlıklar üzerindeki haklar gibi varlık bilgilerini temel alarak bitcoinleri renklendirme ve bunları bitcoin sisteminde dağıtmak için kullanılan teknolojiye verilen isimdir. Colourful Coins, kaynaklı ve genel olarak çok yönlülüğü olan Varlıklar Protokolü ile Bitcoin blok zinciri kullanıcılarının, keyfi varlıklarını kendi inisiyatifleri ile dağıtmalarına olanak sağlamaktadır. Açık Varlıklar Protokolü ve Colourful Coins, ilgili renkleri ayırt etmek için kimlikler tahsis ederek çalışmaktadır (Schär vd., 2019). Bu süreçte ortaya çıkan birçok durumda, bir belgeyle ilgili olarak belgenin oluşturulduğu ya da son değiştirildiği tarihi onaylama gereği duyulmaktadır. Örneğin, fikri mülkiyet meselelerinde, kişinin rakip iddialara kıyasla önceliğini ortaya koyması için patentli bir fikri ilk yazdığı tarihi doğrulaması bazen hayati öneme sahiptir (Haber & Stornetta, 1991).

Bitcoin ağında hangi tür saldırıların önemli derecede ve uygulanabilir olabileceğini sorgulamak yerinde bir düşüncedir. Bunun yanı sıra bir kripto parayla ilgili olası saldırıları hafifletmek için hangi yöntemlerin en etkili olacağı çalışmaları da yine aynı şekilde gündeme gelmektedir. Bitcoin'in bugüne kadar olan saldırılara karşı dirençli olduğu ispatlanmış olduğundan, odak noktasının uzun vadeli sürdürülebilirlik üzerine olması gereklidir. Özellikle İş İspatı madenciliğin artık blok ödülü ile desteklenmemesi ve ağın gerçekleşen

işlem ücretleri ile güvence altına alınmasından sonraki olası saldırı riski ile gündeme gelmektedir (Bentov vd., 2014).

Sağlam bir kripto-parazit protokolünün, varlığını sürdürmek için sistemdeki farklı katılımcıların kendi çıkarına olduğu bir teşvik yapısını sağlama çabasında olması gereklidir. Burada, genişletilmiş protokolün bir saldırısının çok daha zorlu olacağı düşüncesiyle, olası güvenlik tehditleri olduğu iddia edilen olgunun bir çözümü olarak, Bitcoin protokolüne ayrıntılı bir uzantı sunulmaktadır. Pay Proof protokollerinin sonuç avantajları sunduğunu iddia ederken, Teminat İspatının (Proof of Stake), başarılı bir kripto para biriminin karşı karşıya kaldığı önemli riskleri hafifletmekte etkili ve sorunsuz bir yöntem olduğu söylenememektedir (Bentov vd., 2014).

İş ispatı hesaplamaları ve işlem doğrulaması için tahsis edilmiş olan veri merkezlerinin ölçek ekonomisi bağlamında hobi olarak madencilik yapanlara üstün gelmesi büyük bir sorun olan merkezileşmeyi beraberinde getirmektedir. İspat Belgesi Sistemi ile birlikte, iş ispatı veri merkezlerinin riski önemli ölçüde azaltılmış olsa da diğer riskler halen mevcuttur ve yeni riskler ortaya çıkmaktadır (Liv vd., 2020).

İş İspatı bir kişinin güvenilirliğini sağlamak ya da yanlış davranmasını engellemek için onun belirli miktar işi yapmasını onaylayan mekanizmadır. Bu mekanizma ile kişinin gerçekte yaptığı iş kolayca doğrulanabilmektedir. Proof of Work'un somut örnekleri arasında, görüntüleri kullanan CAPTCHA bulunmaktadır. Örneğin, e-posta göndermek için Hashcash adlı bir iş ispatı algoritması benimsenmiştir. Bir e-posta gönderirken her zaman belirli bir özet hesaplaması zorunludur. Böylece istenmeyen e-posta göndericileri bertaraf edilebilmektedir (Louis ve Guegan, 2019).

İş İspatı, Bitcoin'de madencilik denen bir iştir. Ağ katılımcıları, kendilerine iletilen işlem verilerinin toplanması için 1 olmayan herhangi bir değer ekleyerek bir karma değer hesaplar. Bitcoin gönderimi yapılırken, P2P ağının tamamını hedefleyen ilgili işlem verileri gönderilir. Bu nedenle, P2P ağının durumuna bağlı olarak, her bir düğüme ulaşan işlem verileri, zaman içinde belirli noktalarda farklılık gösterebilmektedir. Belirli bir değerden daha küçük bir değer elde edilmesi gerekir ve katılımcılar, değerleri gerektiği gibi elde edinceye kadar farklı değerler kullanarak hesaplamaya devam etmek durumunda kalmaktadırlar. Herhangi bir kişi ilgili değeri elde ettiğinde, ağ katılımcıları değerin

doğruluğunu karşılıklı olarak onaylamaktadır. Hesaplamalar için kullanılan işlem verilerinin toplamı da resmi işlem sonuçları olarak yeni bir blok olacak şekilde onaylanmaktadır. Ardından, bitcoinler hesaplamalar yoluyla doğru değeri elde etmeyi başarmış olan kişiye bir ödül olarak verilmektedir. Bundan sonra, tüm katılımcılar, söz konusu blokta yer almayan ve yeni oluşturulan işlem verilerini kullanarak bir sonraki madenciliğe geçmektedirler. Bitcoin, verilerin bozulmasını önleyebilmek, merkezi bir otorite olmaksızın ödemelerin çoğalmasını sağlayabilmek ve sistemi kötü niyetli kullanıcılar tarafından yapılan saldırılara karşı koruyabilen bir mekanizma oluşturabilmek için İş İspatı'nı kullanmaktadır (Zhang vd., 2019). İş İspatı algoritmasındaki hash fonksiyonu hesaplamaları Şekil 2.7'de verilmiştir



Şekil 2.7. İş İspatı Algoritmasında Hash Hesaplamaları

2.8. Uçtan Uca İletişim

Genel bir istemci-sunucu ağında, bir sunucu verileri koruma ve sağlama görevini üstlenirken bir istemci sunucudan veri talep etmekte ve onlara erişim sağlamaktadır. Bu senaryo bağlamında her iki tarafın da rolleri sabittir. Buna karşılık olarak, bir P2P ağına katılan tüm düğümler (iletişim için bilgisayarlara atıfta bulunarak, aynı zamanda "akranlar" olarak da adlandırılır) sırasıyla verileri tutar ve bu düğümler arasında eşit bir temelde verilerin talep edildiği ve sağlandığı özerk bir ağ oluşturulur. Bir P2P ağında, bir istemci-sunucu ağının durumundan farklı olarak, bir sunucu ya da istemci ile ilgili düğümlerin rolleri sabit değildir (İslam vd., 2014).

Bir P2P ağını benimserken, arama yöntemlerini ve veri aktarım yöntemlerini dikkate almak gerekmektedir. Arama yöntemleri, düğümlerin ve verilerin konumlarını yönetme araçları olup temsili örnekler arasında yalnızca bir P2P ağıyla yönetim yürütme, bir dizin sunucusu kurulumu ve yüksek işlem gücü (süper düğümler) yönetimi gerçekleştiren düğümler bulunmaktadır. Veri iletim yöntemleri, düğümler arasında veri iletme araçlarıdır ve düğümler arasında doğrudan iletime ve başka bir düğüm üzerinden aktarılan aktarımlara bölünmektedirler. Bitcoin için kullanılan P2P (uçtan uca) ağında, P2P (uçtan uca) bir arama yöntemi olarak benimsenirken, işlemler veri iletimiyle ilgili düğümleri birbirine geçirerek gerçekleştirilmektedir (Delgado-Segura vd., 2018).

P2P ağ teknolojisinin, tam bir dağıtılmış ağ için uygun bir temel geliştirmeye ve Bitcoin'deki tek başarısızlık noktasını ortadan kaldırmaya katkıda bulunduğu görülmektedir. Blok zinciri verileri göz önüne alınarak, Bitcoin P2P ağına katılan ve madenciliği gerçekleştiren tüm düğümlerin aynı verilere sahip olması gerekliliğini ortaya çıkarmaktadır (Park vd., 2019).

2.9. Cüzdan

Cüzdan (wallet), kripto para birimlerini güvenli bir şekilde saklamak, göndermek ve almak için özel ve kamuya ait şifreleme anahtarlarının yönetimini kullanan bir yazılım olarak tanımlanmaktadır. Ayrıca cüzdan, kripto para birimlerini onaylamak için bir kullanıcı ara yüzü sağlamakta ve belirli bir işlemi onaylamak için ödeyecekleri ücret gibi bazı işlevleri otomatik hale getirmektedirler (Volety vd., 2019).

Her bir kripto para birimi, temel cüzdan işlevselliğini (örn. Bitcoin Core için Bitcoin, Ethereum için Mist tarayıcı) içeren bir referans uygulamasına sahiptir. Bununla birlikte, çeşitli nedenlerle referans uygulama cüzdanı pek çok kullanıcı için işlevsel değildir. Sonuç olarak, kripto paraların depolanmasını ve cüzdanların kullanımını kolaylaştırmak için son yıllarda çok sayıda cüzdan sağlayıcısı üretilmiştir. Bu cüzdanlar, gönüllü geliştiriciler tarafından yürütülen açık kaynaklı projelerden, risk sermayesi destekli tescilli şirketler tarafından sunulanlara kadar geniş bir yelpazede çeşitlenmektedir (Beckett, 2019).

Sözü geçen cüzdan sağlayıcılarının neredeyse yarısı Amerika Birleşik Devletleri ve Birleşik Krallık'ta bulunmaktadır. Dünya çapında ele alındığında, cüzdan sağlayıcılarının

konumu bağlamında Avrupa %42'lik oran ile birinci sırada yer almaktayken, Kuzey Amerika %39, Asya-Pasifik ise %19'luk oran ile Avrupa'yı takip etmektedir (Hileman ve Rauchs, 2017).

Sınırlı sorumluluğu olan kayıtlı şirketler cüzdan sağlayıcılarının %85'ini temsil ederken, %15'ini ise açık kaynaklı / gönüllü projeleri temsil etmektedir. Kayıtlı kuruluşlar tarafından sağlanan cüzdanlardan "anonim cüzdan" olarak söz edilmektedir (Riehle vd., 2014).

Anlaşmalı cüzdanlarda çalışan 19'u cüzdan sağlayıcısı olmak üzere toplam 418 tam zamanlı çalışan vardır. Bununla birlikte, toplam cüzdan sağlayıcılarının %25'inden fazlası üçten az çalışana sahip olup, %69'u 11'den daha az tam zamanlı çalışana sahiptir. Bu veriler, ortalama bir cüzdan sağlayıcısının oldukça küçük bir organizasyon olduğunu ifade etmektedir. Anket yapılan cüzdanların sadece %22'sinin 20'den fazla tam zamanlı çalışanı bulunmaktadır. Bazı cüzdan sağlayıcıların diğer kripto para birimi sektörlerinde de aktif olduğu ve cüzdan hizmetinde tam zamanlı çalışanların tam sayısının bilinemeyeceği görülmüştür. Cüzdan sağlayıcıların %39'u, kullanıcıların aynı cüzdanda birden fazla kripto para birimi depolayabilmelerini ve %19'unun da kullanıcıların üç kripto para biriminden fazlasını saklamalarını olası kılmaktadır. Cüzdanların büyük çoğunluğu Bitcoin'i desteklemektedir. Litecoin, Etherium ve Dogecoin cüzdan üreticileri tarafından en çok desteklenen diğer üç kripto para birimidir (Houben ve Snyers, 2018).

Cüzdanlar giderek daha farklı kripto para birimlerini desteklemeye devam etmektedir. Şu anda yalnızca tek bir kripto para birimini depolamayı destekleyen cüzdan sağlayıcılarının %31'i, mevcut yol haritasının daha fazla kripto para için destek sunmayı hedeflediklerini ifade etmişlerdir. Çoklu-kripto para cüzdanlarının %78'i mevcut tekliflerine daha fazla kripto para eklemeyi amaçlamaktadır (Moreno-Sanchez vd., 2016).

Cüzdanlar, zaman içinde anahtar yönetimini ele alan basit yazılım programlarından, çeşitli özellikler sunan gelişmiş uygulamalara dönüşmüştür. Hem protokol düzeyinde hem de cüzdan sağlayıcıları arasındaki önemli yenilikler, çoklu imza gibi son teknoloji olarak kabul edilen bazı teknik standartların ortaya çıkmasına neden olmuştur. Bugün cüzdanların yaklaşık olarak %56'sı çoklu imza desteği sunmaktadır. Küçük ve büyük cüzdanlar arasında kayda değer farklar bulunmaktadır. Küçük cüzdan sağlayıcılarının yaklaşık %42'si, büyük

cüzdan sağlayıcılarının ise yaklaşık %86'sı çoklu imza desteği sunmaktadır (Hileman ve Rauchs, 2017).

Bitcoin cüzdanı bu nedenle sadece bir özel anahtar deposudur. Bu özel anahtar deposu bir sabit sürücü, bir CD, cep telefonunuza indirilmiş bir uygulama ya da bir kasada sakladığınız bir parça kağıt şeklinde olabilmektedir. Verileri depolayabilecek herhangi bir sistem Bitcoin cüzdanı olarak hareket edebilmekte ve bu işlevi yerine getirebilmektedir. Cüzdanlar ile ilgili en büyük sorun, cüzdanın kaybedilmesi ya da anahtarların kaldırılması ile bu hesaplardaki paraya erişim ihtimalinin kalıcı olarak ortadan kalkmasıdır. Aslında geçtiğimiz birkaç yıl içinde, insanların özel anahtarlarını kaybettiği ve dolayısıyla büyük miktarlarda Bitcoin kaybettiği bazı talihsiz durumlar yaşanmıştır. Örneğin, bir kişi, özel anahtarlarını sakladığı eski bir bilgisayar sabit diskini çöpe atmış ve 7500 BTC'lik bir kayıp yaşamıştır. O gün sabit disk ile birlikte kaybolan 7500 BTC'nin tahmini değeri yaklaşık olarak 4,6 milyon Pound değerindedir. Benzer şekilde, yeni işlemler için anahtarlar düzenli olarak üretildiğinden, veri kaybını önlemek için cüzdanların da düzenli olarak yedeklenmesi mutlaka gereklidir (nypost.com, 2018). Bu sorunlara karşı bir koruma mekanizması olarak son birkaç yılda cüzdan teknolojisinde bazı gelişmeler görülmüştür. Bu teknolojiler, mevcut hiyerarşik veri tabanlı cüzdanlardan, Bitcoin Trezor gibi donanım tabanlı cüzdanlara kadar çeşitlilik göstermektedir. Her bir cüzdanın kendine özgü avantajları ve tasarım amaçları vardır. Örneğin, yazılım tabanlı şifreli cüzdanlar, yalnızca bir kez yedeklenmelidir. Çünkü yeni anahtarların üretimi, bazı şifreler üzerinde hesaplanabilir özelliğe sahiptir. Diğer taraftan donanım tabanlı cüzdanlar virüslerden, siber saldırılardan ve kötü amaçlı yazılımlardan korunmak için tasarlanmıştır. Örneğin donanım bazlı bir cüzdan türü olan Bitcoin Trezor, özel anahtar hırsızlığını önlemek için tasarlanmış olup işlemler imzalandığında, cüzdanda saklanan özel anahtarları asla göstermeyerek işlemleri gerçekleştirme imkanına fırsat sunmaktadır. Bu, bilgisayarın işlemlerin üretilmesinde ne kadar güvensiz olduğuna bakılmaksızın, özel anahtarların savunmasız hale getirilemeyeceği anlamına gelmektedir. Bu tip çevrim dışı Bitcoin depolamaya soğuk depolama denilmektedir (Eskandari vd., 2015).

2.10. İşlemler

Bir işlem, bir dizi giriş ve bir dizi çıktıyı temsil etmektedir. İşlemin tamamı SHA256 isimli hash fonksiyonu kullanılarak elde edilmekte ve bu hash fonksiyon global olarak benzersiz işlem kimliği olarak hizmet vermektedir. İşlemler ad-hoc ikili format kullanılarak temsil edilmektedir. Bu, Bitcoin'in defacto spesifikasyonu olduğu önemli bir detayın erken bir örneğidir (Bonneau vd., 2015).

İşlemden elde edilen her bir çıktıda, kısa bir kod parçacığının (özel bir betik dilinde) betiği olarak adlandırılan scriptPubKey, işlem çıkışının kullanılabileceği koşulları temsil etmekte ve daha sonraki bir işlemde girdi olarak bulunmaktadır (Al Khalil vd., 2017).

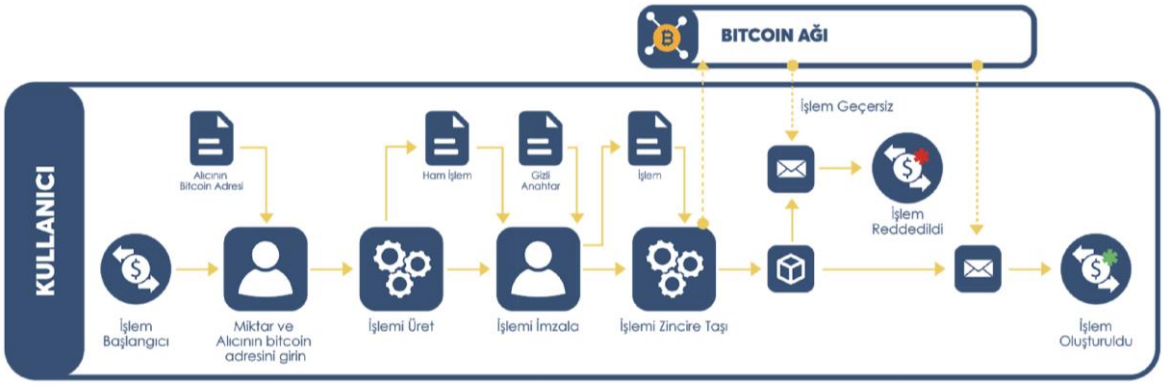
Genellikle, scriptPubKey bir ECDSA ortak anahtarının ve bir imza doğrulama yönteminin karma değerini belirtmektedir. Bu betik, belirtilen anahtar kullanılarak tüm yeniden işlem sözleşmesinin imzalanmasıyla kullanılabilir ve buna "pay-to-pub-key-hash" işlemi denilmektedir. Bitcoin işlemlerinin büyük çoğunluğu, pub-to-key-key-hash'tir ve sistem, diğer işlem türleri mümkün olsa da genellikle işlem komut dosyalarını kullanmaktadır. Komut dosyası dili, opcodes adı verilen 200''den az komut içeren, geçici, Turing-olmayan bir yığın dili olup şifreleme işlemleri için destek içermektedir. Buna örnek olarak veri toplama ve imzaları doğrulama işlemleri verilebilir. İşlem formatı gibi betik dili sadece Bitcoin uygulamasında belirtilmektedir (Chowdhury, 2020).

İşlem girdileri, önceki işlemlere yeni işlem eklenmesi ve bu işlemin çıktı dizisi içindeki indeksiyle ilgilidir. Bir önceki işlemin çıktısını kullanabilmek için birleştirilmiş scriptSig ve scriptPubKey başarılı bir şekilde birlikte işlemelidir. Pub-pub-key-hash işlemleri için, scriptSig sadece bir açık anahtar ve imzadır. Ayrıca, scriptSig olarak adlandırılan işlem çıktısını "yeniden kullanan" bir kod parçacığı da kullanılmalıdır (Giechaskiel vd., 2016).

Değerin korunumu için bir işlemin her girdisi önceki bir işlem çıktısıyla eşleşmelidir. Çünkü işlemler yalnızca, tüm işlem çıktılarının değerlerinin toplamının az olduğu temel kısıtlamayı karşıladığında geçerli olmaktadır (Dorri vd., 2019). Sistemin mülkiyeti bağlamında Bitcoin'in sahibi olan özdeş kimlikler ya da bireysel hesaplar bulunmamaktadır. Mülkiyet sadece belirli çıktıları tasdik ederek bir imza oluşturabilen özel bir anahtarın bilinmesi anlamına gelmektedir. Bunun yanı sıra bir birey kullanabileceği kadar çok

Bitcoin'e sahip olabilir. Ortak anahtar kareleri, pub-pub-key-hash işlemlerinde belirtildiği gibi sistem içinde sahte kimlikler olarak işlev görmekte ve adres olarak adlandırılmaktadır. Kullanıcının gerçek dünyadaki adı ya da tanımlayıcı bilgileri için bir bağlantı gerekmemektedir (Das vd., 2019).

Değer transferi işlemi yapmak için öncelikle alıcının adresini bilmek gereklidir. Gönderilecek olan miktar, adres bilgileri ve karşı tarafın açık anahtarı kullanılarak bir işlem üretilir ve bu işlem gönderen kişinin gizli anahtarı ile imzalanarak blok zincire taşınır. Eğer anahtarların imzalanmasında hata varsa işlem blok zinciri sistemi tarafından reddedilir. Bahsi geçen bu Bitcoin ağı ile işlem oluşturma süreci Şekil 2.8'de sunulmuştur.



Şekil 2.8. Bitcoin ağı ile işlem oluşturma süreci

İlişkisel veri tabanı yönetim sistemlerinde işlem yönetimi, 1970'lerde IBM Corporation içinde oluşturulan System R prototip RDBMS'nin (Relational Database Management System) geliştirilmesine destek olarak Jim Gray ve arkadaşlarının yürüttüğü çalışmalara dayanmaktadır (Gray, vd., 1981). Bir işlem, alınan eylemlerden bağımsız olarak tutarlılığı koruyan bir dizi eylem ve kurtarma birimidir. Bir veri tabanı nesnesi, tüm önermelerini karşıladığında tutarlı olacak şekilde tanımlanmaktadır. Bunu söylemenin bir başka yolu ise aynı veri tabanı nesnesine ilişkin herhangi iki işlemin bazı seri düzende yürütülmesi gerekliliğidir. Kaybedilen güncellemeler ve tutarsız analizler gibi bütünlük ihaleleri, herhangi bir veri tabanının önerilerini karşılamamakta ve tutarsızlığa yol açmaktadır (Lano, 2014).

Bir güncelleme işlemi sırasında, bir veri tabanı nesnesi yeni tutarlı bir duruma dönüştüğü için geçici olarak tutarsız hale gelmektedir. Potansiyel geçici tutarsızlık karşısında tutarlılığı sağlamak için işlemler tasarlanmıştır. Bir iş birimi ve bir kurtarma

birimi olarak ortak tanımların yanı sıra veri tabanını tutarlı bir durumdan başka bir tutarlı duruma geçirdiği için bir işlem tutarlılık birimi olarak da görülebilmektedir. Tüm geçici tutarsızlıklar işlem içinde yalıtılmakta ve asla veri tabanı tarafından görülmemektedir (Gray vd., 1976).

Söz edildiği gibi bir işlem hem bir iş birimi hem de bir kurtarma birimidir. Bir iş birimi olarak, bir veri tabanı üzerinde gerçekleştirilecek sınırlı sayıda SQL işlemini tanımlamaktadır. Bu işlemlerin tümü gerçekleştirilmeli ya da hiçbiri gerçekleştirilemez durumdadır. Buna işlemlerin "atomik mülkiyeti" denilmektedir. Duruma bağlı olarak, sınırlar örtülü ya da açık olarak tanımlanabilmektedir. Bir kurtarma birimi olarak, bir işlem mevcut tutarlı durumunu daha önceki tutarlı bir duruma geri döndürmek için bir veri tabanı üzerinde gerçekleştirilecek sınırlı bir geri alma işlemi dizisini tanımlamaktadır (Fortier ve Howard, 2003). Bu ifadelerin veri tabanı işlemleri açısından özel anlamları Tablo 2.4'te tanımlanmıştır.

Tablo 2.4. İşlemlerin ACID (Atomicity, Consistency, Isolation, ve Durability) özellikleri

İşlemlerin ACID Özellikleri	**Açıklama**
Atomiklik (Atomicity)	Bir işlem ya olur ya hiç olmaz. Bir atomik işlem içinde peş peşe kaç adet işlem olursa olsun her birisi toplu halde gerçekleşip sonlanmalı ya da her birisi iptal olup geri sarmalı. Kısmi işlem gerçekleşemez.
Tutarlılık (Consistency)	İşlem, veri tabanını bir tutarlı durumdan bir başka tutarlı duruma taşır. Ara tutarsız durumların oluşmasına izin verilmez. Bu konuda Date (2003, 2004) çalışmalarında, "Eğer veri tabanı kısıtlamaları doğru şekilde oluşturulursa, tutarlılık sıra dışı bir özellik değil, mantık çerçevesinde gerekli bir durumdur ve İşlem yöneticilerinin ana hedefinin veri tabanı tutarlılığını sağlamak olmalıdır." diye belirtmektedir.
İzolasyon (Isolation)	Bir işlem başlayıp sonlanana kadar diğer tüm işlemlerden gizli tutulur, birbirlerine işlem sırasında müdahale edilmesine izin verilmez. İzolasyon serileştirilebilir kelimesi ile eş anlamlıdır.
Devamlılık (Durability)	Bir işlem tamamlandıktan sonra, yeni durum alt yapıyı oluşturan sistem çökse bile geçerliliğini korur. Devamlılık ve kalıcılık anlamlı olarak kullanılır.

2.11. İşlem Zamanlayıcıları ve İşlem Geçmişleri

İşlem zamanlayıcısı; eklenmiş kümenin çeşitli okuma, yazma, işleme ve geri alma işlemlerinin yürütüldüğü sırayı sınırlandırarak aralıklı işlemlerin eş zamanlı yürütülmesini denetleyen yazılım olarak tanımlanabilir. İşlem planlayıcılarının amacı, sistemdeki tüm işlemlerin hem bağımsız sürdürülebilir hem de kurtarılabilir olması açısından doğru olmasını sağlamaktır. Bir işlem programlayıcısının temel görevlerinden biri, kilitlenmelerin önüne geçmektir. Eş zamanlı olarak çalışması açısından eğer çakışan veri erişimi gereksinimlerine sahip olan işlemler mevcutsa bu işlemlere izin verilmemelidir. Başka bir deyişle, işlem zamanlayıcısı iki işlemin birbiriyle çelişen modlarda aynı veri tabanı nesnesini kilitlemesinin önüne geçmektedir (Tian vd., 2018).

Bir işlem kümesinin okuma ve yazma işlemleri bir araya getirildiğinde işlem geçmişi oluşturulmaktadır. İşlem geçmişleri, işlem zamanlayıcısının oluşturduklarının bir modeli olarak tanımlanabilir. Eş zamanlılık çok kullanıcılı bir ortamda açık bir şekilde olumlu bir olgu olup işlem setlerinin adımlarını birleştirerek eş zamanlılık elde etmenin en iyi yoludur. Eş zamanlı olarak işlemler yürüterek daha da yüksek verimlilik elde etmek olasıdır. Bazen tam olarak anlaşılmayan veri tabanı tutarlılığı, maksimum eş zamanlılık elde etmekten daha cazip olabilmektedir. Sonuç olarak, araya giren eş zamanlı işlemler her zaman veri tabanının tutarlılığı açısından zararsız olmalıdır (Ezio Bartocci ve Falcone, 2018).

Doğru işlem geçmişi, seri hale getirilebilir bir yapıda olmalıdır. Bir diğer deyişle, bir işlem kümesinin okuma ve yazma işlemleri, her bir işlemin okuma ve yazma işlemlerinin değerlerini etkilenmeden birlikte yeniden sıralanabilir olmalıdır (Bailis vd., 2014).

Bir seride olan işlemler aynı göreceli düzende kaldığında, seri hale getirilebilirlik sağlanmış olur. Örneğin, Tx1 işleminin, Tx2 işlemi okunmadan önce yazması durumunda, Tx1 işlemi Tx2 işleminden önce serileştirilmelidir. Bunu söylemenin başka bir yolu da, sistemin bir tarihte herhangi bir işlemin tüm işlemlerinin, modelledikleri gerçek işlemle aynı düzene sahip olması gerektiğini garanti etmesi gerektiğidir. Tam bir işlem geçmişi, geçmişte her işlem için bir işlemi sona erdirme ya da geri alma da dahil olmak üzere birden çok işlemin yürütülmesini sağlayan bir işlem dizisi olarak tanımlanabilir (Viktor vd., 2014).

Bir işlemin en yaygın kullanılan örneği, bir banka ATM'si tarafından üstlenilen borç-kredi işlemidir. Örneğin, bir kişinin döviz hesabından 10 dolar çekeceğini ve tasarruf

hesabına yatıracağı varsayımı üzerine bir senaryo üretildiğinde bu döviz hesabından (borç aşamasından) para çekilmesi ve tasarruf hesabına (kredi aşaması) yatırılması olmak üzere iki aşamalı bir işlem söz konusudur. İşlemin borçlanma aşamasının başarıyla tamamlandığını, ancak kredi aşamasının yapılmadığı düşünüldüğünde, söz konusu o 10 doların kaybolması gündeme gelebilir. Burada söz edilen senaryoda, işlem yöneticisi para yatırılmadığı zaman, para çekme işlemini geri almaktadır. Bu işlem atomik kabul edilmektedir çünkü ya hepsi gerçekleşir ya da hiçbiri gerçekleşmez bir niteliğe sahiptir. İşin sadece bir bölümü gerçekleştirilemediğinden dolayı atomik olarak tanımlanmaktadır. ANSI oturum modu işlem semantiklerinden farklı olarak, sistem bir hata döndürdüğünde, sistem otomatik olarak Teradata oturum modundaki işlemleri geri almaktadır. Ayrıca bir işlem tarafından gerçekleştirilen iş ABORT ya da ROLLBACK deyimleri kullanılarak da açıkça geri alınabilmektedir (Stegelmann, 2000).

Burada sorun, merkezi otorite olmaması durumunda işlemlerin nasıl başlatılabileceğidir. Klasik bir bankacılık sisteminde, müşteri hizmet danışmanından destek almakta ya da ödeme talimatlarını bankanın çevrimiçi bankacılık hizmeti aracılığıyla sunmaktadır. Ticari banka ve diğer merkezi hizmet sağlayıcıları tarafından sağlanan altyapı, işlemin yürütülmesi için gerekli iletimi sağlamaktadır. Merkezi bir otoritenin yokluğunda, geleneksel anlamdaki bu ödeme emrini iletmek mümkün değildir (Berentsen ve Schär, 2018).

Bitcoin sisteminde ise, herhangi bir sayıda ağ düğümüne bir ödeme emri iletilebilmektedir. Elektronik ağ düğümleri gevşek bir ağda birbirine bağlanmakta ve tüm düğümler işlem hakkında bilgilendirilene kadar iletiyi iletmektedirler. Bu noktada sistemin dağıtık olmasının birçok avantajı olduğu söylenebilir. Özellikle, bu dağıtık yapı sistemi son derece sağlam hale getirmektedir. Ne saldırıya uğrayabilecek bir merkezi hata noktası ne de sistemin çökmesine neden olabilecek sistemle ilgili düğümler yer almadığından dolayı sistem dayanıklı olarak tanımlanmaktadır. Bu dağıtık yapıda, sistem bazı ağ düğümlerine ulaşılamadığında bile çalışabilmektedir. Aynı zamanda sürekli olarak yeni bağlantılar ve iletişim kanalları kurabilmek mümkündür (Moosbrugger vd., 2017).

İşlem meşruiyeti ödeme emri mesajları sürecinde önemli bir sorun olarak gündeme gelmektedir. Her katılımcı yeni ödeme emirleri oluşturabilir ve bunları ağ üzerinden

yayınlayabilir. Bu özellik hileli mesajların gönderilme riskini de taşımaktadır. Bu bakımdan, aşağıda belirtilen iki önemli soru gündeme gelmektedir:

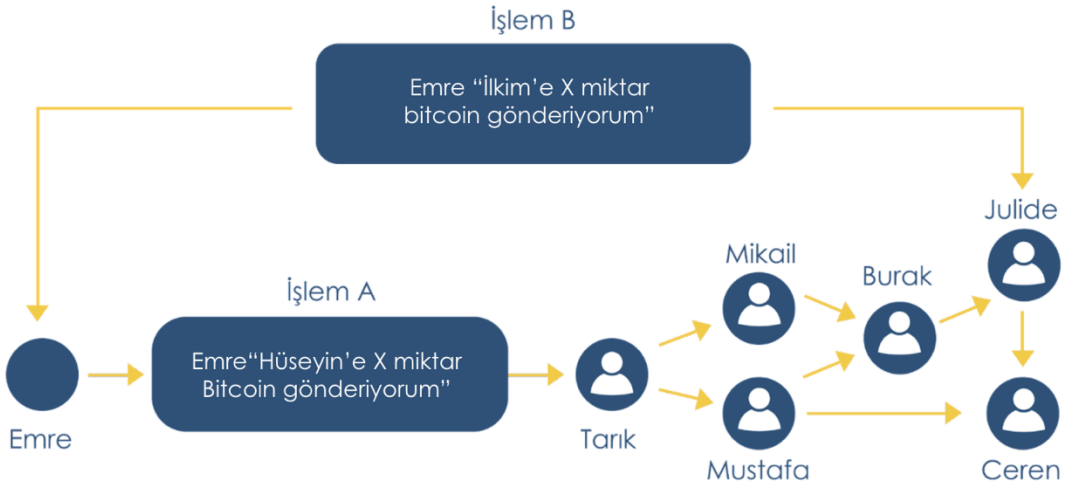
1. Düğümler, işlem başlatıcısının hak sahibi olduğunu ve bu nedenle Bitcoin ünitelerini transfer etme hakkına sahip olduğunu nasıl bilecektir?

2. İşlem mesajının bir düğümden diğerine geçmeden önce başkası tarafından okunmayacağına nasıl emin olunacaktır?

Bitcoin sisteminde, asimetrik kriptografi kullanılarak işlem geçerliliği garanti altına alınmıştır. Çözüm yolu, özel ve açık anahtarlardan oluşan anahtar çiftlerini kullanmayı gerektirmektedir, özel bir anahtar paylaşılmamaktadır. Bu durum ise inanılmaz derecede büyük bir sayı grubundan rastgele bir değere karşılık gelmektedir. Diğer taraftan, bir ortak anahtar bu sayıdan türetilmekte, serbestçe paylaşılabilmekte ve Bitcoin ağında bir takma ad olarak hizmet edebilmektedir (Berentsen ve Schär, 2018).

Özel bir anahtar, yalnızca karşılık gelen ortak anahtar kullanılarak deşifre edilebilen bir mesajı şifrelemek için kullanılmaktadır. Şifreleme türü de "imza" olarak bilinmektedir. Bu durum sözü geçen imzanın şifrelenmiş mesajdaki herhangi bir bilgiyi gizlemek için kullanılmadığı anlamına gelmektedir. Herkes kendi özel anahtarını kullanarak bir mesajın şifresini çözebilir. Ancak bu imza, mesajın ilgili özel anahtarı kullanılarak daha önce şifrelenmiş olduğuna dair bir ispat olarak hizmet etmektedir. El yazısı imzadan çok daha güvenilir kabul edilmektedir (Umar, 2003). Örneğin, Bitcoin ağı üzerinden A kişisine Bitcoin ödemesi yapmak isteyen B kişisinin ele alındığı bir senaryo olduğunu varsaydığımızda B kişisi mesajı şifrelemek için özel anahtarını kullanmaktadır. Diğer ağ katılımcıları bu mesajı sadece B kişisinin açık anahtarını kullanarak çözebilmektedir. Bir girişim başarılı olursa, mesajın karşılık gelen özel anahtarı kullanılarak şifrelenmesini sağlamaktadır. Başka birinin B kişisinin özel anahtarına erişimi olmadığından, bu yaklaşım işlemin kaynağını doğrulamak için kullanılabilmektedir. İşlem ağda dolaştığı zaman, herhangi bir ağ katılımcısı bu mesajın şifresini çözebilir ve daha sonra ödeme talimatlarını değiştirmek için konum alabilmektedir. Ancak, katılımcı B kişisinin özel anahtarına sahip olmadığı için, önceki mesajı yeniden şifreleyemez. Bu nedenle, değiştirilmiş işlem, ağın geri kalanı tarafından tanımlanmakta ve reddedilmektedir. Böylece sistemin güvenli hale geldiği kabul edilmektedir (Koops, 1999).

Bir işlem mesajının nasıl iletildiği ve kaynağının nasıl doğrulanabileceği önemli bir sorundur. Bitcoin birimlerinin sahiplenilmesine ilişkin fikir birliğinin, iş ispatı uzlaşma protokolünü kullanarak Bitcoin ağında nasıl elde edildiği A kişisi ve B kişisi örneği üzerinden bir senaryo ile açıklanmıştır (Şekil 2.9). Bununla birlikte, B kişisi, aynı Bitcoin birimlerine referans veren iki işlem üretebilecektir. Her iki işlem de ağ üzerinden eş zamanlı olarak yayılabilecek (aktarım yeteneği) ve her ikisi de geçerli bir işlem meşruluğu gösterecektir. Bu iki mesajın Bitcoin ağında yayılmasındaki farklılıklardan ötürü, bazı düğümler işlem X için bir mesaj alırken diğerleri işlem Y için bir mesaj alacaklardır. Çift harcama olmasının engellenebilmesi için, iki işlemden sadece birinin Bitcoin blok zincirine girmesi önemlidir. Bu noktada iki işlemden hangisinin blok zincirine dahil olduğuna karar veren bir mekanizma gerekli hale gelmektedir. Bitcoin sistemi bu çift harcama ihtimalini ortadan kaldırabilme yeteneğine sahiptir. Geçerli bir blok adayına eklenen ve bu yüzden blok zincirine eklenmiş olan bir işlemin muhakeme edildiği kabul edilmektedir. Madenciler sözleşmelerini blok adaylarına eklemekten vazgeçmektedir. Böyle bir blok gayri meşru olacak ve dolayısıyla diğer tüm ağ katılımcıları tarafından reddedileceği için bir madenci için aynı blok adayıyla sözleşme imkanı söz konusu değildir (Rubasinghe, 2017). Yukarıdaki senaryoda bahsi geçen çift işlem (İşlem A ve İşlem B) doğrulama sistemi Şekil 2.9'da sunulmuştur.



Şekil 2.9. Çift İşlem Doğrulama Sistemi

2.12. Bölüm sonucu

Bu bölümde, dağıtık atomik takas için sisteminin temelini temsil eden kripto para yapıları, bu sistemlerin tarihsel gelişimi, kripto paranın alt yapısını oluşturan blok zincir ve açık anahtar şifreleme, hash fonksiyonları gibi kriptoloji teknolojileri ile ilgili literatürel bilgi sunulmuştur. Ayrıca bu teknolojilerin uygulama alanı bulduğu kriptolojik para cüzdanı ve cüzdanlardan geçen işlemlerin tanımlandığı alt yapılar sunulmuştur. Literatür bilgisi çeşitli veri tabanlarındaki akademik çalışmalar ve kripto alanında güvenilir haber kaynaklarından derlenmiştir. Bu bölümde konu ile ilgili kavramsal bilginin sunumunun ardından 3. bölümde tez çalışmasının orijinal çıktısı olan *Dağıtık Atomik Takas Modeli*'nin yöntemi ve akış şeması ifade edilmiştir.

BÖLÜM 3. YÖNTEM

Bu çalışma kapsamında söz konusu sistem geliştirilirken öncelikle piyasadaki mevcut kripto para sistemleri ve alt yapıları incelenerek değişim mantığı ve haritası çıkarılmış olup, çevik yazılım geliştirme (Agile Software Development) geliştirme yöntemi kullanılmıştır.

Amaçlanan bu sisteme uygun bir takas yöntemi ve borsası tasarlanmış olup bu proje kodlanarak gerçek hayatta denenmiştir. Atomik işlemler tasarlanırken mevcut veri tabanı sistemleri (ACID- Atomiklik, Tutarlılık, İzolasyon, Devamlılık), asenkron ağlardaki dağıtık işlem sistemleri ve mevcut kripto para borsası incelenerek tüm sisteme uygun genel bir işlem (transaction) yapısı oluşturulmuştur.

Oluşturulan bu yapının ardından, takas işi genelleştirilerek en büyük takas aracı olan Merkez Bankaları'nın kullanabilecekleri bir para altyapısı sunularak sistem tamamlanmıştır. Bu sistem tasarlanırken yöntem olarak öncelikle tüm kripto para birimlerinin farklı özellikleri ve avantajları listelenmiş, Merkez Bankaları'nın ihtiyaçları göz önünde bulundurularak tasarım gerçekleştirilmiştir.

3.1. Araştırma Modeli

İnsanlar çeşitli kripto paralarını, birbirleriyle özgür ve güvenli bir biçimde takas işlemi yapabilmektedir. Günümüzde bu takas işlemi merkezi kripto para borsaları aracılığıyla gerçekleşmektedir. Bu merkezi kripto para borsalarında kullanıcılar takas yapmak istedikleri kripto paraları bu borsalara göndermektedir. Bu durum kullanıcıların zaman zaman hileye maruz kalmalarına ya da borsa çalışanları tarafından oluşabilecek hırsızlık risklerine sebep olabilmektedir. Bu riskleri ortadan kaldırmak için tez çalışmasının literatür kısmında da olumlu özellikleri sunulan merkezi olmayan, dağıtık kripto para borsaları üzerine çalışmalar yapılmaktadır.

Bahsi geçen merkezi olmayan kripto para borsalarının çalışması iki ana başlık altında incelenebilir; emir eşleştirme ve atomik takas.

Olağan bir senaryoda iki kişinin takas yapmaları için önce fiyat üzerinde anlaşmaları gerekmektedir. Merkezi olmayan bir borsada bu işlem yine kripto paralarda olduğu gibi blok

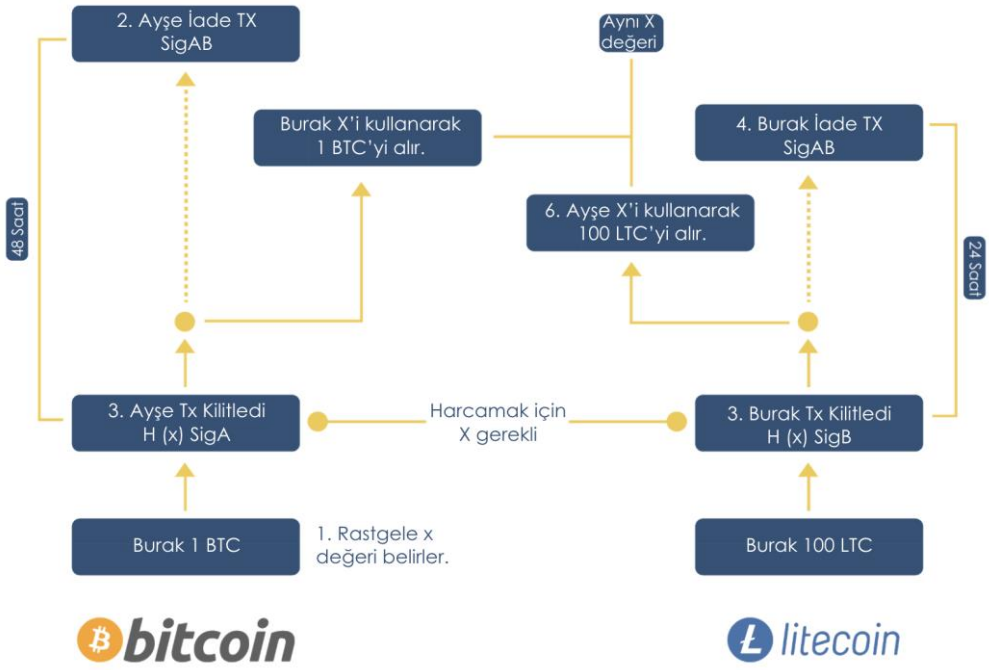
zincir teknolojisi kullanılarak sağlanmaktadır. Aslında, borsanın kendisi de bir kripto para olarak kabul edilebileceğinden dolayı borsanın çalışması için merkezi bir sunucuya gereksinim duyulmamaktadır. Ayrıca atomik takas sırasında tarafların anlaşmayı tamamlamaları için gerekli özendiriciliği ve caydırıcılığı sağlama amacıyla da bu kripto para kullanılmaktadır. Bu kısımda Atomik Takas örnek bir senaryo eşliğinde sunulacaktır.

3.2. Atomik Takas Örnek Senaryo

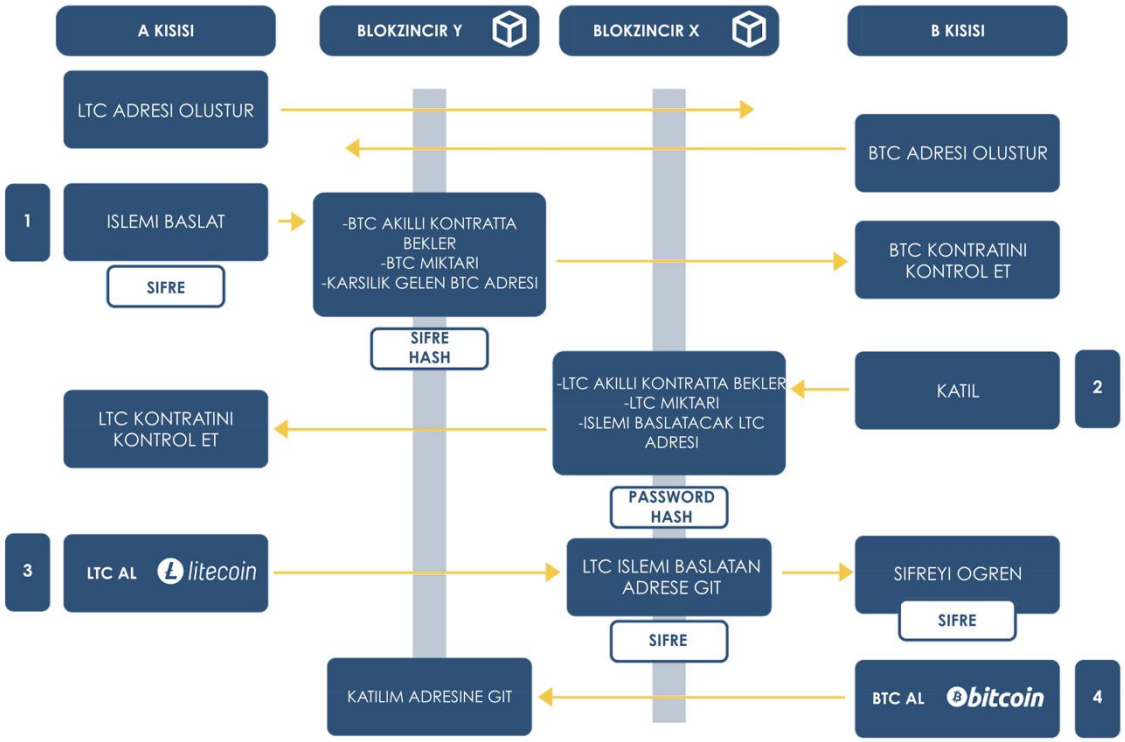
Emir eşleştirme sırasında anlaşılan miktarların karşılıklı olarak karşı tarafa güven gerektirmeyecek şekilde gerçekleştirilebilmesi için atomik takas yapılır. Normal bir atomik takas işlemi aşağıdaki şekilde yapılır:

- A ve B kişilerinin 100 Litecoin (LTC) karşılığında 1 Bitcoin (BTC) için anlaştığını varsayalım. A kişisi, B kişisine 1 BTC gönderecek, B kişisi ise A kişisine 100 LTC gönderecektir.
- Blok zincirlerde kripto paralar bir adrese gönderilebildiği gibi, bir Script'e de gönderilebilir. Betiklerin sonucunu doğru döndüren girdilerle bu kripto paralar başka adreslere ya da başka betiklere gönderilebilir.
- A kişisi kendi bildiği bir şifre ile B kişisinin adresine ya da uzun bir süreden sonra kendi adresine gönderilebilecek bir betiğe 1 BTC gönderir.
- B kişisi, A kişisinin şifresi ile A kişisinin adresine ya da kısa bir süreden sonra kendi adresine gönderilebilecek bir betiğe 100 LTC gönderir.
- Eğer A kişisi, B kişisinin gönderdiği betikten 100 LTC'yi kendi adresine gönderirse, diğer kişilere ve B kişisine şifresini göstermiş olur.
- Böylece B kişisi, A kişisinin 1 BTC gönderdiği betikten kendi adresine aynı şifreyi kullanarak 1 BTC'yi gönderebilir.
- Eğer A kişisi B kişisinin betiğe girdiği süre sonunda 100 LTC'yi kendi adresine göndermezse süre dolduğundan B kişisi 100 LTC'yi kendi adresine gönderir.
- A kişisi de daha uzun olan kendi süresi doluncaya kadar bekleyip 1 BTC'yi kendi adresine gönderebilir.
- Yani ya iki işlem de gerçekleşmekte ya da iki işlem de gerçekleşmemektedir.

Dağıtık kripto para borsasında bu sürece bazı zorluklar dahil olmaktadır. Örneğin bekleme süreleri sebebiyle taraflar arasında fikir değişiklikleri gündeme gelebilmektedir. Bu bekleme süreleri zarfında ilkin anlaşılan fiyatın taraflardan biri için karlılığını yitirmesi sonucunda taraflardan birinin takastan vazgeçebilme ihtimali bulunmaktadır. Yaşanan bu durumu engellemek üzere caydırıcı önlemler almak gerekmektedir. Genel olarak işleme başlamadan önce takasa konu olan değerin belirli bir oranı borsanın kripto parası cinsinden rehin bırakılmakta ve ancak kendi sorumluluğunu yerine getiren tarafa geri verilmektedir (Şekil 3.1 ve Şekil 3.2).



Şekil 3.1. Atomik Takas Senaryo



Şekil 3.2. Atomik Takas Senaryo

3.3. Bulgular

Bu bölümde, tez çalışması kapsamında tasarlanan modelin kodu sunulmuştur. Model; Python programlama dili ile geliştirilmiş olup, takas için gerekli olan girdilerin sağlanması ve iptal işlemlerini içermektedir. Mal takas etmek isteyen birisi, doğal olarak hırsızlık ve dolandırıcılığa maruz kalmamak ve en uygun orandan en az masraf ile takas yapmak istemektedir. Kripto para borsalarının yeni olmasından dolayı takas sistemi henüz düzenlenmemiş ve gelişmemiştir. Bu borsalardaki takas herhangi iki para birimi arasındaki takastan farksızdır. Borsalarının 7/24 açık olması ve programlanabilir yapıları sebebiyle kripto paralar gün geçtikçe pek çok alanda kullanıcıların ilgisini çekmektedir. Kullanım sırasında karşılaşılan zorluklar ve alınan riskler değerlendirildiğinde, dünyadaki tüm kripto para çevrelerinde bu beklentilere benzer beklentiler olmasına karşın; piyasalarda bu beklentileri karşılayan bir borsa bulunmamaktadır.

Bu çalışma kapsamında; söz konusu özel blok zincir teknolojisi, atomik takas yöntemi ve ödeme kanalları teknolojileri kullanarak piyasadaki büyük merkezi borsalar kadar iyi oranların olduğu, kripto para kullanıcılarının mevcut borsalardaki risklere girmeden en az masraf ödediği, hacklenme, hırsızlık ve dolandırıcılığın mümkün olmadığı;

bunun yanı sıra mevcut borsaların sağladığı tüm imkanlardan faydalanabildiği, merkezi olmayan bir kripto para borsası modeli geliştirilmiştir.

Bu çalışma sürecinde tasarlanan atomik takas modeli kapsamında, merkezi borsalarda kullanıcıların takas yapabilmeleri için önce sahip oldukları kripto paraları borsanın kendi hesabına göndermelerinden kaynaklanan kripto paraların tek bir havuzda toplanması sorununa çözüm üretilmektedir. Atomik takas modeli ile kullanıcıların kripto paraları takas gerçekleşene kadar kendi sahip olduğu cüzdanlarda beklemesi sağlandığından dolayı merkezi dolandırılma tehlikesi de ortadan kalkmaktadır. Bu akış şemasının matematiksel modeli bir sonraki bölümde detaylı olarak formüller ile açıklanmıştır. Bunun yanı sıra, *takas işlemlerinde birden çok kullanıcı, şifre, hash fonksiyonu, zaman ve para transferleri* gibi öğeleri içeren algoritmalar matematiksel bir model içerisinde sunulmuştur.

3.3.1 Takas Algoritması Formülleri

Bu bölümde takas algoritması matematiksel notasyonlar kullanılarak açıklanmıştır. İlk aşamasında notasyonların karşılık geldiği formüller ve açıklamalara yer verilmiş, ardından bu matematiksel açıklamaların kurduğu denklem detaylandırılarak takas sistemi formüller ile açıklanmıştır.

Takas algoritmasının matematiksel modelinin anlatımında kullanılacak ifadelerin açıklamaları aşağıda belirtilmiştir:

A: A kişisinin sahip olduğu adresten türetilen imza

B: B kişisinin sahip olduğu adresten türetilen imza

$S_1, S_2, S_3 \dots S_n = hash(n) \mid n \in N^+$: Belirli bir uzunlukta ve istenilen özeti üretebilecek şifre

$T_1, T_2, T_3 \dots T_n = time(n) \mid n \in N^+$: Zaman kesitleri

$\{T_i : i \in N^+, \forall T_i \in time(i) \mid T_i < T_{i+1}\}$: her bir zaman kesitinde, sayı büyüdükçe zaman kesiti daha ileri bir zamanı ifade eder.

$K_1, K_2, K_3 \ldots K_n$: $krip(n)$Farklı kripto paraları ifade eder.

$X_1, X_2, X_3 \ldots . X_n$: Farklı miktarları temsil eder.

{} : Adres.

$\{\{K_i\,(X): D\} \mid K_i \in krip(n), X \in N^+, D \in signature(d)\}$:

Adresleri yazarken **{**Kripto para cinsi x Miktar: İmza**}** şeklinde, parantez içerisinde kripto para cinsi, miktar ve imza kuralı şeklinde ifade edilmektedir.

ÖR: {K1x1: A}

$\Rightarrow (A_i, T_i) \Rightarrow$: Transfer işlemini ifade etmektedir.

Transfer işlemi içerisinde yer alan imza, işlem yapılırken sisteme yazılacağı için herkes tarafından öğrenilmiş olmakta ve zaman tamamlanmış ise yanında yer almaktadır.

3.3.2. Takas Algoritması Açıklamaları

Kripto para transfer işleminde, RSA temelli bir algoritma kullanıldığı için o kişinin iki çeşit anahtarı bulunmaktadır. Bunlardan ilki olan gizli anahtar, açık anahtarı üretmeye aracılık etmektedir. Açık anahtar tüm paydaşlara açık şekilde paylaştırılmakta ve kişinin kimliğinin doğrulanması amacıyla kullanılmaktadır. Bir kişinin gizli anahtarı ile imzaladığı işlemi, diğer kişi açık anahtarı ile o kişiye ait olup olmadığını öğrenecek şekilde doğrulayabilmektedir.

Notasyon olarak ilk başta belirlenen formüllerde, büyük harfler, bir şahsa ait o adresten türetilen imzayı temsil etmektedir. Bitcoin adresleri, içindeki kripto paralar küçük köşeli parantez adresi ile o adresten transfer yapabilecek imza ise köşeli parantez içinde ifade edilmektedir.

Örneğin **{**A**}**, A imzası ile transfer edilebilen bir adresteki kripto parayı temsil edecektir.

Basit adreslerin yanında kripto paralarda belirli bir fonksiyon içeren adresler de bulunmaktadır. Bu tarz adresler atomik takas ve ödeme kanalları gibi yöntemlere olanak sağlamaktadır.

Örneğin, $\{K_1(X): A|B\}$ gibi iki kişinin de tek başına kullanabileceği veya $\{K_1(X): A\&B\}$ gibi iki kişinin de hemfikir olmasıyla kullanılabilecek adresler tanımlanabilir.

Bunların yanı sıra, zaman kilitli ya da hash kilitli adresler de tanımlanabilmektedir.

Örneğin, $\{K_1(X): (A\&T_2)|(B\&S_1)\}$ adresi T_2 anından itibaren A imzası ile veya S_1 şifresi ve B imzası ile transfer edilebilecek bir adresi temsil etmektedir. S_1 şifresinin hash değeri, A ve B nin açık anahtarı adres içerisinde açıkça yazmalıdır. Ardından transferi yapabilmek için S_1 şifresini açıkça içeren transaction B ile imzalanmalıdır ya da T_1 'den sonra ise A ile imzalanmalıdır.

3.3.3. Atomik Takas Algoritması

Atomik takas işleminin ideal durum senaryosu ise aşağıda sırasıyla Eş. 3.1 ile 3.4 arasında belirtildiği şekliyle gerçekleşmektedir:

$$\{K_1(1): A\} \Rightarrow (A,) \Rightarrow \{K_1(1): (B\&S_1)|(A\&T_2)\} \quad (3.1)$$

$$\{K_2(2): B\} \Rightarrow (B,) \Rightarrow \{K_2(2): (A\&S_1)|(B\&T_1)\} \quad (3.2)$$

$$\{K_2(2): (A\&S_1)|(B\&T_1)\} \Rightarrow (A, S_1) \Rightarrow \{K_2(2): A\} \quad (3.3)$$

$$\{K_1(1): (B\&S_1)|(A\&T_2)\} \Rightarrow (B, S_1) \Rightarrow \{\{K_1(1): B\} \quad (3.4)$$

Yukarıda formüle edilmiş sistemde iki adet anormal durum oluşması riski söz konusudur. Bu anormal durumlardan ilki; A kişisi ile B kişisi arasında geçecek işlemde B kişisi aldığına karşılık gelen ödemeyi yapmaz ise oluşmaktadır. Bu durumda işlem sırası Eş. 3.5 ve Eş. 3.6 görüldüğü gibi olacaktır:

$$\{K_1(1): A\} \Rightarrow (A,) \Rightarrow \{K_1(1): (B\&S_1)|(A\&T_2)\} \quad (3.5)$$

$$\{K_1(1): (B\&S_1)|(A\&T_2)\} \Rightarrow (A\&T_2) \Rightarrow \{K_1(1): A\} \quad (3.6)$$

Diğer bir anormal durum ise, A kişisi ona gönderilen ödemeyi çekip işlemi tamamlamaz ise oluşmaktadır. Bu durumda işlem sırası Eş. 3.7 ile Eş 3.10 arasında belirtilen şekilde olacaktır:

$$\{K_1(1): A\} \Rightarrow (A,) \Rightarrow \{K_1(1): (B\&S_1)|(A\&T_2)\} \quad (3.7)$$

$$\{K_2(2): B\} \Rightarrow (B,) \Rightarrow \{K_2(2): (A\&S_1)|(B\&T_1)\} \quad (3.8)$$

$$\{K_2(2): (A\&S_1)|(B\&T_1)\} \Rightarrow (B\&T_1)) \Rightarrow \{K_2(2): B\} \quad (3.9)$$

$$\{K_1(1): (B\&S_1)|(A\&T_2)\} \Rightarrow (A\&T_2) \Rightarrow \{\{K_1(1): A\} \quad (3.10)$$

3.3.4. Ödeme kanalları

Ödeme kanalları teknolojisi, bir müşterinin bir ödeme kanalı sağlayıcısı birden çok defa alışveriş yapması durumunda her seferinde komisyon ödememesi için tasarlanmış bir sistemdir. Ayrıca bu metodoloji ile ödemeler blok zincire göre çok daha hızlı olabilme fırsatını yakalamaktadır. Müşteri ilk olarak ödeme kanalına para göndermekte, sonra imzasını kullanarak parçalı olarak daha küçük ödemeler yapabilmektedir. Kanal süresi dolmadan da bu ödeme kanalı sağlayıcısı parayı kendi adresine çekebilmektedir.

Bu durumda gerçekleşen işlemlerin sırası Eş. 3.11 ile Eş. 3.14 arasında belirtilen şekilde olacaktır:

$$\{K_1(1): A\} \Rightarrow (A,) \Rightarrow \{K_1(1): A\&(B|T_1)\} \quad (3.11)$$

$$\{K_1(1): A\&(B|T_1)\} \Rightarrow (A,) \Rightarrow \{K_1(2): B\} + \{K_1(3): A\} \quad (3.12)$$

$$\{K_1(1): A\&(B|T_1)\} \Rightarrow (A,) \Rightarrow \{K_1(4): B\} + \{K_1(5): A\} \quad (3.13)$$

$$\{K_1(1): A\&(B|T_1)\} \Rightarrow (A,) \Rightarrow \{K_1(6): B\} + \{K_1(7): A\} \quad (3.14)$$

...

...

$$\{K_1(1): A\&(B|T_1)\} \Rightarrow (A\&B,) \Rightarrow \{K_1(N): B\} + \{K_1(N+1): A\} \quad (3.15)$$

Ve

$$X_1 = X_2 + X_3 = X_4 + X_5 = X_n + X_{n+1}$$

$$X_2 < X_4 < X_6 \ldots . X_n < X_{n+2} \mid n \in çift\ doğal\ sayılar$$

Her ödeme işlemi, aralarındaki işlemin farkı kadardır. 2, 3 ve 4 numaralı takas işlemleri yarım imzalı olduğundan blok zincirde yayınlanmamaktadır. Bu sayede aradaki işlemler daha hızlı gerçekleşebilmektedir. Bu işlemlerin sonunda sadece birinci ve sonuncu takas işlemleri yayınlanmaktadır.

3.3.5. Atomik takaslı ödeme kanalları

Ödeme kanallarında kullanılan atomik takas yapısı ise Tablo 3.1'de belirtilen formüllerle gerçekleştirilmektedir.

Tablo 3.1. Ödeme Kanallarında Kullanılan Atomik Takas Yapısı Formülü

No	Denklem
1	$\{K_1(1): A\} \Rightarrow (A,) \Rightarrow \{K_1(1): A\&(B\|T_2)\}$
2	$\{K_2(2): B\} \Rightarrow (B,) \Rightarrow \{K_2(2): B\&(A\|T_1)\}$
3	$K_1(1): A\&(B\|T_2)\} \Rightarrow (A,) \Rightarrow \{K_1(3): (B\&S_1)\|(A\&T_2)\} + \{K_1(4): A\}$
4	$\{\{K_2(2): B\&(A\|T_1)\} \Rightarrow (B,) \Rightarrow \{K_2(5): (A\&S_1)\|(B\&T_1)\} + \{K_2(6): B\}$
5	$\{K_1(1): A\&(B\|T_2)\} \Rightarrow (A,) \Rightarrow \{K_1(7): (B\&S_2)\|(A\&T_2)\} + \{K_1(8): A\}$
6	$\{K_2(2): B\&(A\|T_1)\} \Rightarrow (B,) \Rightarrow \{K_2(9): (A\&S_2)\|(B\&T_1)\} + \{K_2(10): B\}$
7	$\{K_1(1): A\&(B\|T_2)\} \Rightarrow (A,) \Rightarrow \{K_1(11): (B\&S_3)\|(A\&T_2)\} + \{K_1(12): A\}$
8	$\{K_2(2): B\&(A\|T_1)\} \Rightarrow (B,) \Rightarrow \{K_2(13): (A\&S_3)\|(B\&T_1)\} + \{K_2(14): B\}$
…	…
n-3	$\{K_1(1): A\&(B\|T_2)\} \Rightarrow (A\&B,) \Rightarrow \{K_1(11): (B\&S_3)\|(A\&T_2)\} + \{K_1(12): A\}$
n-2	$\{K_2(2): B\&(A\|T_1)\} \Rightarrow (B\&A,) \Rightarrow \{K_2(13): (A\&S_3)\|(B\&T_1)\} + \{K_2(14): B\}$
n-1	$\{K_1(11): (B\&S_3)\|(A\&T_2)\} \Rightarrow (B, S_3) \Rightarrow \{K_1(11): B\}$
n	$\{K_2(13): (A\&S_3)\|(B\&T_1)\} \Rightarrow (A, S_3) \Rightarrow \{K_2(13): A\}$

burada miktarların birbirleri arasındaki ilişki aşağıdaki gibidir, her ödeme aralarındaki fark kadardır.

$$X_1 = X_3 + X_4 = X_7 + X_8 = X_{11} + X_{12} \ldots . X_n + X_{n+1}$$

$$X_2 = X_5 + X_6 = X_9 + X_{10} = X_{13} + X_{14} \ldots . X_n + X_{n+1}$$

$$X_3 < X_7 < X_{11} \ldots X_n < X_{n+3}$$
$$X_5 < X_9 < X_{13} \ldots X_n < X_{n+4}$$

3.3.6. Yüksek Hız ve Derinlikli Merkezsiz Borsa:

Atomik takas yapısı yüksek güvenlik sağlarken, merkezi borsalardaki hız ve derinliğe ulaşamamaktadır. Bunun nedeni blok zincirlerde işlemlerin uzun sürmesi ve çok hızlı işlem yapması gereken ve borsalara derinlik katan piyasa yapıcı yatırımcıların bu borsalardan uzak durması olarak sıralanabilir. Atomik takas ve ödeme kanalı birleşimi çok hızlı işlemlere izin verdiği için kanal sağlayıcı adında yeni bir yatırımcı türüyle normal yatırımcılar ve piyasa yapıcılar arasında köprü oluşturulması sağlanabilmektedir. Bu işlemlerde kazanç modeli komisyon olacak ve merkezi borsaların komisyon oranlarından çok daha az oranda komisyon alınması yeterli olacaktır.

Piyasa yapıcılar kanal sağlayıcılar ile 2 ayrı blok zincirde ödeme kanalı oluştururlar. Kanal sağlayıcılar normal borsa kullanıcıları ile normal atomik takas işlemi yaparken, piyasa sağlayıcılar ile bu işlemin tersi yönde atomik takaslı ödeme kanalı işlemi yapmaktadırlar. Bu senaryon Tablo 2.6'daki formüller ile ifade edilmiştir.

A piyasa yapıcı, B normal kullanıcı ve C kanal sağlayıcı olduğuna göre,

Burada,

$$X_1 = X_3 + X_5 = \ldots . X_n + X_{n+2}$$
$$X_2 = X_4 + X_6 = \ldots . X_n + X_{n+2}$$

Kanal sağlayıcı ve piyasa yapıcı son işlemleri yapmadan ve kanalı kapatmadan birçok işlem daha yapabilir durumdadır.

Tablo 3.2. Piyasa Yapıcı, Normal Kullanıcı ve Kanal Sağlayıcı arasındaki takas ilişkisi formülü

Denklem No	Denklem
1	$\{K_1(1): C\} \Rightarrow (C,) \Rightarrow \{K_1(1): C\&(A\|T_4)\}$
2	$\{K_2(2): A\} \Rightarrow (A,) \Rightarrow \{K_2(2): A\&(C\|T_3)\}$
3	$\{K_1(3): C\} \Rightarrow (C,) \Rightarrow \{K_1(3): (B\&S_1)\|(C\&T_2)\}$
4	$\{K_2(4): B\} \Rightarrow (B,) \Rightarrow \{K_2(4): (C\&S_1)\|(B\&T_1)\}$
5	$\{K_1(1): C\&(A\|T_4)\} \Rightarrow (C,) \Rightarrow \{K_1(3): (A\&S_2)\|(C\&T_4)\} + \{K_1(5): C\}$
6	$\{K_2(2): A\&(C\|T_3)\} \Rightarrow (A,) \Rightarrow \{K_2(4): (C\&S_2)\|(A\&T_3)\} + \{K_2(6): A\}$
7	$\{K_2(4): (C\&S_1)\|(B\&T_1)\} \Rightarrow (C, S_1) \Rightarrow \{K_2(4): C\}$
8.	$\{K_1(3): (B\&S_1)\|(C\&T_2)\} \Rightarrow (B, S_1) \Rightarrow \{K_1(3): B\}$
…	…
n-1	$\{K_1(3): (A\&S_2)\|(C\&T_4)\} \Rightarrow (A, S_2) \Rightarrow \{K_1(3): A\}$
n	$\{K_2(4): (C\&S_2)(A\&T_3)\} \Rightarrow (C, S_2) \Rightarrow \{K_2(4): C\}$

Bu bölümde iki kişi arasındaki gerçekleşecek atomik takasın ana hatları senaryo bağlamında açıklanmıştır. Akış şeması içeren grafikleri birbiri ardına takip ederek atomik takas işleminin ve hata olması durumunda işlemlerin nasıl iptal edileceği görülebilmektedir. İşlemlerin sırasıyla takip edilmesi durumunda yazılım için gerekli olan teknik analizi bu modelden çıkarmak mümkündür.

BÖLÜM 4. SONUÇ

Merkezi platformlar ya da güvenilir üçüncü kişilere dayalı sistemler insan faktöründen kaynaklanan hataları içerebilmektedir. Bu çalışma kapsamında tasarlanan atomik takas modeli ile merkezi olmayan yapının sağladığı avantajlar ile insan hatasından kaynaklanan güvenlik risklerinin önlenmesi öngörülmektedir. Bunun yanı sıra, güvenilir üçüncü kişilere duyulan gereksinim ortadan kalktığında merkezi sistemlerde meydana gelen hacklenme ve dijital saldırılar gibi güvenlik risklerinin de ortadan kalkacağı öngörülmektedir.

Tasarlanan atomik takas modelinin kullanılmasıyla birlikte, kişilerin cüzdanlarında ya da bilgisayarlarında herhangi bir güvenlik sorunu olması durumunda sadece her iki uçta takas yapan kişi ve güvenlik sorunu olan kişinin cüzdanı etkilenmektedir. Atomik işlem yapısı sayesinde, işlem sırasında eşlerden herhangi biri transferi doğrulamazsa, transfer tamamen iptal edilecek ve tarafların paraları kendi cüzdanlarına iade edilecektir. Böylece herhangi bir sistem arızasında ekonomik kayıp yaşanmayacaktır.

Merkezi platformlar, işlemleri takas etmek ve aracı olarak hareket etmek için operasyonel süreçler gerektirmektedir. Bu ihtiyaç, kullanıcıları bir platforma bağımlı hale getirmekte ve yürütülmesi için belirli bir işlem zamanını gerekli kılmaktadır. Bu çalışmada tasarlanan atomik takas modeli ile gerçekleşen takas süreci, sistem yüküne bakılmaksızın sadece eşler arasında meydana gelmektedir. Merkezi platforma yapılan yatırım ve aracılık yapabilmek için gerekli iş yükü azalacağından işlemlerden kesilen yüksek komisyon ücretlerinin ortadan kalkması öngörülmektedir. Atomik takas modeli ile blok zincir teknolojilerinin kullanım ve yaygınlığının artması düşünülmektedir. Bu yaygınlığı arttırmak ve takas işlemlerinin ödeme süreçlerine hız kazandırmak için, ödeme kanalları teknolojisi ve kanal sağlayıcı yatırımcılar aracılığıyla likidite sorununun çözülmesi de gerçekleşmiş olacaktır.

Atomik takas modelinin, merkezi borsalarda ortaya çıkan pek çok soruna çözüm sunmasının yanı sıra, zayıf noktaları de bulunmaktadır. Bunlar, daha uzun işlem süresi gereksinimi ve ilk kullanım esnasında daha yüksek alım satım marjları olarak sıralanabilmektedir. İlk zayıf nokta, dağıtık takas borsasında uzlaşma için gereken süre tek bir makinedeki işlem süresinden daha uzun olmasıdır. TCP modelindeki karşılıklı uzlaşma

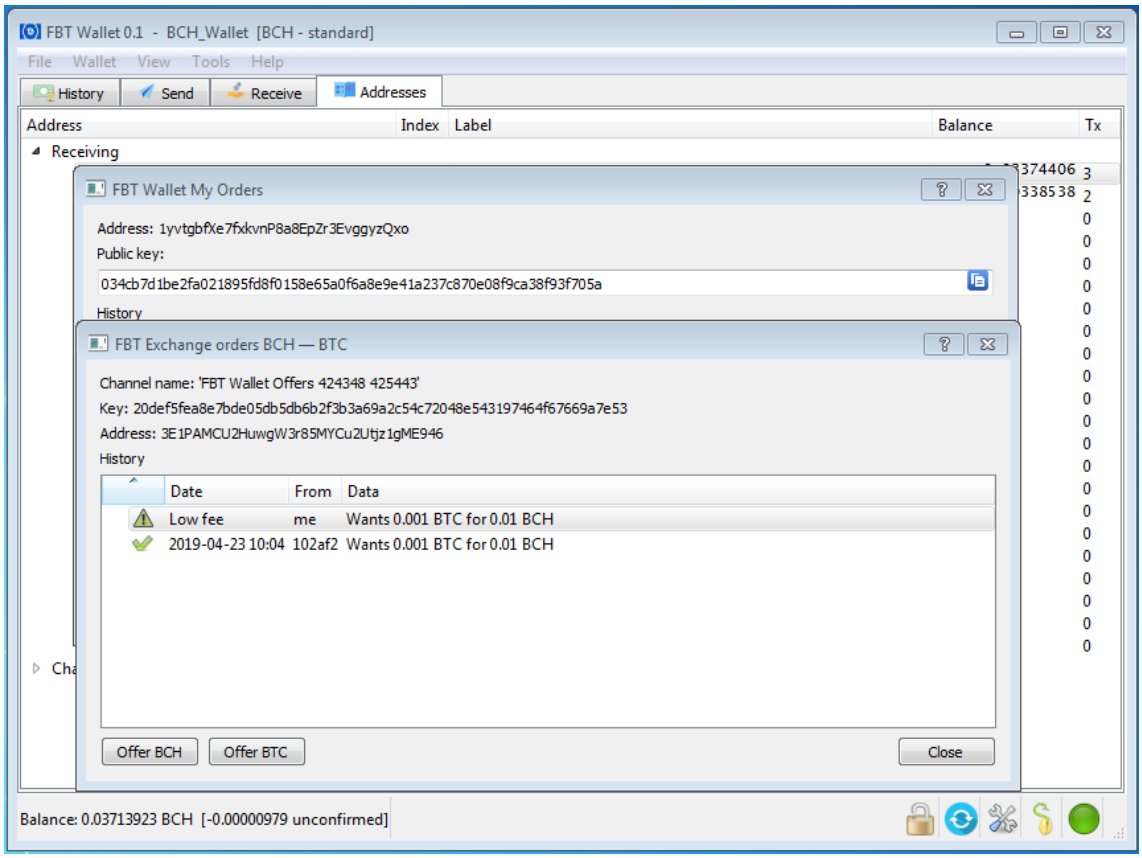
modeli gibi, dağıtık sistemlerdeki uçların birbirleri arasında haberleşme ve anlaşması için bazı mesajların gidip gelmesi gerekmektedir. Ağdaki bu gidip gelme süreleri aynı işlemcide yapılan takas algoritmasına kıyasla göreceli olarak çok daha uzun sürmektedir.

Diğer bir zayıf nokta ise, sistemin dağıtılmış bir modele sahip olmasından dolayı, bazı sunucuların bu zinciri saklayıp değişiklikleri yayınlaması gereksinimidir. Dağıtık zincir sistemi maliyet ve eşleşme tutarları konusunda avantajlara sahip en az bir sunucu sisteminin bu zinciri yayınlaması ve üzerindeki eşleşmeleri doğrulaması gerekmektedir. Çalışmaların hali hazırda özel zincir algoritmalarını saklayan ve yayınlayan sunucuların üzerinde başlatılması ile çözülebilmesi öngörülmektedir. Bir diğer konu olan alım-satım fiyatları arasında oluşabilecek yüksek farklar konusunda, sistemde ilk aşamada çok fazla alıcı ve satıcı olmayacağından bir piyasa yapıcının ilk aşamada alım satım fiyatları arasındaki farkı düzenlemesi gerekmektedir. İlerleyen dönemde piyasada atomik takas sisteminin daha fazla kişiyi çekebilmesi ve artan taleple birlikte daha düşük alım-satım farkları oluşması sağlanacaktır. Merkezi olmayan borsa belirli bir kullanıcı sayısına ulaştıktan sonra en ucuz alış ve en yüksek satış fiyatlarını verecek uzlaşma fiyatlarına ulaşacaktır. Örneğin, torrent dosyalarının çalışma mantığı, bazı kişilerin bu dosyaları paylaşması ile başlamaktadır. Aynı dosyayı daha fazla kişi indirip paylaşmaya başladıkça, indirme hızı artmakta ve hız arttıkça daha çok kişi kullanmaya başlamaktadır. Birbirini destekleyen bu katkı sayesinde gün geçtikçe bu platformu kullanan insan sayısı artacaktır. Merkezi olmayan takas borsaları da daha çok kişinin kullanmaya başlaması ile verimliliğini arttırarak gittikçe daha verimli platformlar haline gelecektir.

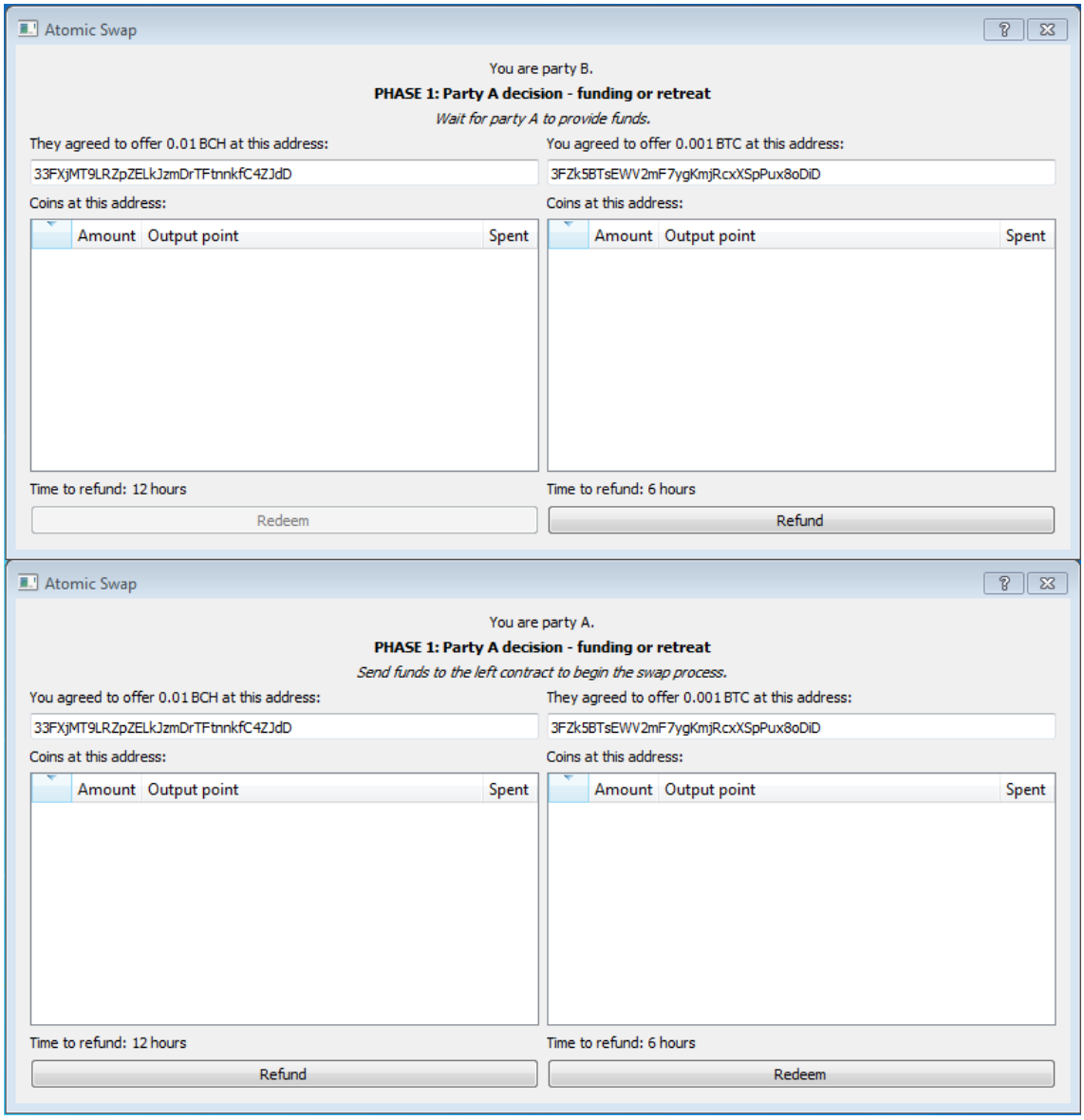
Bu çalışma kapsamında tasarlanan atomik takas modelinin yenilikçi kısmı, alım satım işlemi yapmak isteyen kişilerin, merkezi borsa ve güvenilir üçüncü taraflara gereksinim duymadan, blok zincir üzerinde akıllı kontrat tabanlı bir altyapı kullanarak fiyat ve değişim miktarları üzerinde anlaşarak takas yapabilmesine olanak sağlamasıdır. Akıllı kontrat tabanlı takas yönetim sistemi ile, işlem sırasında herhangi bir hata meydana gelmesi ya da herhangi bir kişinin takas işleminden vazgeçmesi durumunda, her bir tarafın parasını geri alacağı ve başlangıç durumuna kayıpsız dönüleceğini taahhüt edilmektedir.

EKLER

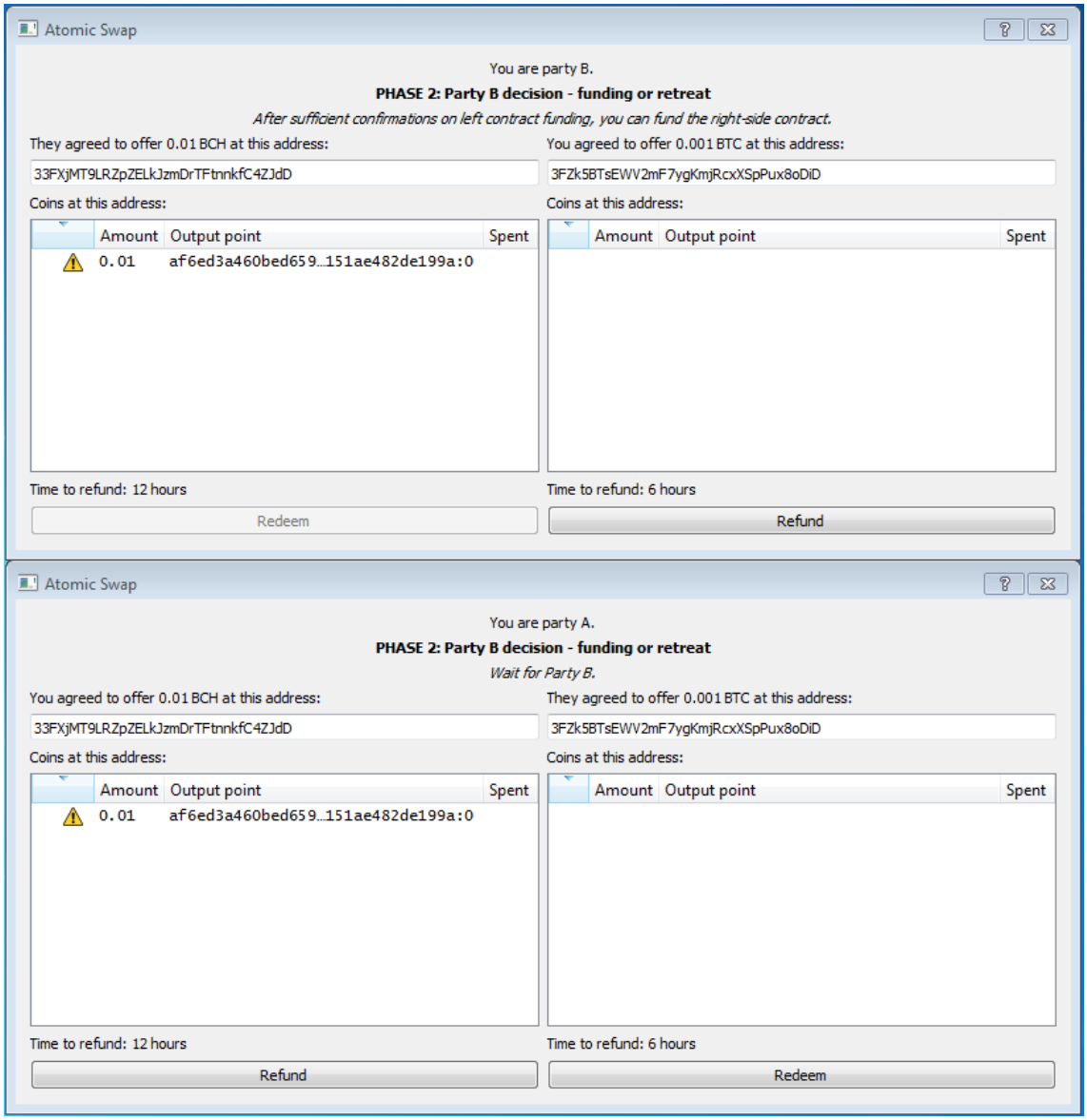
Ek 1. Uygulama Ekran Görüntüleri



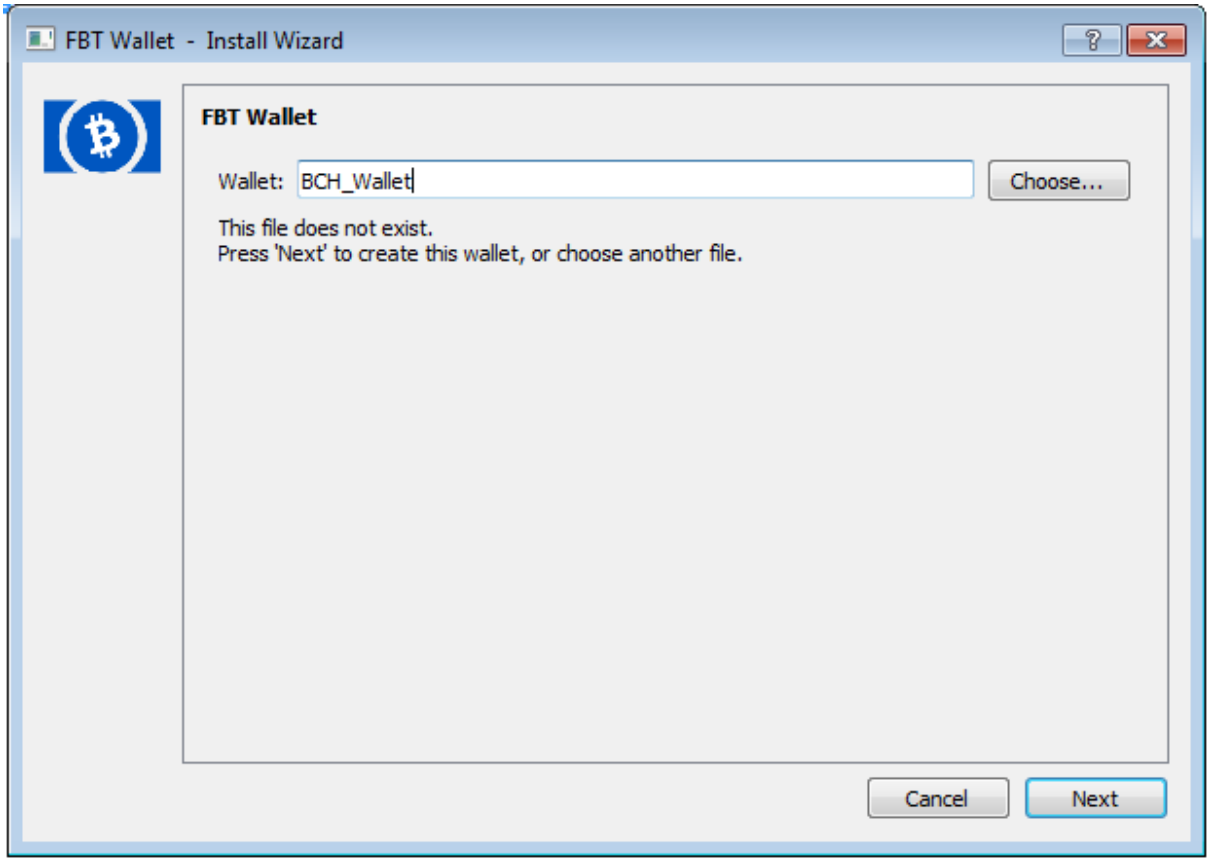
Emir Yayın Ekranı



Takas Ekranı



Karşı Tarafın Takas Ekranı



Emir Giriş Ekranı

KAYNAKÇA

Adedoyin, A. & Kapetanakis, S. & Samakovitis, G. & Petridis, M., *Predicting Fraud in Mobile Money Transfer Using Case-Based Reasoning*. 325-337, 2017.

Al Khalil, Firas & Butler, Tom & O'Brien, Leona & Ceci, M., *Trust in Smart Contracts is a Process, As Well.* 1st Workshop on Trusted Smart Contracts. In Association with Financial Cryptography, 2017.

Al-Amri, R., Zakaria, N. H., Habbal, A. & Hassan, S. Cryptocurrency adoption: current stage, opportunities, and open challenges. *International Journal of Advanced Computer Research* 9(44), 293–307, 2019.

Allessie, D., Sobolewski, M., Vaccari, L., Pignatelli, F. *Blockchain for digital government,* EUR 29677 EN, Publications Office of the European Union, Luxembourg, 2019.

Allison, I., If banks want benefits of blockchains they must go permissionless: https://www.ibtimes.co.uk/nick-szabo-if-banks-want-benefits-blockchains-they-must-go-permissionless-1518874, 2015.

Alpago, H. Bitcoin'den Selfcoin'e Kripto Para. *Journal of International Scientific Researches*, 3, 411-428, 2018.

Greenberg, A., Crypto Currency: https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html?sh=1a4bd705353e, 2011.

Torpey, K., Are Any Altcoins Currently Useful? No, Says Monero developer Riccardo Spagni: https://bitcoinmagazine.com/culture/are-any-altcoins-currenty-useful-no-says-monero-developer-riccardo-spagni-1458743546, 2016.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Čapkun, S. (2016). On the security and performance of Proof of Work blockchains. Association for Computing Machinery *CCS 2016 - Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 24-28-October-2016, pp. 3-16, 2016.

Atkins, Allen B.& Edward A. Dyl., Price Reversals, Bid-Ask Spreads, and Market Efficiency, *The Journal of Financial and Quantitative Analysis*, 25, 4, 535–547, 1990.

Aydar, M., Cetin, S. & Ayvaz, S. & Aygun, B. Private key encryption and recovery in blockchain: https://arxiv.org/abs/1907.04156, 2019.

Bailis, P., Fekete, A., Franklin, M., Ghodsi, A., Hellerstein, J. & Stoica, I., Coordination avoidance in database systems. *Proceedings of the VLDB Endowment.* 8. 185-196, 2014.

Bartos, J., Does Bitcoin follow the hypothesis of efficient market?. International *Journal of Economic Sciences*, 4(2), 10-23, 2015.

Beckett, P., *Ownership, Financial Accountability and the Law.* London: Routledge, 2019.

Bentov, I., Lee, C., Mizrahi, A. & Rosenfeld, M., Proof of Activity. ACM SIGMETRICS *Performance Evaluation Review*. 42. 34-37, 2014.

Berentsen, A. & Schär, F., A Short Introduction to the World of Cryptocurrencies. *Federal Reserve Bank of St. Louis Review,* 100(1): 1-16, 2018.

Bitguru web sitesi, www.bitguru.co.uk, 2017.

Blockchains: Her şeyden emin olmanın büyük zinciri: https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things, 2015.

Tian, B., Huang, J., Mozafari, B. & Schoenebeck, G., Contention-aware lock scheduling for transactional databases. *Proc. VLDB Endow*, 11, 5, 648–662, 2018.

Bremer, M. & Sweeney, R.J., The Reversal of Large Stock-Price Decreases. *The Journal of Finance*, 46: 747-754, 1991.

Briere, M., Oosterlinck, K. & Szafarz, A., Virtual Currency, Tangible Return: Portfolio Diversification with Bitcoin, *Journal of Asset Management*, 16, 6, 365-373, 2015.

Brown, K. C., W.V. Harlow and S. M. Tinic, Risk Aversion, Uncertain Information, and Market Efficiency. Journal of Financial Economics, 22, 355 – 385, 1988.

Bruneau, G. & Moran, K., Exchange rate fluctuations and labour market adjustments in Canadian manufacturing industries, *Canadian Journal of Economics*, Canadian Economics Association, 2017, vol. 50(1), 72-93.

Caporale, G.M. & Plastun, A., The day of the week effect in the crypto currency market, *Working Paper No. 17-19*, October 2017, Brunel University, London, 2017.

Caradonna, T. Blockchain and society. Informatik Spektrum 43, 40–52. https://doi.org/10.1007/s00287-020-01246-7), 2020.

Carrick, J. Bitcoin as a Complement to Emerging Market Currencies, Emerging Markets Finance and Trade 52, 2321-2334, 2016.

Chan, S., Chu, J., Nadarajah, S. & Osterrieder, J., A Statistical Analysis of Cryptocurrencies, *Journal of Risk and Financial Management*, 10, 12, 2017.

Cheung, A., E. Roca &J.-J. Su, Crypto-Currency Bubbles: An Application of the Phillips-Shi-Yu (2013) Methodology on Mt. Gox Bitcoin Prices, Applied Economics, 47, 2348-2358, 2015.

Choi, H.S. & Jayaraman, N., Is reversal of large stock-price declines caused by overreaction or information asymmetry: Evidence from stock and option markets, *Journal of Futures Markets*, 29, 4, 348-376, 2009.

Chowdhury, N., *Inside Blockchain, Bitcoin, and Cryptocurrencies.* New York: Auerbach Publications, 2020.

Chu, J. & Nadarajah, S. & Chan, S., Statistical Analysis of the Exchange Rate of Bitcoin. *PloS one*, 10, 2015.

Corlu, C.G. & Corlu, A. Modelling exchange rate returns: Which flexible distribution to use? *Quantitative Finance*, 15: 1851–64, 2015.

Çarkacıoğlu, A., Kripto Para-Bitcoin: https://www.spk.gov.tr/SiteApps/Yayin/YayinGoster/1130, 2016.

Riehle, D., Riemer, P. Kolassa, C. & Schmidt, M., Paid vs. Volunteer Work in Open Source," *2014 47th Hawaii International Conference on System Sciences, Waikoloa, HI,* 3286-3295, 2014.

Dai, P., Delpachitra, S. & Cottrell, S., Real exchange rate and economic growth in east asian countries: The role of financial integration. *The Singapore Economic Review*, 62, 2016.

The Economist: https://www.economist.com/briefing/2016/05/02/craig-steven-wright-claims-to-be-satoshi-nakamoto-is-he, 2016.

Dai, B., Forsythe, S. & Kwon, W.S., The impact of online shopping experience on risk perceptions and online purchase intentions: Does product category matter?, *Journal of Electronic Commerce Research*, 15. 13-24, 2013.

De Bondt, W.F.M. & Thaler, R., Does the Stock Market Overreact? *Journal of Finance*, 40, 793-808, 1985.

Delgado-Segura, S., Pérez-Solà, C., Herrera-Joancomartí, J., Navarro-Arribas, G., & Borrell, J., Cryptocurrency Networks: A New P2P Paradigm. Mobile Information Systems. Hindawi Limited, 2018.

Deloitte, Blok- zincir potansiyelinin keşfi: https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/consulting/blokzincir-potansiyelinin-kesfi.pdf, 2018 .

Destais, C., Central Bank Currency Swaps and the International Monetary System: http://www.obela.org/system/files/CentralBankCurrencySwap_ChristopheDestais.pdf, 2014.

Dorri, A., Kanhere, S.S., Jurdak, R., & Gauravaram, P., LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy, ArXiv, 2019.

Dwyer, G. P., The Economics of Bitcoin and Similar Private Digital Currencies, *Journal of Financial Stability*, 17, 81-91, 2014.

Bartocci, E. & Falcone. Y., Introductory and Advanced Topics, *Lectures on Runtime Verification*, Springer, 10457, 1-240, 2018.

Fang, W., Chen, W., Zhang, W. vd. Digital signature scheme for information non-repudiation in blockchain: A state of the art review. *J Wireless Com Network*, 56, 2020.

Ferri, M., G. & C. Min., Evidence that the Stock Market Overreacts and Adjusts. *The Journal of Portfolio Management*, 22, 71-76, 1996.

Fortier, P. & Michel, H., Computer Systems Performance Evaluation and Prediction. Computer Systems Performance, *Evaluation and Prediction*, 1-525, 2003.

Gandal, N. & Hałaburda, H., Competition in the cryptocurrency market, *Bank of Canada Working Paper, No. 2014-33*, Bank of Canada, Ottawa, 2014.

Hileman, G. & Rauchs, M., 2017 Global Cryptocurrency Benchmarking Study, *SSRN Electronic Journal*, 2017.

Giechaskiel, I., Cremers, C. & Rasmussen, K., On Bitcoin Security in the Presence of Broken Cryptographic Primitives. European Symposium on Research in Computer Security, 9879. 201-222, 2016.

Goodman, L. M., The Face Behind Bitcoin: https://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html, 2014.

Gray, H. & Zhang, N.F., On Generalized Fractional Processes. *Journal of Time Series Analysis*, 10. 233 – 257, 1989.

Greene, R., Liquidity Or Leakage Plumbing Problems With Cryptocurrencies, Distributed futures:
https://www.zyen.com/media/documents/Liquidity_Or_Leakage_KQg79GR.pdf, 2018.

Haber, S. & Stornetta, W.S., How to time-stamp a digital document, *J. Cryptology*, 3, 99–111, 1991.

Hencic, A. & Gourieroux, C., Noncausal Autoregressive Model in Application to Bitcoin/USD Exchange Rates, *Studies in Computational Intelligence*, 583, 17-40, 2015.

Islam, S., Abedin, Z. & Das, S., Mobile Wireless Peer-To-Peer Network with Higher End-To-End Throughput And Lower End-To-End Delay, *American Journal of Engineering Research*, 3. 8-21, 2014.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A. & Felten, E.W., SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," *2015 IEEE Symposium on Security and Privacy*, San Jose, CA, 104-121, 2015.

Joshi, J., Nepal, S., Zhang, Q., Zhang, L.J., Blockchain – *ICBC 2019: Second International Conference, Held as Part of the of the Services Conference Federation*, SCF San Diego, CA, USA, 2019.

Cermeño, J.S., Blockchain in financial services: Regulatory landscape and future challenges for its commercial application: https://www.bbvaresearch.com/en/publicaciones/blockchain-in-financial-services-regulatory-landscape-and-future-challenges-for-its/, 2018.

Brito, J. & Castillo, A., Bitcoin: A Primer for Policymakers. George Mason University: https://www.mercatus.org/publications/technology-and-innovation/bitcoin-primer-policymakers, 2016.

Koops, E.J., The Crypto Controversy : *A Key Conflict in the Information Society*, The Hague, London, Boston : Kluwer Law International, 1999.

Kristoufek, L., What Are the Main Drivers of the Bitcoin Price? Evidence from Wavelet Coherence Analysis. *PLoS ONE*, 10(4), 2015.

Lano, K., Clark, T. & Kolahdouz-Rahimi, S., A framework for model transformation verification. *Form Asp Comp*, 27, 193–235, 2015.

Lano, K., Null considered harmful (for transformation verification). *VOLT 2014, STAF Conference*, York, 2014.

Lansky, J., Bitcoin System. Acta Informatica Pragensia, 6. 20-31, 2017.

Leis, V., Kemper, A. & Neumann, T., Exploiting hardware transactional memory in main-memory databases. *Proceedings - International Conference on Data Engineering*, 580-591, 2014.

Lemieux, V., A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation, *2017 IEEE International Conference on Big Data*, 2271-2278, 2017.

Li, A., Wei, X. & HE, Z., Robust Proof of Stake: A New Consensus Protocol for Sustainable Blockchain Systems, *Sustainability*, 12, 2824, 2020.

Locher, T., Obermeier, S. & Pignolet, Y.A., When Can a Distributed Ledger Replace a Trusted Third Party?: https://arxiv.org/abs/1806.10929, 2018.

Abraham, L.& Guegan, D., The Other Side of the Coin: Risks of the Libra Blockchain, *University Ca' Foscari of Venice, Dept. of Economics Research Paper Series*, 30/WP/2019, 2019.

Quiniou, M., *Blockchain: The Advent of Disintermediation*, Wiley, 2019.

Meijer, D.B., Blockchain Technology: Trust and/or Control?: https://www.semanticscholar.org/paper/Blockchain-Technology-%3A-Trust-and-%2F-or-Control-Meijer/43865e89dec44e9305086013c9c0999bfb8c6281, 2017.

Monrat, A.A., Schelén, O. & Andersson, K. Survey of Blockchain from the Perspectives of Applications, Challenges and Opportunities, *IEEE Access*, PP. 117134-117151, 2019.

Moosbrugger, P., Rozier, K.Y. & Schumann, J., R2U2: monitoring and diagnosis of security threats for unmanned aerial systems. *Form Methods Syst Des*, 51, 31–61, 2017.

Moreno-Sanchez, P., Zafar, M. & Kate, A., Listening to Whispers of Ripple: Linking Wallets and Deanonymizing Transactions in the Ripple Network. *Proceedings on Privacy Enhancing Technologies*, 2016.

Musonera, E. & Vincent, S. (2008). Establishing a Stock Exchange in Emerging Economies: Challenge and Opportunities, *Development Economics eJournal*, 2008.

Mynhardt, R.H. & Plastun, A., The overreaction hypothesis: The case of Ukrainian stock market, *Corporate Ownership and Control*, Volume 11(1), 406-422, 2013.

Tahir, M. & Nadarajah, S., Parameter induction in continuous univariate distributions: Well-established G families, *Anais da Academia Brasileira de Ciências*, 87, 2015.

Nakamoto, S., Bitcoin: A Peer-to-Peer Electronic Cash System: https://bitcoin.org/bitcoin.pdf, 2009.

Nassiry, D., The Role of Fintech in Unlocking Green Finance: Policy Insights for Developing Countries, *ADBI Working Paper 883*, Tokyo: Asian Development Bank Institute, 2018.

Natenberg, S., *Option Volatility Trading Strategies*, Wiley, 2007.

Halaburda, H. & Gandal, N., Can we predict the winner in a market with network effects? Competition in cryptocurrency market, *Games*, NET Institute Working Paper No. 14-17, 7 (3), 16, 2016.

Nian, L. & Chuen, D., Introduction to Bitcoin, Handbook of Digital Currency, 2015.

Nofer, M. & Gomber, P. & Hinz, O. & Schiereck, D., Blockchain. *Business & Information Systems Engineering*, 59, 2017.

Kaplan, M., I accidentally threw away $60M worth of Bitcoin: https://nypost.com/2018/05/26/i-accidentally-threw-away-60m-worth-of-bitcoin/, 2018.

Park, S., Im, S., Seol, Y. & Paek, J., Nodes in the Bitcoin Network: Comparative Measurement Study and Survey, *IEEE Access*, 7, 57009–57022, 2019.

Parlapiano, F., Alexeev, V. & Dungey, M., Exchange rate risk exposure and the value of European firms, *The European Journal of Finance*, 23. 1-19, 2015.

Pimentel, E. & Boulianne, E. & Eskandari, S. & Clark, J., Systemizing the Challenges of Auditing Blockchain-Based Assets. SSRN Electronic Journal, 10.2139/ssrn.3359985, 2020.

Pirinççi, A. E., Evaluation of Virtual Money Bitcoin in the New World Edition, Uluslararası Ekonomi Siyaset İnsan ve Toplum Bilimleri Dergisi, 1 (1), 45-52, 2018.

Popper, N., Borsa Zili Çalıyor, Bilgisayar Başarısız, Wall Street Cringes: https://www.nytimes.com/2015/07/09/business/dealbook/new-york-stock-exchange-suspends-trading.html, 2015.

Das, P., Faust, S. & Loss, J., A Formal Treatment of Deterministic Wallets, *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). Association for Computing Machinery,* New York, NY, USA, 651–668, 2019.

Raval, S., *What Is a Decentralized Application?, Decentralized Applications: Harnessing Bitcoin's Blockchain Technology, O'Reilly*, 2016.

Houben, R. & Snyers, A., *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion*, 2018.

Rubasinghe, I., Transaction Verification Model over Double Spending for Peer-to-Peer Digital Currency Transactions based on Blockchain Architecture. *International Journal of Computer Applications*, 163. 24-31, 2017.

Zhang, R., Xue, R. & Liu, L., Security and Privacy on Blockchain. *ACM Comput. Surv.*, 1, 1, 35, 2019.

Eskandari, S., Barrera, D., Stobert, E. & Clark, J., A First Look at the Usability of Bitcoin Key Management, Internet Society, 2018.

Sapuric, S. & Kokkinaki, A., Bitcoin Is Volatile! Isn't that Right?, *Lecture Notes in Business Information Processing*, 183. 255-265, 2014.

Schär, F., Roth, J. & Schöpfer, A., The Tokenization of Assets: Using Blockchains for Equity Crowdfunding. SSRN Electronic Journal, 2019.

Schröder, M., The equilibrium real exchange rate and macroeconomic performance in developing countries, *Applied Economics Letters*, 24. 1-4, 2016.

Seyyedi, S., Analysis of the Interactive Linkages Between Gold Prices, Oil Prices, and Exchange Rate in India, *Global Economic Review*, 46. 1-15, 2017.

Sitonio, C. & Nucciarelli, A.,The Impact of Blockchain on the Music Industry, *29th European Regional ITS Conference, Trento, International Telecommunications Society (ITS)*, 2018.

Sonstebo, D., IOTA First Chapter Synopsis: https://medium.com/iotatangle/iota-first-chapter-synopsis-506fdf874437, 2016.

Sultan, K., Ruhi, U. & Lakhani, R., Conceptualizing Blockchains: Characteristics & Applications, *Computers and Society*, 2018.

Volety, T., Saini, S., McGhin, T., Liu, C.Z. & Choo, K.K.R., Cracking bitcoin wallets: I want what you have in the wallets, *Future Generation Computer Systems*, 91,136–143, 2019.

Tasca P., Digital Currencies: Principles, Trends, Opportunities, and Risks, ECUREX Research and University of Zurich, Department of Banking & Finance: https://faculty.fuqua.duke.edu/~charvey/Teaching/898_2016/Readings/Tasca.pdf, 2015.

The Economist, Satoshi Nakamoto, bitcoin's enigmatic creator: https://www.economist.com/technology-quarterly/2018/08/30/satoshi-nakamoto-bitcoins-enigmatic-creator, 2016.

Browne, R., UK Launches initiative to explore potential of virtual currencies, The UK News, https://www.cnbc.com/2021/04/19/uk-to-explore-issuing-its-own-digital-currency-amid-bitcoin-boom.html, 2021.

Umar, A., *Information Security and Auditing in the Digital Age: A Practical and Managerial Perspecive*, 2003.

Vejačka, M., Basic Aspects of Cryptocurrencies. Journal of Economy, *Business and Financing*, 2. 75 – 83, 2014.

Steadman, I., Wary of Bitcoin? A guide to some other cryptocurrencies: https://arstechnica.com/information-technology/2013/05/wary-of-bitcoin-a-guide-to-some-other-cryptocurrencies/, 2013.

wikipedia.com: https://en.wikipedia.org/wiki/Mt._Gox

Bitcoin: www.coinmarketcap.com/tr/currencies/bitcoin/, 2018.

Wilmoth, J., What is an Altcoin? Crypto Coins News: https://www.cryptocoinsnews.com/altcoin/, 2014.

Zhao, Y., Cryptocurrency Brings New Battles into the Currency Market, *Seminar Future Internet*, 2014.

Zhu, H. & Zhou, Z., Analysis and outlook of applications of blockchain technology to equity crowdfunding in China, *Financial Innovation*, 2, 2016.

Radivojak, G. & Grujić, M., Future Of Cryptocurrencıes And Blockchain Technology in Fınancial Markets, 1. 56-75, 2019.