BLOK ZİNCİR TEKNOLOJİSİNİN ÖĞRENİMİ İÇİN BİR SİMÜLATÖR TASARIMI

Gizem Sarıkaya Yaylamış
191402201

YÜKSEK LİSANS TEZİ
Lisansüstü Eğitim Enstitüsü
Bilgisayar Mühendisliği Yüksek Lisans Programı
Danışman: Prof.Dr. Emin Murat Esin

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Ocak, 2022
İstanbul

BLOK ZİNCİR TEKNOLOJİSİNİN ÖĞRENİMİ İÇİN BİR SİMÜLATÖR TASARIMI

Gizem Sarıkaya Yaylamış
191402201
Orcid: 0000-0003-4066-3004

YÜKSEK LİSANS TEZİ
Lisansüstü Eğitim Enstitüsü
Bilgisayar Mühendisliği Yüksek Lisans Programı
Danışman: Prof.Dr. Emin Murat Esin

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Ocak, 2022



JÜRİ VE ENSTİTÜ ONAYI

Bu belge, Yükseköğretim Kurulutarafından 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 Kurulutarafından 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

Bütün çalışmam boyunca desteklerini benden esirgemeyen, yardım ve yönlendirmeleriyle gelişimime önemli katkılar sağlayan değerli hocam Sn. Prof. Dr. Emin Murat Esin'e, bu süreçte her anlamda desteğini üzerimden çekmeyen eşim Erdem Yaylamış'a, eğitim hayatım boyunca her zaman sorgusuz sualsiz arkamda olan annem Zeynep Sarıkaya, babam Musa Sarıkaya ve kardeşim Can Sarıkaya'ya en içten teşekkürlerimi sunuyorum.

Gizem Sarıkaya Yaylamış

Ocak, 2022

ÖZ

BLOK ZİNCİR TEKNOLOJİSİNİN ÖĞRENİMİ İÇİN BİR SİMÜLATÖR TASARIMI

Gizem Sarıkaya Yaylamış
Yüksek Tezi
Bilgisayar Mühendisliği
Danışman: Prof. Dr. Emin Murat Esin
Maltepe Üniversitesi Lisansüstü Eğitim Enstitüsü, 2022

Teknoloji gün geçtikçe ilerlemekte ve birçok alanda etkisini göstermektedir. Bu alanlardan biri de finanstır. Finansal teknolojiler zaman ilerledikçe etki alanını yükseltmekte ve birçok insana da doğrudan ya da dolaylı olarak dokunmaktadır. Günümüzde finansal teknolojiler arasında popüler olanlardan biri de blok zincir teknolojisidir. Blok zincir ile finansal alanda birçok kullanıcıya çözüm odaklı bir hizmet sunma hedefi bulunmaktadır. Fakat bu teknoloji yeni olduğu için tüm dünyada gelişim göstermeye ve etki alanını büyütmeye devam etmektedir. Bu tezde finansal teknolojilerin ne olduğu, kullanım alanları, bu teknoloji içerisinde blok zincirin yeri, blok zincir teknolojileri, kullanım alanları ve bu teknoloji ile geliştirilen ürünlerin incelenmesi, bu incelemenin ardından blok zincir teknolojisinin temel fonksiyonları, yapılan transactionlar, transactionların durum değişiklikleri, ağ yapısı ve bu yapı içerisinde bulunan veri ve kayıt dolaşımı incelenecek ve bu kavramları somutlaştırabilmek adına bir simülatör yapılmıştır. Simülatör ile bahsedilen tüm bu yapı taşları somutlaştırılmış olacak ve anlaşılır, bahsedilen kavramları somutlaştıran bir yapı kurgulanmış olacaktır. Somutlaştırmayı pekiştirebilmek adına örnek uygulamalar da simülatör üzerinde gösterilmiş ve detayları ile belirtilmiştir.

Anahtar Sözcükler: Blok zincir, Finansal Teknolojiler, İşlem, Sanal Paralar; Simülatör

ABSTRACT

DESIGNING A SIMULATOR FOR LEARNING BLOCKHAIN TECHNOLOGY

Gizem Sarıkaya Yaylamış
Master Thesis
Computer Engineering
Advisor: Prof.Dr.Emin Murat Esin
Maltepe Üniversitesi Lisansüstü Eğitim Enstitüsü, 2022

Technology is developing day by day and shows its effect in many areas. One of these areas is finance. Financial Technologies are increaing in their area and it influences all of the areas and touch many people directly or indirectly. Today, Blockchain is one of the popular technology among financial technologies. There is a goal of providing a solution oriented servise to many users in the financial area with blockchain. However, this technology is new so it continues to develop and expand its area and affects all over the World. In this thesis, it was planed to examine what financial Technologies are and their usage areas, the effect of blockchain in this technology, blockchain Technologies, it's usage areas and products that developed with this technology. Also the basic functions of the blockchain technology, the transactions' property, the state of changes of the transactions, the network structure and these transactions record in this structure will be examined in the simulator. All these buildings will be shown by the simulator and this way it will be easy to undestand this structure and also lots of examples about blockchain's structure was shown on the simulator and detailed.

Keywords: Blockchain**,** Financial Technologies, Transaction, Crypto currency, Simulator

İÇİNDEKİLER

JÜRİ VE ENSTİTÜ ONAYI ii
ETİK İLKE VE KURALLARA UYUM BEYANI iii
TEŞEKKÜR iv
ÖZ v
ABSTRACT vi
İÇİNDEKİLER vii
TABLOLAR LİSTESİ ix
ŞEKİLLER LİSTESİ x
KISALTMALAR xi
ÖZGEÇMİŞ xii
BÖLÜM 1. GİRİŞ 1

Problem 2
Amaç 2
Önem 3
Varsayımlar 3
Sınırlıklar 4
Tanımlar 4
BÖLÜM 2. Fİnansal Teknolojiler ve Blok zincir 5

2.1 Finansal Teknolojiler 5

2.1.1 Finansal teknolojilerin kullanım alanları 7

2.1.1.1 Fon Transferleri 7
2.1.1.2 Ödeme Sistemleri Uygulamaları ve Sanal Paralar 8
2.1.1.3 Kredi Skorlama İşlemleri 9
2.1.1.4 Sigorta İşlemleri 9

2.2. Blok Zincir Teknolojisi 10

2.2.1 Blok Zincir Tanımı ve Temel Yapısı 11

2.2.1.1. Node (Düğüm) 11
2.2.1.2 Blok 12
2.2.1.3. Hashing 15
2.2.1.4 Ağ Yapısı 16
2.2.1.5 Merkle Ağaçları 18
2.2.1.6 Mutabakat 21

2.2.1.6.1 Proof of Work (PoW) 21

2.2.1.6.2 Proof of Stake (PoS) 21
2.3. Blok Zincir Kullanım Alanları 22
2.4. Blok Zincir ile Finansal Teknoloji Arasındaki İlişki 22
2.5. Finansal Teknolojilerde Blok Zincir Teknolojisinin Kullanım Alanları 23
2.5.1. Uluslararası Fon Transferi 24
2.5.2. Kimlik Tanıma Sistemi 24
2.5.3. Kredi Skorlama İşlemi 25
2.5.4. Akıllı Kontratlar 25
BÖLÜM 3. BLOK ZİNCİR SİMÜLATORÜ VE UYGULAMA ALANLARI 27
3.1 Simülatör İş Akışı 27
3.2. Simülatöre Giriş 29
3.3. Simülatör İşlemler Sayfası 30
3.3.1. Zorluk Seviyesi 32
3.4 Simülatörde İlk Bloğun (Genesis Blok) Oluşması 33
3.5. Simülatörde Blokların Oluşması ve Zincire Eklenmesi 34
3.6. Simülatörde Bloğun Hash Koduna Müdahale Edilmesi 40
3.7. Simülatör Uygulama Örnekleri 42
Örnek 1: 42
Örnek 2: 44
Örnek 3: 46
Örnek 4: 48
BÖLÜM 4. SONUÇ 50
Özet 50
Yargı 50
Öneriler 51
KAYNAKÇA 52

TABLOLAR LİSTESİ

Tablo 1. Blok İçeriği……13
Tablo 2. Blok zincirde bulunan Blok içeriği……... 14
Tablo 3. Blok zincirde kullanılan veri yapısı……..17

ŞEKİLLER LİSTESİ

Şekil 1. Finansal Teknolojiler……6
Şekil 2. SHA 256 gösterimi ……16
Şekil 3. Merkle Ağacı ……19
Şekil 4. Blok yapısında Merkle Ağacı……20
Şekil 5. Simülatör Çalışma Prensibi İş Akış Şeması……...29
Şekil 6. Simülatör Giriş Sayfası ……30
Şekil 7. Simülatör İşlemler Sayfası ……31
Şekil 8. Simülatör Zorluk Seviyesi ……32
Şekil 9. Simülatör Genesis Blok ……33
Şekil 10. "Mine" butonu görseli ……35
Şekil 11. Blok oluşturulması ……..37
Şekil 12. Oluşan Bloğun diğer düğümlerde gösterimi ……...38
Şekil 13. Zincire yeni blok eklenmesi ……..39
Şekil 14. Eklenen yeni bloğun diğer düğümlerde gösterimi ……..39
Şekil 15. Bloklardaki hash kodu ilişkisi gösterimi ……40
Şekil 16. Bloktaki hash koduna elle müdahale edilmesi ……41
Şekil 17. Node A'daki elle müdahalenin diğer düğümleri etkilememesi ……...41
Şekil 18. Örnek 1 işlem sayfası……42
Şekil 19. Örnek zorluk seviyesi alanı ……43
Şekil 20. Örnek 1 blok oluşturulması ……44
Şekil 21. Örnek blokların diğer düğümlerde gösterilmesi ……..44
Şekil 22. Örnek 2 işlem sayfası …….45
Şekil 23. Örnek 2 blok oluşturulması……46
Şekil 24. Örnek 3 yeni işlem sayfası ……..47
Şekil 25. Örnek 3 blok oluşturulması ……48
Şekil 26. Örnek 4 blokta hash değerinin bozulması.....48
Şekil 27. Örnek 4'te blokta hash değerinin diğer düğümleri etkilememesi……...49

KISALTMALAR

PoS: Proof of Stake

PoW: Proof of Work

Fintech: Finansal Teknolojiler

SHA: Secure Hash Algorithm

Prev: Previous

Nonce; Number only used once

ÖZGEÇMİŞ

Gizem Sarıkaya Yaylamış

Bilgisayar Mühendisliği Ana Bilim Dalı

Eğitim

Yüksek Lisans	2020-Halen	Maltepe Üniversitesi Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Tezli Yüksek Lisans
Lisans	2013	Bilkent Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği
Lise	2006	Malatya Anadolu Lisesi

İş/İstihdam

2017-Halen	Kıdemli İş Analisti- Türkiye Cumhuriyet Merkez Bankası
2015-2017	Uzman İş Analisti – Türk Ekonomi Bankası
2013- 2015	İş Analisti- Akbank TAŞ

BÖLÜM 1. GİRİŞ

Finansal teknolojiler gün geçtikçe ilerlemekte ve gelişim göstermektedir. Teknolojiye paralel olarak finansal alanda da yapılan geliştirmeler zamanla değişim ve büyüme göstermektedir. Finansal teknoloji; teknoloji dünyasına hemen hemen yeni giren bir alan olarak düşünülebilmektedir.

Finansal teknolojilerden günümüzde en yeni olarak kullanılan teknolojilerden biri blok zincirdir. Finans alanında yapılan herhangi bir işte, birçok iş birlikçi, onay mekanizması ve kurallar bulunmaktadır. Blok zincir teknolojisi ile bu yapının biraz daha farklılaşması hedeflenmektedir. Blok zincir ile ortak bir onaya ihtiyaç duymadan dağınık yapıda bulunan bir bilgisayar ağı ile işlemler hızlı şekilde ilerleyebilmektedir. Böylece işlemler geleneksel yapıda olan finansal işlemler gibi olmayıp; hızlı şekilde merkezi bir onay olmadan seri olarak işlenebilmektedir.

Aynı zamanda finansal teknolojilerde blok zincir kullanımı ile fon transferi, kimlik yönetimi, akıllı sözleşmeler farklı kurum ve kuruluşlar tarafından incelenmekte ve günümüzde kullanılabilirliği irdelenmektedir.

Blok zincir teknolojileri, işin genel mantığını anlayabilmek ve etki alanını kavrayabilmek adına önem arz etmektedir. Bu teknolojilere ilk adımda bakıldığında dağıtılmış defter teknolojisi ve blok zincir teknolojisi öne çıkmaktadır.

Bu teknolojilerle beraber blok zincirin finans ve finansa ek olarak mevcutta kullanılan sektörlerdeki etki alanları ele alınmaktadır.

Bu çalışma kapsamında finansal teknolojilerin tanımı, kullanım alanları ve içerikleri, bu teknolojilerin günümüze kadar olan süreçteki gelişimi ve ilerleyişinin incelenmesi sağlanacaktır. Bu duruma ek olarak finansal teknolojiler kapsamında blok zincirin tanımı ve blok zincir teknolojisin anlatan bir simülatör tasarlanması hedeflenmiştir.

Simülatörü oluştururken, blok zincirin ana fikri ve temel yapısı incelenmiş; zincir içerisinde yapılan transactionlar ve bu transactionların sistemde meydana getirdikleri durum değişiklikleri detaylandırılarak; zincirin temelini oluşturan ağ yapısı içerisinde

meydana gelen veri ve kayıt dolaşımı incelenmiştir. Ayrıca blok zincirde oluşan tüm yapılar ve işlemler yapılan simülatör aracılığı ile görselleştirilmiştir. Böylece blok zincir yapısı interaktif hale gelmiştir. Hazırlanan bu simülatör ile örnek uygulamalar yapılmış ve konu hakkında inceleme yapan her bir kullanıcı bahsedilen blok zincir uygulamasını temel fonksiyonları ile detaylı şekilde inceleme fırsatı yakalaması hedeflenmiştir.

Problem

Günümüzde finansal teknolojiler, sanal paralar, bitcoin, akıllı kontraktlar gibi terimler sıklıkla duyulmaktadır fakat bu terimlerin gerçekten ne anlama geldiği, etki alanları, kullanıcıları, arkasında kullanılan teknolojiler ve ortaya çıkan ürünler hakkında gerçekten bilgi sahibi olan insan sayısı yok denecek kadar azdır. Blok zincir kelimesine finansal kuruluşlarda, televizyonlarda ve birçok alanda sıklıkla rastlanılmaktadır. Buna rağmen içeriği ve teknolojisi hakkında akademik olarak fazla bilgi bulunmamaktadır. Bu bilgi eksikliğinden dolayı insanlar bu konuya önyargılı yaklaşabilmekte, dolayısıyla önemini ve gelişimini takip edememektedir.

Bu çalışma ile hem finansal teknolojiler hem de bu alanda kullanılan en önemli teknolojilerden biri olan blok zincir detayları ile incelenerek, bu konular hakkında ürün geliştirmek veya bilgi sahibi olmak isteyen herkese ışık tutacaktır. Tüm bu bilgiler göz önünde bulundurulduğunda tez çalışmasında blok zincir teknolojisini anlatan bir simülatör tasarlanmıştır. Hazırlanan simülatör ile örnek uygulamalar yapılmış ve konu hakkında inceleme yapan her bir kullanıcı bahsedilen blok zincir uygulamasını temel fonksiyonları ile detaylı şekilde inceleme fırsatı bulması da hedeflenmiştir.

Amaç

Finansal teknolojiler, özellikleri, etki alanları ve kullanılan teknolojilerin yanı sıra blok zincir teknolojisi ve temel fonksiyonları detaylı şekilde incelenmiş, terim olarak bilinen bu bilgiler tez kapsamında yapılan simülatör ile görselleştirilmiştir. Somutlaştırmayı pekiştirebilmek adına örnek uygulamalar da simülatör üzerinde gösterilmiş ve detayları ile belirtilmiştir.

Bu sayede öğrenilen bilgiler hem akademik düzeyde çalışma yapmak isteyen kişiler için, hem de bu konularda bilgi sahibi olmak isteyenler için fayda sağlaması öngörülmüştür. Bunun yanı sıra blok zincir dünyası hakkında veya finansal teknolojiler alanında girişimi olacak veya bu konularda geliştirme yapan veya yapacak olan kişilere yol gösterebilecektir.

Önem

Bu çalışmalar ile finansal teknolojiler ve blok zincir üzerinde piyasada oluşan bilgi kirliliğinin temizlenmesine katkı sağlanacak; daha akademik bir bakış açısı ile blok zincirin soyut bir kavramdan daha somut bir kavrama geçişine katkı sağlanacak ve blok zincir altyapısının mevcut durumu ile ilgili analiz çalışması yapılabilecektir.

Yapılan blok zincir simülatörü, temel zincir yapısını öğrenebilmek veya pekiştirebilmek adına fayda sağlayabilecektir. Böylece finans alanında birçok kurum ve kuruluş yapacakları finansal teknoloji ile ilgili gelişmelerinde temel yapıyı oturtabilmek adına bu çalışmadan katkı alabileceklerdir. Buna ek olarak işlerinde fikir oluşturabilecek başlıkları görebileceklerdir. Aynı zamanda kişisel olarak da kendini geliştirmek isteyen insanlar bu çalışmayı inceleyerek temel yapıyı ve onu oluşturan detay bilgiye ulaşabilecek; bu işlerin teknolojik boyutu ve ilerleyişi hakkında bilgi sahibi olabilecektir. Ayrıca akademik çalışma yapmak isteyen kişiler de bütün bir akışı bu çalışma ile görüp, inceleyebileceklerdir.

Varsayımlar

Bu çalışmada akademik olarak fayda sağlayabilmek adına mevcutta finansal teknolojiler ve blok zincir üzerine yapılan tezler incelenmiştir. Bu durumun dışında blok zincir ile geliştirilen uygulamalar ve sunumlar incelenmiş, bilgi sahibi olunmuştur. Akademik dergiler ve makaleler de incelenmiş; ayrıca internette araştırmalar yapılmıştır. Tüm bu ön çalışmalar ışığında genel olarak blok zincir yapısını anlatan, gerçekte oluşan altyapısı ve zincirin arkasında kullanılan ağ ve transaction örgüsünü tanıtan yeterli akademik bilgilere rastlanılmamıştır.

Bu çalışma ile blok zincir yapısının temel yapı taşlarının simülatör aracılığı ile görselleştirerek kullanıcılara fikir vereceği varsayılmıştır.

Sınırlıklar

Blok zincir teknolojisi tüm dünyada yeni ortaya çıkan bir teknoloji olduğu için geliştirilen ve ilerleme kaydedilen ürün sayısı son derecede azdır. Büyük teknoloji firmaları hala etki analizi yapıp, geliştirme adımlarında bulunmaktadır.

Sanal paralar ve bitcoin üzerine birçok ülkenin merkez bankaları ve ticari bankaları da çalışmalarına devam etmekte olup, henüz kendi sanal parasını üretime çıkabilen resmi bir finans kuruluşu olmamıştır.

Birkaç "start-up" firması blok zincir teknolojisi kullanarak yeni ürün girişimlerinde bulunup; henüz üst seviyelere çıkabilen örnekler oluşmamıştır. Dolayısıyla blok zincir teknolojisi kullanılarak ortaya ürün çıkarabilmek elde olan verilere göre zorlaşmaktadır. Aynı zamanda bu yapıyı detaylı ve teknik biçimde anlatıp, uygulamaları olan ve bunları inceleyen ürün sayısı da son derece azdır.

Tanımlar

Finansal teknoloji: Finansal alanda verilen hizmetleri iyileştirmek için teknolojiden faydalanmaya yarayan yeni bir alandır.

Blok zincir (Blockchain): Blok zincir 2008 krizi zamanında Satoshi Nakamoto tarafından kripto para altyapısı olarak tasarlanmış ve bu tasarım ile bitcoin temelini oluşturmuştur. (Nakamoto, 2008)

Bitcoin: Blok zincir altyapısı kullanılarak ortaya çıkan bir kripto para türüdür.

BÖLÜM 2. FİNANSAL TEKNOLOJİLER VE BLOK ZİNCİR

Finansal teknolojilerin tanımı, günümüzdeki önemi, finans işlemleri kapsamında kullanılan teknolojiler ve kullanım alanları incelenmiştir. Finansal teknolojilerin genel işleyişine ek olarak bu teknolojilerde blok zincirin yeri, tanımı, bu teknolojiyi oluşturan temel kavramlar ve blok zincir kullanım alanları detaylandırılmıştır.

Finansal teknolojiler, blok zincir tanımları ve bu teknolojilerin temel yapı taşlarının irdelenmesinin ardından finansal teknolojiler ile blok zincir arasındaki ilişki gözlemlenmiş ve finansal teknolojilerde blok zincir teknolojisinin kullanım alanları üzerine de ağırlık verilmiştir.

2.1 Finansal Teknolojiler

Finansal teknolojiler sözlük anlamı ile finansal alanda verilen hizmetleri iyileştirmek için teknolojiden faydalanmaya yarayan yeni bir alandır. Bu alanda insanların hayatlarını kolaylaştırmak, yardımcı olabilmek adına girişimler yapılıp, teknolojiden faydalanılmaktadır. Terim olarak Fintech olarak da geçmektedir. (Izyco, 2019)



Şekil 1: *Finansal Teknolojiler (FintechTime, 2019)*

Finansal teknolojilerde finans kapsamında yapılacak işlemlerin olabildiğince hızlı, müşteri memnuniyeti ve müşteri odaklı olarak ilerleyebilmesi, mevcutta kullanılan işlemlerin daha güvenilir bir ortamda yapılabilmesi adına ilerleme kaydedilmesi beklenmektedir. Bu teknoloji ile hem kullanılan altyapı daha sağlam olabilecek, verilerin güvenirliği herkes tarafından bilinecek, hem de bu teknolojiler kullanılarak oluşturulan ürünler ile müşterilere yeni bakış açıları kazandırmış olacaktır. Böylece bu teknoloji ile yapılan ürünler ile hem kurumlar hem de müşteriler için daha hızlı ve zaman tasarruflu yapılar kurgulanmış olacaktır.

Finansal teknolojilerin yani kısa adı ile Fintech'in etki alanlarını inceleyebilmek ve detaylarına hâkim olabilmek adına bu teknolojilerin hangi alanlarda kullanıldığı, bu alanların içerikleri, ilk ortaya çıktığı andan günümüze kadar gelen süreçte gelişimi detay şekilde irdelenmeli ve hem kurumlar hem de insanlar üzerindeki etkilerine bakılmalıdır.

2.1.1 Finansal teknolojilerin kullanım alanları

Finansal teknolojilerin gelişimi ve her geçen gün büyümesi ile etki alanı da aynı şekilde değişmekte ve gelişmektedir. Birçok sektör, finansal teknolojilerin etki alanı büyüdükçe birbiri ile etkileşim halinde olduklarından, hızlı şekilde ilerleyebilmektedirler. İnternete erişimin olduğu her yerde kolaylıkla iş yapılabileceğinden, teknolojinin günümüzdeki ilerlemesi göz önünde bulundurulduğunda yeni girişimlerle beraber, farklı birçok sektörün de bu teknolojinin etki alanına girmesi ve ilerlemesi beklenmektedir.

Şu aşamada genel yapılar göz önünde bulundurulduğunda finansal teknolojilerin kullanıldığı sektörler kategorize edilmek istenirse bu teknolojinin en çok kullanıldığı sektörler aşağıdaki gibi gruplanabilmektedir: (Haddad ve Hornuf, 2019)

- Finans Sektörü
- Sigorta Sektörü
- Ödeme Sistemleri
- Risk Yönetimi

Bu şekilde verilen finansal hizmetler, sigorta hizmetleri, ödeme sistemleri ve uygulamaları, risk yönetimi gibi alanlar alt kırımlarında mobil cüzdan olanakları, akıllı sözleşmeler, fon transferleri, kredi skorlama araçları, sigorta kontratları/sözleşmeleri ve hızlı ödeme seçenekleri gibi durumlarla şekillenebilmektedir. Bu örnek alanlar gün geçtikçe dijitalleşmektedir ve gelişimini sürdürüp, arka planında yeni teknolojilerle kendini yenileyebilmekte ve müşterilere hızlı seçenekler sunabilmektedir.

2.1.1.1 Fon Transferleri

Fon transferi tüm dünyada yapılan gerek ülkelerin kendi içlerinde gerekse ülkeler arası yapılan bir işlemdir. Çok sıklıkla yapılan bir işlem olduğundan bu alana dair Finansal teknoloji girişimleri bulunmaktadır. Burada amaç maliyeti düşürmeye çalışarak daha basit bir yapı kurulmasını sağlamaktır. Fon transferlerinde son zamanlarda sanal paralar, elektronik paralar ve kripto paralar ve onların transferleri üzerine fintech çalışmaları yapılmaktadır.

Günümüzde fon transferleri yapıldığında ilgili kurum ve kuruluşlar bu transfler için çeşitli ücretler almaktadır. Bu durumun müşterileri memnun etmediği durumlar da

olmaktadır. Günde birden fazla kez fon transferi yapılan durumlarda aynı müşterinin bu transferler için ödeme yaptığı düşünüldüğünde ortaya çıkan masraf gittikçe artmaktadır.

Fon transferlerinde ayrıca kullanılan altyapılardan kaynaklı veya ülkeler arası fon transferi durumlarında fonların hızlı şekilde gitmesinde de teknik olarak bazı sorunlar yaşanabilmektedir. Teknik olarak yaşanabilecek aksaklıkların yanı sıra ülkeler arası fon transferlerinde tabii olunan çeşitli kural ve yasalardan dolayı anında transfer imkanı olamayacağı; bir yerden başka yere ve kişiye fon transfer isteği yapıldığı andan itibaren de arka planda çeşitli kurallardan geçilebileceği için uzun sürebilmekte ve anlık transferler olmayabilmektedir.

Günümüzde gelinen noktada fon transferi sanal paralar, elektronik paralar ve kripto paralar üzerinde de yapabilmektedirler. Böylece fiziki bir para olmadan elektronik ortamda değeri ilgili mercilerce kabul edilen paraların transfer imkânı da yeni gelişen finansal teknoloji ürünleri ile yapılmakta ve bu ürünlerin gelişimi de gün geçtikçe artmaktadır.

2.1.1.2 Ödeme Sistemleri Uygulamaları ve Sanal Paralar

Ödeme sistemleri fon transferleri, kredi kartı ve diğer kart işlemlerinde kullanılmaktadır. Finansal teknolojiler ile bu işlemlerin daha az maliyet ve hızlı bir şekilde yapılmasına olanak tanıyan uygulamaların geliştirilmesi hedeflenmektedir. Bu uygulamalar ile sanal paralar oluşacak ve bu paraların yönetimi yeni uygulamalar üzerinden yapılabilecektir.

Mevcutta günümüzde kredi kartları genel bağlamda fiziki olarak kullanılmakta ve kişilerin yaptıkları işlemler yani ödemeler fiziksel kart ile olmaktadır. Yeni geliştirilen ve gelişimi devam eden teknolojik ürünlerle fiziki kartların yanı sıra cep telefonlarında kullanılacak mobil uygulamalar ile ödemelerin gerçekleştiği ve bu gelişimin devam edeceği öngörülmektedir.

Kredi kartlarına benzer şekilde sıklıkla kullanılan banka kartları için de fiziki kart halinden mobil teknolojiye evirilmesi de hızlı şekilde olabilmektedir. Bankamatiklerden çekilen fiziksel paralarda günümüzde bile artık fiziksel banka kartına ihtiyaç olmamakta; bankaların mobil uygulaması üzerinden barkod okutularak ilerletilmekte ve para çekimi

sağlanmaktadır. Bu konuda yapılan çalışmalar günümüzde ilerlemiş ve bir noktaya gelmiş olsa da ilerleyen dönemlerde finansal teknolojilerin gelişmesi ile daha farklı bakış açıları getirilmesi ve bu ürünlerin iyileştirilmesi hedeflenebilmektedir.

2.1.1.3 Kredi Skorlama İşlemleri

Kredi işlemlerinde kullanıcıların fatura ödeme bilgileri, alınan / verilen kredilerin ödeme zamanları, kredi tutarları gibi bilgiler baz alınarak her müşteri için bir skorlama çıkarılıp, müşterinin karnesi şeklinde sunulmaktadır. Fintech ile bu veriler kolaylıkla toplanarak yeni skorlama ürünleri geliştirilebilecektir.

Skorlama işlemlerinde müşterilerin içinde para barındıran bütün detaylar izlenebilmekte ve yapılan veya ödenen harcamalara göre müşteriler için çeşitli istatistikler çıkarılabilmektedir. Bu kapsamda müşterilerin yaptığı bütün geçmiş işlemlerin bilgileri tutulmaktadır. Böylece daha önceden alınan krediler; ödenen krediler, hesapta bulunan bakiye bilgileri, para transferleri, kredi kartı harcamaları, kredi kartı ödeme bilgileri, kredilerin ve kredi kartlarının ödeme zamanlarında gecikme olup olmadığına bakılması gibi bütün detay bilgiler tutularak, her müşteri için bir skorlama kartı oluşmaktadır. Böylece bu skor kartı, müşteri yeni bir kredi çekmek veya kredi kartı almak istediğinde bile analiz edilerek kredi verecek veya kredi kartı teslim edecek kurum ve kuruluşlar için bilgi vermektedir.

Finansal teknolojiler kapsamında kredi skorlama işlemleri de baz alınarak bu ürünleri geliştirmek adına yeni ürünler sunulmakta ve bu gelişime devam edilmesi beklenmektedir. Bu kapsamda yeni geliştirilen ürünler ile hem müşteriler için hem de bu bilgileri kullanan kurum ve kuruluşlar için daha esnek yapıda ve daha detay bilgileri içeren ve müşterinin nakit akışını gösterilecek arşiv bilgileri de detaylı şekilde görülebilecektir.

2.1.1.4 Sigorta İşlemleri

Sigorta işlemleri ile sigorta veren firmalar bu teknolojiler ile birleşerek internet üzerinden verilen hizmetleri daha hızlı ve müşterinin zaman kazancı olacak bir yaklaşımla güvenilir bir platform üzerinden sağlayabilmektedirler.

Sigorta işlemleri insanların sağlık işlemleri üzerine olabildiği gibi taşınabilir ve taşınmaz mallar üzerinde de yapılabilmekte ve sigortacılık ürünleri olarak bakıldığında çok geniş bir yelpazeye yayılabilmektedir. Sigorta işlemleri kapsamında herhangi bir insan veya ürün sigorta ettirilmek istendiğinde fazla sayıda belge olup, bu belgelerin her biri için müşterinin imzası gerekmektedir.

Finansal teknolojiler kapsamında sigortacılık ürünleri de fiziki kâğıt işlemlerinden ayrılıp, mobil şekilde ilerleyebilecek ürünler sunularak gelişim göstermesi hedeflenebilmektedir. Böylece fiziksel kağıtlar üzerinde yapılan işlemler mobil ortamlara aktarılabilecek; ortaya çıkan belgelerin her bir sayfasında atılan ıslak imzalar yerine artık mobil uygulamalarda oluşacak mobil onay durumları ile daha hızlı şekilde yapılabilecektir. Böylece yapılan işlemler hem daha hızlı olarak yapılabilecek; müşteri ve kurum açısından zaman kazancı olabilecek; bu işlemler kapsamında ortaya çıkan kâğıt israfının önüne geçilmiş olacak ve belgelere dair arşiv bilgisine ulaşım daha kolay olabilecektir.

2.2. Blok Zincir Teknolojisi

Blok zincir 2008 krizi zamanında Satoshi Nakamoto tarafından kripto para olarak tasarlanmış ve bu tasarım ile bitcoin temelini oluşturmuştur. Burada ortaya çıkan ürün, dağıtılmış defter yapısı olarak planlanmıştır. (Nakamoto, 2008)

Blok zincir genel olarak bakıldığında bir veri yapısıdır. Bu teknolojinin temelinde bir dijital defter oluşturulur. Blok zincir veri yapısında işlemler/veriler bu dijital defterde tutulur ve dağınık bir şekilde olan bilgisayar ağları arasında bu defterin paylaşılmasını sağlamaktadır.

Burada geleneksel yapıdan ziyade, ortak bir otorite olmadan dağınık ağda bulunan her kullanıcı ile kayıt oluşmasına imkân sağlanabilmektedir. Bu kayıt sırasında şifreleme yapılmaktadır. Blok zincir üzerinde oluşan bu şifreleme durumu yapılan işlemlerin güvenilir bir şekilde zincirde tutulmasını sağlamaktadır. Blok zincir içerisinde her bir veri kaydedildiğinde – burada veriler, veri bloğu olarak düşünülmektedir- bu kayıt üzerinde herhangi bir silme, güncelleme yapılması mümkün olmamakta, yapılan her işlemin verisi blok zincirdeki bloklarda arşiv bilgi olacak şekilde tutulmaktadır.

2.2.1 Blok Zincir Tanımı ve Temel Yapısı

Blok zincir teknolojisinin temelinde dağınık bir ağ yapısı bulunmaktadır. Bu dağınık yapı ile sisteme kayıtlı olan birçok kullanıcı işlemlerini kaydedip, takip edebilmektedir. Bu işlemler güvenli bir şekilde blok zincirde tutulmaktadır. Böylece diğer kullanıcılar da bu işlem kayıtlarını görebilmektedir. Bu aşamada herhangi merkezi, ortak bir onay yapısı bulunmamaktadır.

Bu teknolojinin temelinde belirli kavramlar bulunmaktadır. Bu kavramlar aşağıdaki gibidir:

- Node (Düğüm)
- Blok
- Hashing
- Ağ yapısı
- Merkle Ağaçları
- Mutabakat
    - Proof of Work
    - Proof of Stake

2.2.1.1. Node (Düğüm)

Blok zincir içerisindeki yani bu ağdaki her bir cihaza node (düğüm) denilmektedir. Bilgisayar, cep telefonu ve bunlar gibi internete bağlı olabilen ve IP adresi barındırabilen her bir ürün node (düğüm) olarak değerlendirilebilir. Bu teknolojide en temel kısım bu düğümlerdir. Her bir düğüm ile blok zincirdeki blokların kopyası tutularak ve bu bloktaki işlemler çalıştırılarak bu ağ desteklenmektedir.

Blok zincir içerisinde kullanılan madencilik işlemlerinde yüklü seviyede bilgisayar işlem gücü lazım olduğundan bilinen bilgisayarların işlem gücü yetersiz kalabilmektedir. Bu noktada bu işlem gücünü sağlayabilmek adına yüksek donanımı olan nodeler (düğümler) tercih edilebilmektedir. (Atabaş, 2018) Bu durum bitcoin madenciliğinde göze çarpmaktadır.

Zincirde bulunan Nodelar (düğümler) birbirine eşittir fakat bu nodelar ağı farklı şekillerde destekleyebilmektedir. Bu nodeların tümü bir blok zincir yapısına bağlıdır

fakat bu nodeların hepsi bu yapının tümünü depolayamayabilirler; böyle bir durumda parçalara bölünür ve bu şekilde kopyalanıp, depolanabilmektedir. Bu durum olsa dahi her node birbiriyle mantık olarak bir bütün halinde bulunmalıdır.

Zincirde oluşan her bir blok ağı farklı şekilde destekleyen nodelarda tutulur. Bir node (düğüm) içerisinde görünen ve onaylanan bloklar, blok içerisinde güvenliği tehdit eden herhangi bir unsur olmadığı sürece tüm nodelarda aynı şekilde görünür ve geçmiş bloklara dair bilgiler de aynı şekilde tüm nodelarda görünür olmaktadır.

2.2.1.2 Blok

Blok zincirde ilgili veriler blok denilen bir yapı üzerinde tutulmaktadır. Bir blok içerisinde blok numarası, başlığı, bir önceki blokta bulunan verilerin bilgileri ve ilgili bloktaki verilerin özellikleri bulunmaktadır.

Her bir blokta, bir önceki bloktaki şifre olmasından dolayı güvenlik açısından yüksek seviyelerdedir. Hepsi bir zincir olarak birbirine bağlı olduğundan bir blokta şifre değiştiğinde, diğer bloklar da etkileneceğinden ve bozulacağından güvenlik üst seviyelere taşınabilmektedir. (Günen, 2020)

Bir blok içerisinde bulunabilen bitcoin blok bilgileri temsili olarak aşağıdaki gibidir:

BITCOIN BLOK İÇERİĞİ			
Sihirli sayı		4 byte	"0xD9B4BEF9" şeklinde sabit değer
Yükseklik		4 byte	Blok numarası
BAŞLIK (HEADER)	Versiyon	4 byte	Kullanılan güncel sürüm
	Önceki başlık	32 byte	Önceki blokun başlık özeti (hash)
	Merkle kökü	32 byte	İşlemlerin özet değeri (hash)
	Zaman damgası	4 byte	1 Ocak 1970'ten itibaren geçen süre
	Zorluk	4 byte	Ağın zorluk bilgisi
	Nonce	4 byte	Ağ zorluğuna göre ayarlanmış rastgele sayı
İşlem sayısı		1-9 byte	Belirli uzunlukta tam sayı değeri (integer)
İşlemler		-	Bloktaki transferlerin listesi

Tablo 1: *Blok içeriği (Günen, 2020)*

Burada "sihirli sayı" olarak geçen değer hash değerini ifade etmektedir. Bu değer bloğa özgü bir değerdir.

"Yükseklik" denilen değer, o bloğun numarasını ifade etmektedir.

"Başlık (header)" alanında, kullanılan güncel sürüm; bir önceki bloğun hash değeri, o blokta var olan işlemler, zaman bilgisi, "zorluk" ve "nonce" bilgisi bulunmaktadır. Burada "nonce" değeri yetkilendirme için kullanılan rastgele bir değerdir. "Başlık (header)" alanında bulunan "Zorluk" değeri, bitcoin madenciliğinde oluşturulacak hash kodunun başında kaç tane sıfır olacağını belirleyerek ağın zorluk seviyesini belirlemektedir.

Nonce değeri; "Number only used once" olarak geçen terimin kısaltılmasıdır. Bu değer elde var olan belirli bir kriter için oluşturulan sayıdır. Blok zincirin kullanıldığı Bitcoin işlemlerinde madenciler (yani ağa bağlı bilgisayarlar) bu değeri bulmaya

çalışmaktadırlar. Bu madencilik işleminde asıl önemli olan 2 değer vardır; bunlar “hash” ve “nonce” değerleridir.

Aşağıdaki örnek resimde Blok zincir teknoloji kapsamında oluşan işlemler baz alınarak meydana gelen bir blok örneği bulunmaktadır. Bu örnekte “hash” değeri birçok sıfırdan meydana gelmektedir. Bitcoin’de, hash değerinin önünde birçok sıfır değerinin bulunması bilinen bir durum olmakla birlikte, bitcoin madenciliği bu birçok sıfırlı hash değerini bulabilmek için farklı “nonce “değerlerini kullanırlar. Bu örnekte “nonce” değeri 56.775.714 olarak görünmektedir. “Nonce” değeri değişken bir değer olduğu için madencilik yapan kişiler, blok içerisinde sabit verileri kullanarak “nonce” değerini değiştirerek kullanabilmektedir. “Nonce” değerleri kullanıcılar tarafından denenerek, oluşan hash kodunun başında zorluk derecesinde belirtilen adette sıfır sayısını bulana kadar devam etmektedirler. Belirtilen sıfır kadar değeri hash kodunda bulunca işlem tamamlanmış olup, blok oluşmakta ve zincire eklenmesi için kullanıcıların onayına gitmektedir. (Günen, 2020)

Hash	00000000000000000036d2d80c0e1e21e324c13e6b4d93e8a267971c744e6c3
Onaylar	1
Zaman Damgası	2021-10-10 22:59
Yükseklik	704425
Kazıyıcı	F2Pool
İşlem Sayısı	306
Zorluk	19.893.045.048.575,13
Merkle kökü	0c0d26de4544b9f92b04230a4623152c9ff5b0a1c5ab2800e57d1b4401d4e838
Versiyon	0x3fff0004
Bit	386.803.250
Ağırlık	279.189 WU
Boyut	107.712 bytes
Yalnızca Bir Kez Kullanılan Sayı (Nonce)	56.775.714
İşlem Hacmi	24870.76983851 BTC
Blok Ödülü	6.25000000 BTC
Ücret Ödülü	0.00920422 BTC

Tablo 2: *Blok zincirde bulunan Blok içeriği (Blokchain, 2021)*

“İşlem sayısı” o blokta bulunan işlem sayılarını belirtmektedir; blokta kaç tane işlem varsa onların sayısını belirtir.

“İşlemler” ise blok içerisinde bulunan işlemleri belirtmektedir.

“Blok ödülü” alanı ise yapılan madencilik işlemlerinde zincirde oluşan transferler baz alınarak blok oluşturulması için “mine” edildiğinde o blok için belirtilen hash kodu ve nonce değeri bulunduktan sonra blokların zincire eklenmesi tamamlanmış olmaktadır. Bloklar zincire eklendiğinde yani onaylandığında bu işlem için efor sarfedildiğinden, işlemi yapan kullanıcılara bloğu bulup, zincire ekledikleri için ödül mekanizması olarak belirli bir miktar ilgili para biriminden verilmektedir.

“Boyut” alanı ise o blokların içerisindeki işlemlerden oluşan listenin yani bekleyen işlemlerin o blokta ne kadarlık yer kapladığını gösteren bir değer olup, byte cinsinden gösterilmektedir.

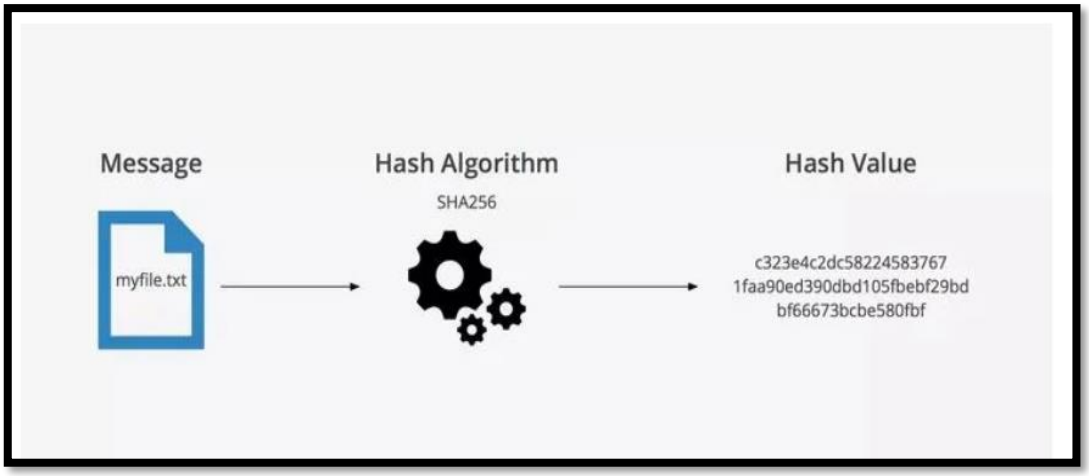
“İşlem hacmi” alanında o bloğun oluşmasında sırasında baz alınan işlemlerin toplam ne kadarlık hacim yarattıkları bilgisi tek bir değer olarak gösterilmekte ve o blok oluşunca içerisinde ne kadarlık işlemin transfer edildiği gösterilmektedir.

2.2.1.3. Hashing

Şifreli sabit bir değer ortaya çıkmasına hashing denir. Secure Hash Algorithm (SHA) özet bir değer üretmektedir. Bu algoritmalar ile büyük verilerden daha küçük özet bilgiler çıkarılabilmektedir ve bu durum kişisel dijital bir parmak izi olarak düşünülebilmektedir. Küçük veri değişiklikleri olsa da farklı özet bilgiler ortaya çıkabilmektedir (Usta A ve Doğantekin S, 2017).

Blok zincir teknolojilerinde Secure Hash Algorithm kullanılmaktadır. Son zamanlarda bitcoin işlemlerinde de kullanılan algoritma SHA 256’dır. Bu algoritma ile ne kadarlık bir girdi olsa da 32 karakterlik çıktı bilgisi verilmektedir. Blok zincirde bloğun içerisindeki tüm veriler birleşerek hash kodunu oluşturmaktadır.

Hash kodunun en temel halinden SHA 256 algoritması ile nasıl oluştuğuna ait görsel aşağıdaki gibidir:



Şekil 2: *SHA 256 gösterimi (Vargönen, 2020)*

SHA 256 algoritmasında ne kadarlık bir veri girilirse de hash algoritmasına girildiğinde ortaya 32 karakterlik tek bir değer çıkmaktadır. Burada girilen veri bir karakter de olabilir, 200 sayfalık bir roman da olabilmektedir fakat SHA 256 algoritması ile girilen verilerin ne kadarlık boyutta olduğunda bakılmaksızın ortaya çıkan değerin her zaman 32 karakterlik olduğu görülmektedir.

Blok zincir altyapısı kullanılarak buradaki veriler, bekleyen işlemlerin listesi olabileceği gibi, dosya transferlerinde istenilen dokümanların da buraya veri girdisi olarak kullanılabileceği düşünülmektedir. Bu veri kümeleri de yine SHA 256 algoritması kullanılarak şifrelenmekte ve bu şifreleme yapısı ile güvenli bir şekilde zincirde yerini alabilmektedir ve rastgele algoritmadan gelen 32 karakter çıktısı ile gösterilmekte ve tahmin edilmesi ve dış etkenler tarafından müdahale edilmesi zorlaşmaktadır.

2.2.1.4 Ağ Yapısı

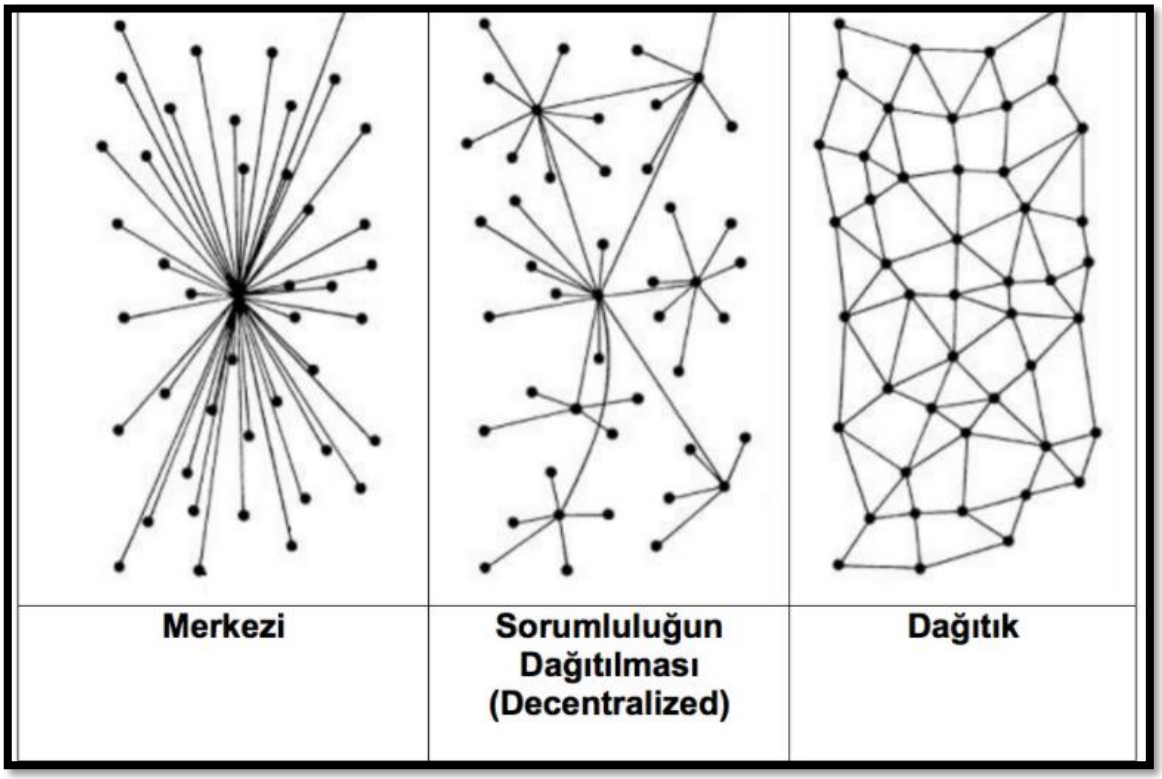
Blok zincir veri tabanlı art arda gelen bir zincirdir. İlk veri girişi anından itibaren bloklara giriş yapılarak ve blokların da birbirilerine bağlanarak zincire eklenmesi ile sonsuza kadar gidebilmektedir. Bu veriler eklenirken herhangi bir noktadan başlanabilmekte, blok zincir içerisinde tüm kullanıcılar bu aşamadan itibaren etkilenip, kullanabilmektedir. Böylece bilinen bir veri kaydı, zincirde bulunan farklı bilgisayarlarda üzerinde tutulabilmektedir. Bu yapı dağıtık ağ yapısı olmaktadır. Dağıtık ağ yapısı ile bir

veri, ağdaki tüm bilgisayarlarda bulunduğundan, ağdaki herhangi bir bilgisayarda bilgi gitse de diğer bilgisayarlarda tutulmaya devam ettiğinden uygulamada bir sıkıntı olmadan çalışma devam edebilmektedir.

Aşağıdaki örnek ekran görüntüsünde ilk resimde bulunan ağ yapısı "merkezi" yapıyı ifade etmektedir. Bu yapıda her kullanıcı nihai halde aynı bilgisayara bağlı olarak düşünülebilmektedir.

Ortadaki resimde bulunan ağ yapısı "sorumluluğun dağıtılması "olarak düşünülüp; kullanıcıların ortak bir merkeze bağlanmayıp, kendi içlerinde en verimli olduklarını düşündükleri sunuculara bağlanması ile neticelenmektedir.

Sondaki resimde bulunan ağ yapısı "dağıtık" olarak düşünülüp; ağ içerisindeki kullanıcılar aynı zamanda verinin sahibi olup, veri sağlayanlar olarak düşünülebilmektedir.



Tablo 3: *Blok zincirde kullanılan veri yapısı (Tübitak, 2017)*

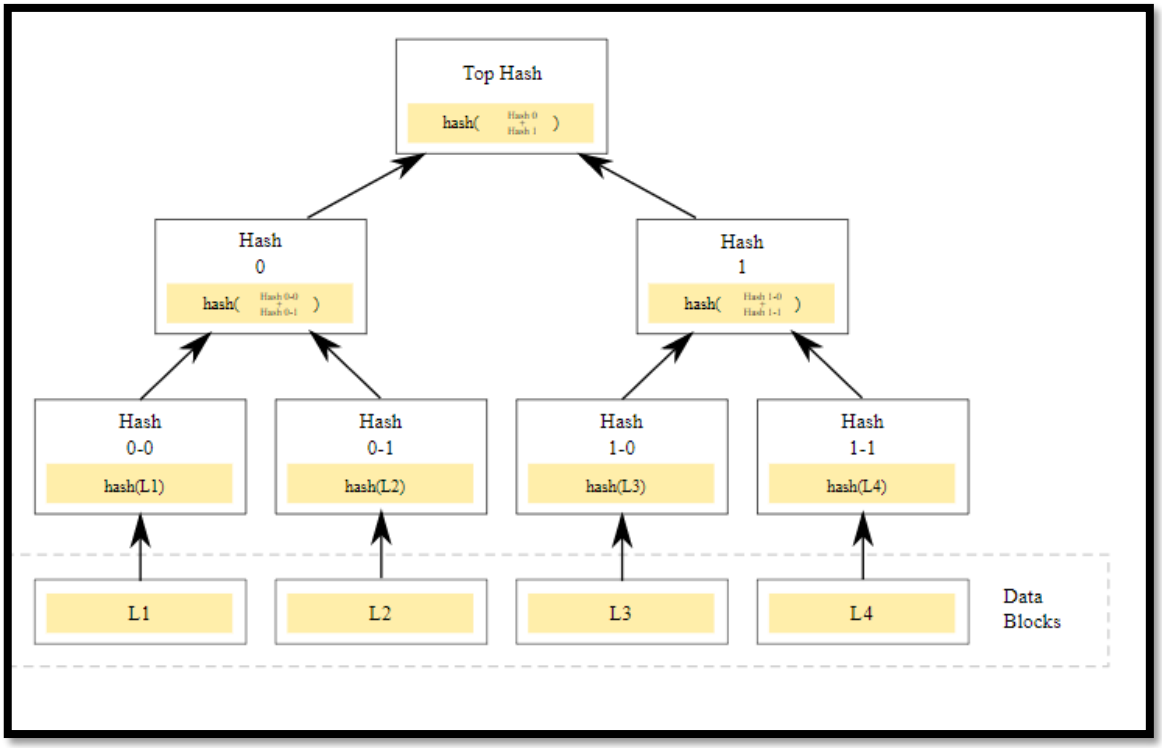
Blok zincir teknoloji “dağıtık” yapıyı kullanmaktadır. Bu yapı ile merkezi bir sistem olmayıp, ağdaki tüm kullanıcılar veri sağlayıcısı olarak hareket edebilmektedir. Böylece, ağ içerisinde bulunan tüm kullanıcılar eşit haklara sahip olabilmektedir.

Blok zinciri diğer teknolojilerden ayıran en önemli özelliklerinden biri de bu dağıtık ağ yapısıdır. Blok zincir kapsamında temel kavramlardan olan nodelar (düğümler) burada dağıtık ağ yapısının birer noktaları olarak düşünülmelidir. Her bir node, bu ağ içerisinde bir nokta olarak yerini alıp, diğer nodelarla bağlantı da zincir ile sağlanmış olmaktadır.

2.2.1.5 Merkle Ağaçları

Bir işlemde orijinal bilgiyi tutabilmek için özet anlamında bir tanımlama kodu bulunmaktadır. Blok içerisinde özet tutulan bu değerlerin hepsi “Merkle Ağaçları” altında değerlendirilmektedir.

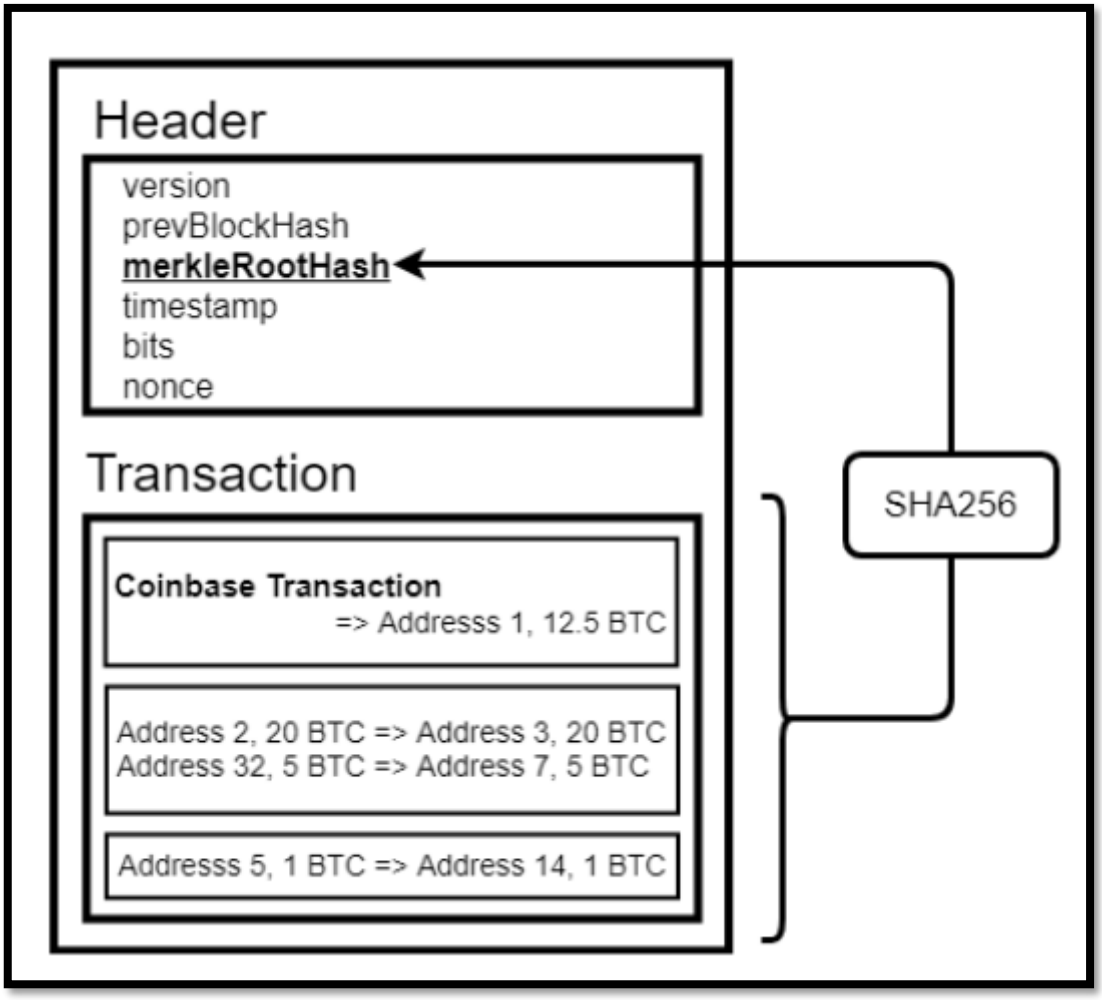
Bir özet değerde, önceki blokta bulunan özet bilgiler ve özellikleri yeni bloğa tanışmalıdır. Böylece yeni blok içerisinde, bir önceki blokta bulunan bilgiler olmaktadır. Bu durum blokların değiştirilmesini ve herhangi bir şekilde üçüncü kişilerin eline geçip, kötü niyetli kullanılmasını engelleyebilmektedir. Merkle ağacı ile bloktaki bütün işlemler organize edilebilmektedir; böylece veriler düğümler halinde ele alınarak bütünlükleri korunabilmektedir.



Şekil 3: *Merkle Ağacı (Wikipedia, 2021)*

Her bir üst düğüm, alttaki iki düğümün birleşimi ile oluşur; bu durum köküne kadar devam eder ve böylece kökünde son özet bilgisi de tutulur. Böylece blok içerisinde bulunan tüm işlemler için bir hash değeri oluşunca; oluşan hash değeri merkle ağacı sayesinde oluşup, buradaki kök değeri alınmaktadır.

Aşağıdaki örnek ekran görüntüsündeki gibi blok içerisindeki işlemler alınır ve merkle ağacı yapısı ile SHA 256 algoritması ile kök değeri alınarak hash değeri bulunur ve bloğun içerisine yazılır.



Şekil 4: *Blok yapısında Merkle Ağacı (Researchgate, 2018)*

Blok yapısı içerisinde ne kadarlık işlem girilirse girilsin her bir işlem için Merkle ağacı yapısı baz alınarak tüm işlemler için SHA 256 algoritmasına tabii tutularak en son adımda tek bir kök merkle değeri bulunması sağlanır. Oluşan merkle kök değeri blokta tek bir hash değeri olarak yerini almaktadır. Her bir işlemin Merkle ağacı yapısına sokulması ile işlemlerin her birinin ayrı ayrı şifrelenmesinden dolayı güvenlik daha sıkı olmakta ve dış etkenler tarafından tahmin edilmesi ve yazılıma zarar vermesi daha da zorlaşmaktadır.

2.2.1.6 Mutabakat

Blok zincirde her bir gelen düğümde blokların onaylanması ve zincire eklenmesi gerekmektedir. Bu durum bu ağda bulunan kullanıcıların kabul etmesi anlamına gelmektedir. Bu kabul etme işlemi mutabakat olarak değerlendirilmektedir.

Mutabakat işleminde de her bir düğümde tüm ağ yapısı değişebileceğinden farklı görünümler ortaya çıkabilmektedir. Bu farklı görünümü yok edebilmek adına ve tek bir noktaya varabilmek için mutabakat protokolleri kullanılmaktadır. Bunlara örnek Proof of Work ve Proof of Stake verilebilmektedir.

2.2.1.6.1 Proof of Work (PoW)

Siber saldırılara karşı önlem olarak ortaya çıkan bir protokoldür. Blok zincir ağında bulunan bilgisayarların bu ağda işlem yaptıklarını ispat ettikleri yöntemdir. Blok zincirde bulunan blok yapısında başında sıfır kullanılacak zorluk seviyesine göre (hash kodunun başında kaç tane sıfır değeri olacağı, o bloğun zorluk seviyesini belirtmektedir) belirlenmiş hash kodunu yakalayabilmek için madencilik yapıldığı zaman, belirtilen hash değerine ulaşmak için "nonce" sayısını bulmaya çalışırlar. Bu sayı rastgele bir sayıdır. Doğru sonucu bulana kadar birçok kez deneme yapılır ve doğru "nonce" sayısı ile başında istenilen kadar sıfır bulunan hash kodu elde edilmiş olur. Böylece ilk madencilik işlemi gerçeklemiş olur ve proof of work bu durumu onaylar. Yani bu işlem için emek sarfedildiği görülür ve gereken işlem gücü harcanmıştır.

2.2.1.6.2 Proof of Stake (PoS)

Proof of Stake protokolü, Proof of Work protokolüne alternatif olarak ortaya çıkmıştır. Burada diğer protokolden farklı olarak işlem gücü veya hesaplama gücüne bakılmaksızın elde olan dijital varlıklara bakılmaktadır. Burada yapılan işlemlerin içinde olduğu blokların doğrulanması kripto para birimleri kullanılarak yapılmaktadır. Burada blokların doğrulanmasını isteyen kullanıcılar kripto para varlıklarını belirttikleri ölçüde kilitler. Bu kilitleme işlemi ile doğrulama işleminde kullanılmak istenen tutar, kilit kaldırılana kadar cüzdanlarında durur ve bu tutar ile işlem yapılamaz. Her kullanıcı blok doğrulama için farklı miktarlarda tutarı hesaplarında kilitleyebilirler. Blok doğrulandıktan sonra ise doğrulama ile kazanılacak tutar, doğrulama işlemi için cüzdanlarında kilitledikleri

para miktarlarına göre orantılı şekilde paylaştırılır. Bu durumda doğrulama işlemi için ne kadar çok tutar kilitli yapıldıysa, o kadar çok tutar kazanılabilmektedir.

Proof of Stake ile, Proof of Work protokolünden farklı olarak blokların doğrulaması için yüksek enerji tüketimi olmaması da hedeflenen kontrollerden biri olarak düşünülebilmektedir. (Btcturk, 2020)

2.3. Blok Zincir Kullanım Alanları

Blok zincirle beraber ortak bir onay yapısı olmadan, şeffaf bir şekilde aynı ağda bulunan katılımcılar işlemlerini güvenli bir ortam içerisinde gerçekleştirebilmekte ve başka kurum/kuruluş ve onaya ihtiyaç duymadan ilerlenebilmektedir. Güven ortamı olası siber saldırılara karşı çeşitli önlemler alınarak yapılabilmektedir. Blok zincir ile yapılan işlemlerde mevcutta var olan işlemlerin yapılmasına kıyasla çok daha az masraf ve risk oluşmaktadır.

Bütün bu durumlar göz önünde bulundurulduğunda birçok alanda blok zincir alt yapısı kullanılarak işlemler yapılabilecektir. Bu uygulama alanlarından bazıları aşağıdaki gibidir: (academy.binance.com, 2020)

- Kripto paralar
- Kimlik Tanıma Sistemi
- Enerji Sektörü
- Akıllı Sözleşmeler
- Finans Sektörü
- Tedarik Zinciri Uygulamaları
- Yardım Kuruluşları
- Sağlık Hizmetleri
- Ödeme Sistemleri

2.4. Blok Zincir ile Finansal Teknoloji Arasındaki İlişki

Mevcutta bulunan finans kuruluşlarının temelinde her zaman bir onay yapısına ihtiyaç duyulmaktadır. Blok zincir bu duruşa farklı bir boyut getirerek merkezi onay yapısı olmadan, hızlı bir şekilde bir ağ üzerinden işlemlerin yapılmasını, ilerlemesini ve

sonlanmasını sağlayan yapı olarak ortaya çıkmıştır. Sağladığı güven ortamı da insanları buraya yönlendirebilmektedir.

Finans sektörlerinin başında bankalar gelmektedir. Bankalar gerek sağlam onay yapısı gerek çeşitli kurallara sonuna kadar bağlı olması sebebiyle sıkı kurumlardır.

Bankaların genel işleyişi ve süreçleri de kolay kolay değişmemektedir. Blok zincir ile bankacılık sektörüne de hareket gelmesi ve farklı bir bakış açısının kazandırılması düşünülmektedir.

Bankacılık alanlarında çeşitli kredi sözleşmeleri, müşteri edinim dokümanları gibi belge gerektiren ve müşteri imzası bulunması zorunlu olan belgelerin blok zincir teknolojindeki akıllı kontratlar ile yerini alması beklenmektedir.

Aynı şekilde fon transferleri bankaların sıklıkla yaptığı işlemlerden biridir. Blok zincir teknolojisi ile masrafsız ve güvenilir şekilde fon transferleri yapılmasına olanak tanınarak fon transferi olayına farklı bir bakış açısı getirebilmektedir. Ayrıca her bankanın kendi sanal parasını yaratarak bunu piyasalarda farklı alanlarda kullanabilme ihtimali bile bankacılık sektörüne yeni bir heyecan getirmektedir.

Bütün bu durumların temelinde blok zincir teknolojisinin güvenilir olması ve siber saldırılara karşı önlemlerinin güçlü olması ileride bankaların kullanması için de başlı başına bir sebep olabilecektir.

Bu ve bunun gibi örnekler ile bankacılık sektörünün blok zincir teknolojisinden fazlasıyla etkilenebileceği ve teknolojilerinde blok zincir kullanabilecekleri öngörülmektedir.

2.5. Finansal Teknolojilerde Blok Zincir Teknolojisinin Kullanım Alanları

Finans sektöründe, özellikle bankalarda, blok zincir kullanım alanları ve ileride teknolojinin ve bankaların sağlayacağı güven ortamlarıyla kullanabilecekleri alanlar gün geçtikçe ilerlemekte ve genişlemektedir. Bu bilgiler baz alındığında blok zincirin kullanım alanları ve müşteri ihtiyaçlarının yanı sıra kurum ve kuruluşların da ilerleyen bu teknolojilere uyum sağlaması adına gelişim kaydetmeleri gerekmektedir.

Bu bilgiler göz önünde bulundurulduğunda finansal teknolojilerde blok zincir teknolojisinin kullanım alanları genel haliyle aşağıdaki gibidir:

- Uluslararası Fon Transferi
- Kimlik Tanıma Sistemi
- Kredi Skorlama İşlemi
- Akıllı Kontratlar

2.5.1. Uluslararası Fon Transferi

Bankalarda fon transferi hem bulunulan ülke içinde hem de ülkeler arası yapılabilmektedir. Bu işlem birçok müşteri tarafından aynı gün içerisinde sıklıkla ve belirli bir güven ortamında gerçekleşmektedir. Blok zincir ile uluslararası fon transferi farklı bir boyuta taşınabilmektedir. Blok zincir ile mevcutta var olan aracılar ortadan kaldırılarak direkt müşteriden müşteriye olacak şekilde, hızlı ve nerdeyse masrafsız olarak ve blok zincirin getirdiği kendi güven ortamı ile sağlanabilecektir. (fintechistanbul.org, 2019)

Bu teknoloji ilerleyen dönemlerde kullanılabilecektir fakat kanunlar ve kurallar çerçevesinde mevcut durumda engeller ve öğrenilmesi gereken tecrübeleri bulunmaktadır. Çünkü blok zincirde sanal paralar kullanılacaktır fakat ülkeler içerisinde veya ülkeler arasında sanal paralarda yapılacak düzenlemeler ile ilgili kuralların sınırları yeterince tanımlanmamıştır.

2.5.2. Kimlik Tanıma Sistemi

Finans sektöründe müşteri edinimi sırasında veya banka ya da sigorta şirketlerinin çeşitli ürünlerini müşterilere satma süresince kimlik tanımlanmasına ihtiyaç duyulmaktadır. Herhangi bir müşterinin bir bankaya veya sigorta şirketine tanımlanması; bu banka veya sigorta şirketlerinden ürün alması süresince kimlikleri, ehliyetleri veya çeşitli tanıtım kartları ile kendilerini göstermek zorundadırlar. Bu durum hem banka için maliyet gerektirmekte hem de müşteri için birçok belgeye imza atmak durumunu ortaya çıkarmaktadır. (Karahan Ç ve Tüfekçi A, 2020)

Blok zincir ile kimlik tanımlama kısmında da yenilikler olabilecektir. Kullanıcılar kendilerini istedikleri gibi tanımlayabilmekte ve kimlerle hangi adımlarla

paylaşabileceğini seçebilmektedir. Blok zincir ağında bulunan kullanıcılar bu bilgilere ihtiyaçları doğrultusunda ulaşabilecektir. Fakat buradaki durum da uluslararası fon transferi durumuna benzer şekilde gerekli kurallar ve standartlar henüz yeterince açık olamadığı için geliştirme aşamasında şeklinde düşünebilir. (Karahan Ç ve Tüfekçi A, 2020)

2.5.3. Kredi Skorlama İşlemi

Finans kuruluşlarından kredi veren kurumlarda skorlama işlemi yapılmaktadır. Kredi skorlama yapılırken müşterinin veya müşterinin sahip olduğu şirketin/kurumun kredi bilgileri, borç ödeme dönemleri, hesap bakiyeleri gibi birçok parametreye bakılmakta ve bu parametreler sonucunda her bir müşteri/şirket için bir kredi skoru çıkmaktadır. Bu skora göre müşteriye kredi verilip, verilmeyeceği ile ilgili genel bir kanıya sahip olunur.

Fakat her bir müşterinin banka hesabı veya kredi geçmişi bulunmayabilir. Bu durumda olan müşterileri veya şirketler için skorlama sıkıntı olabilmekte ve işlem yapamamaktadırlar. Blok zincir ile işlem yapamayan bu kitle göz önünde bulundurularak bu sisteme kaydolan kişilerin verileri baz alınarak, ağ içerisindeki verileri detaylandırılarak fon sağlamak mümkün olabilecektir. (economist.com.tr, 2019)

2.5.4. Akıllı Kontratlar

Finans sektöründe müşteri işlemlerinin hemen hemen hepsinde kontratlar imzalanmakta ve bu kontratların karşılıklı alınmasının ardından işlemler tamamlanabilmektedir. Bu sözleşmeler mevcutta bankalar ya da farklı finans kuruluşlarında yazıcıdan çıktı olarak alınıp, müşterilere verilip, ıslak imzalar atıldıktan sonra işlemlerin tamamlanması ile son bulmaktadır. Bu durum da hem zaman kaybı açısından hem de kâğıt israfı açısından sorun oluşturabilmektedir.

Blok zincir teknolojisi ile arada herhangi bir aracı olmadan direkt sözleşme metni kullanıcı tarafından onaylanıp, ağ içerisinde tutulabilecektir. Bu sözleşme metninin standart bir metin olması düşünülmektedir. Fakat bu durumda da diğer kullanım alanlarında olduğu gibi yasal düzenlemeler yapılması; herhangi bir sorun çıktığı zaman

hakların korunabilmesini kuralların ve kanunların açık şekilde belirtilmesi gerekmektedir.

BÖLÜM 3. BLOK ZİNCİR SİMÜLATORÜ VE UYGULAMA ALANLARI

Tez çalışması kapsamında blok zincir temel yapısını anlatan bir simülatör yapılmış olup, bu simülatör ile zincirin çalışma prensibi, ağ yapısı, veri yapısı ve birbirleriyle olan bağlantıları detaylı şekilde gösterilmiştir. Simülatörün doğruluğunu gösterebilmek için ise birkaç örnek uygulama konulacak ve transactionların ilk adımdan son adıma kadar nasıl bir yol izlediği incelenecektir.

Simülatörün çalışma prensibi için öncelikli olarak blok zincir temelinin öğrenilmesi, fonksiyonlarının çıkarılması, zincirin temel bileşenlerinin öğrenilmesi önem kazanmaktadır. Bu kapsamda simülatör için zincirin detaylarının öğrenilmesi şarttır.

Zincir teknolojisinin temelinde dağınık bir ağ yapısı bulunmaktadır. Bu dağınık yapı ile sisteme kayıtlı olan birçok kullanıcı işlemlerini kaydedip, takip edebilmektedir. Bu işlemler güvenli bir şekilde blok zincirde tutulmaktadır. Böylece diğer kullanıcılar da bu işlem kayıtlarını görebilmektedir. Bu aşamada herhangi merkezi, ortak bir onay yapısı bulunmamaktadır.

Bu teknolojinin temelinde node(düğüm), blok, merkle ağacı, hashing, mutabakat (proof of stake ve proof of work), ağ yapısı gibi belirli kavramlar bulunmaktadır.

Temel fonksiyonlar, transactionlar ve ağ yapısı öğrenildikten sonra simülatör için bu verilerin görselleşmesi ihtiyacı doğmuştur. Görselleştirmeler için kodlama öncesinde örnek ekran tasarımları ve gereksinimleri belirlenmiş; ardından kodlamaya geçilmiştir.

Yapı görselleştirildikten sonra kodlama adımıyla simülatör interaktif hale gelmiş ve ekranlar arası bağlantı olmuştur. Bu bağlantı sayesinde simülatörde hashing adımı, blokların gösterimi, blokların zincir içerisindeki dizilimi, her bir ağ yapısında blokların birbiri arasındaki etkileşimi ve bu etkileşim içerisinde transaction yapısı gösterilmiştir.

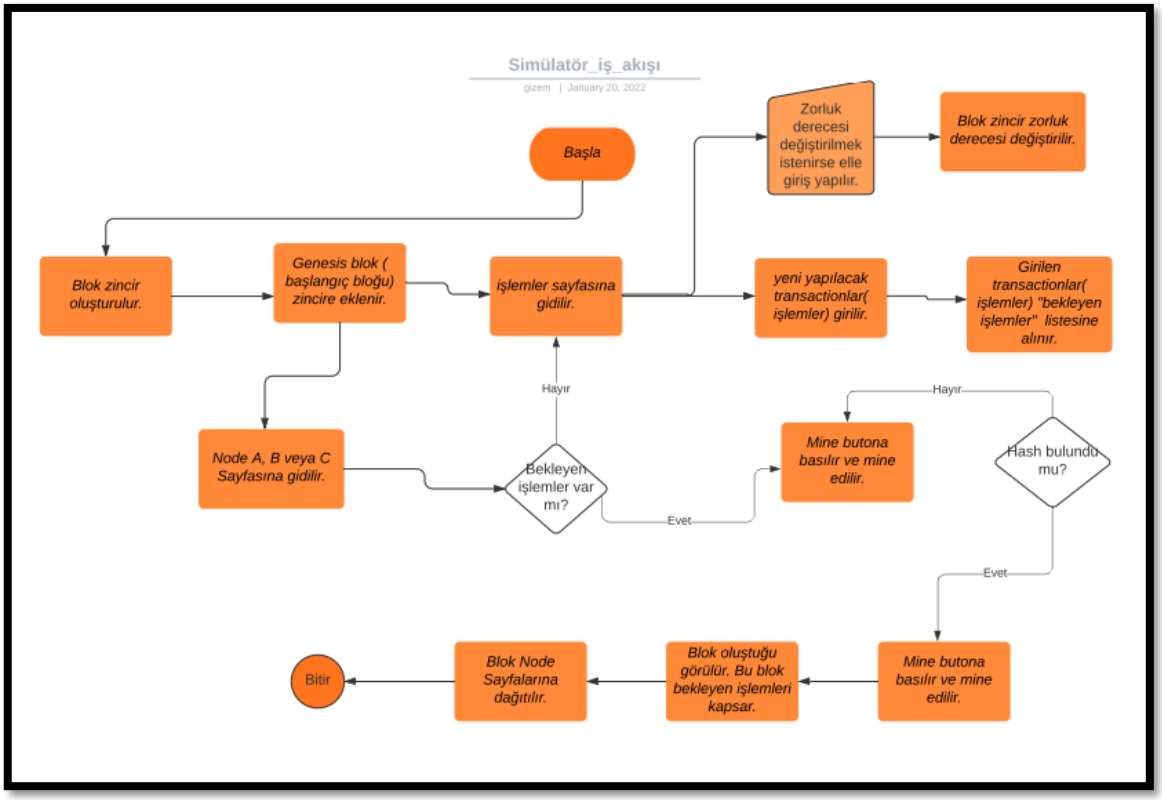
3.1 Simülatör İş Akışı

Bu çalışma ile blok zincir ağ yapısı incelenip, birden fazla kullanıcının aynı ağa bağlanması ile oluşacak zincir ve blok yapısı gözlenmesi ve bunun yapılacak olan bir simülatör ile gösterilmesi hedeflenmiştir.

Simülatör ile blok zincir temel yapısının nelerden oluştuğu, ağ yapısının nasıl olması gerektiği, zincirde bulunan bloklarda, blok içeriklerinin nasıl oluştuğu, transactionların nasıl işlediği, giriş anahtarları oluşturulurken nelerin baz alındığı detayları gözlenmiştir.

Simülatörde yapılan işlemler genel hatlarıyla aşağıdaki gibidir:

- Uygulama çalıştığı anda bir blok zincir yaratılır ve zincirin ilk bloğu (genesis blok) simülatör tarafından direkt zincire eklenir.
- İşlemler sayfasında uygulamada kullanılan zorluk derecesi değiştirilebilir.
- İşlemler sayfasında bloğu oluşturacak transactionlar (işlemler) girilir.
- Node (Düğüm) sayfalarında bekleyen transactionlar (işlemler) alınarak zorluk seviyesine göre blok oluşturması için ’mine’ edilir.
- Transactionlarla beraber zincirde oluşan bloklar tüm node sayfalarında gösterilir. Burada hash değeri, önceki bloğun hash değeri, nonce değeri, blok numarası ve bloğa giren transactionlar gösterilir.
- Bir node’da oluşan blokların, diğer node sayfalarında da aynı şekilde oluştuğu görülür.
- Herhangi bir blok üzerinde hash değeri değiştirilirse zincir yapısı bozulacağı için geçersiz olan bloklar gösterilir.



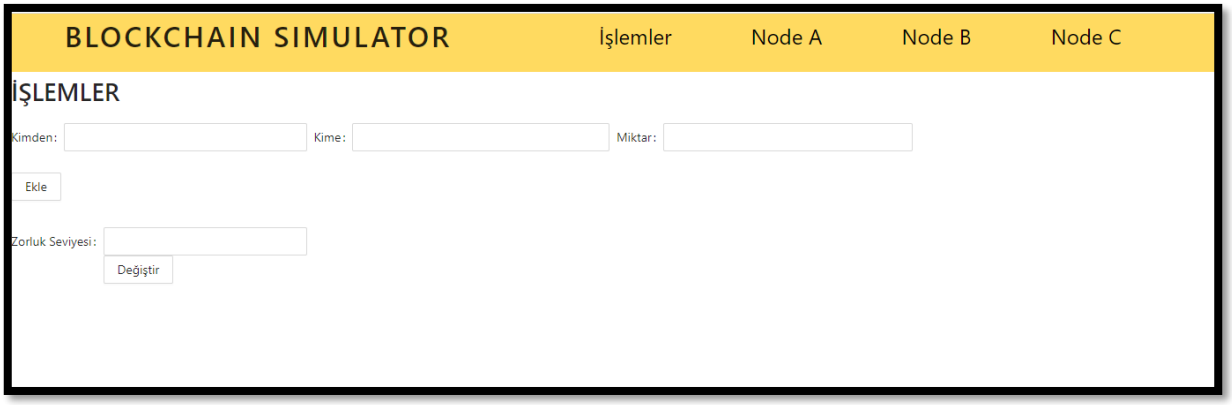
Şekil 5: *Simülatör Çalışma Prensibi İş Akış Şeması*

3.2. Simülatöre Giriş

Simülatöre ilk giriş anında yeni bir blok zincir arka planda oluşturulur. Ekranlarda ise "İşlemler", "Node A", "Node B" ve "Node C" sayfaları görüntülenir.

Burada "İşlemler" sayfasında girilecek olan transactionlar (işlemler) yapılır. "Node A", "Node B" ve "Node C" sayfası blok zincir yapısında dağınık yapıda olan ağlar olarak düşünülmüş olup, her bir node, IP barındıran bir düğüm olarak düşünülmüştür.

"İşlemler" sayfasında ayrıca "zorluk derecesi" alanı vardır. Bu alan ile bekleyen işlemlerden oluşacak hash kodunun başında ne kadar sıfır olacağı bilgisi elle değiştirilebilir olmaktadır.



Şekil 6: *Simülatör Giriş Sayfası*

Simülatör giriş sayfası işlemlerin girileceği, listeye eklenebileceği ve zorluk seviyesini belirtmesi adına önemlidir. Burada işlemleri içeren transfer bilgileri, listeye eklenmesi bu sayfada yapılmaktadır. İşlemler baz alınarak oluşturulacak hash kodunun zorluk seviyesi de yine aynı şekilde işlemler sayfasından yapılabilmekte ve zorluk seviyesi kullanıcının değiştirebileceği şekilde girilebilmektedir.

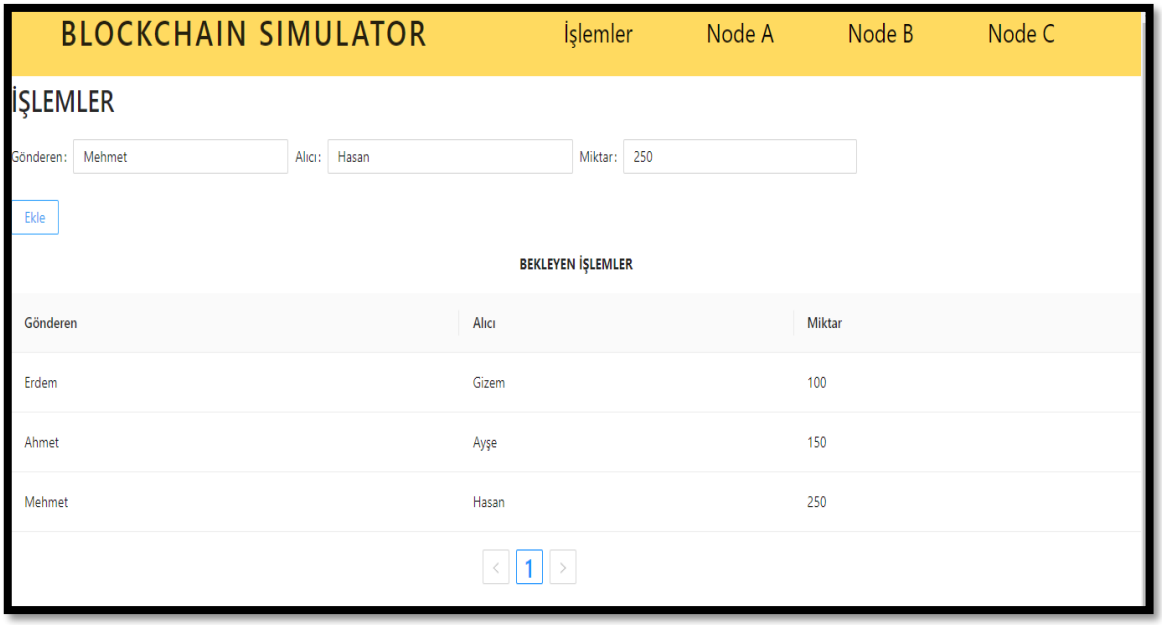
3.3. Simülatör İşlemler Sayfası

Simülatöre girildiğinde ana sayfada "İşlemler" ekranı bulunmaktadır. Bu ekrana girildiğinde işlemlerde kimden kime ne kadarlık transfer olacağı bilgisi girilir; bekleyen işlemlere girilen bu transaction bilgisi eklenir.

Her bir işlem girildikten sonra "bekleyen işlemler" listesine getirilmektedir.

İşlemler sayfasında transactionlar (işlemler) oluşturulurken girilmesi gereken alanlar aşağıdaki gibidir:

- Gönderen: Para transferinin kimin tarafından gönderileceği bilgisidir.
- Alıcı: Para transferinin kimin tarafından alınacağı bilgisidir.
- Miktar: Ne kadarlık bir para transferi yapılacağı bilgisidir.



Şekil 7: *Simülatör İşlemler Sayfası*

Gönderen alanına gönderen kullanıcının ismi yazılır; ardından alıcı alanına transferi alacak kullanıcının adı yazılır. Ardından miktar alanına ne kadarlık bir para transferi yapılmak isteniyorsa o kadarlık tutar yazılır. Alanlara giriş yapıldıktan sonra "ekle" butonuna basılır ve işlemler "bekleyen işlemler" listesine düşmektedir.

Burada istenilen kadar işlem girilebilmektedir.

Yukarıdaki örnek ekran görüntüsünde 3 adet işlem girilmiştir. İşlemler girilirken:

1- Erdem'den Gizem'e 100'lük transfer
2- Ahmet'ten Ayşe'ye 150'lik transfer;
3- Mehmet'ten Hasan'a 250'lik transfer için art arda işlemler girilmiştir.

Bu aşamada girilen bu üç işlem "bekleyen işlemler" alanında gösterilmektedir. Bu işlemler listede olduğu ve henüz mine edilmediği için bu alanda tutulmaktadır ve henüz bir bloğa yazılmamıştır.

3.3.1. Zorluk Seviyesi

Blok zincir yapısında bloklar oluşturulurken bekleyen işlemlerden oluşan hash bilgisinde, hash'in oluşturulması ve bulunması aşamasında zorluk seviyesi değiştirilebilmektedir. "Zorluk seviyesi" bloklarda oluşan hash değerinin başında kaç tane sıfır olması gerektiğini ve bu sıfırlara göre de hash değerinin bulunmasının zorluğunu göstermektedir.

Örneğin; zorluk seviyesi 2 olarak yazıldığında girilen işlemlerden oluşan ve şifreleme yöntemi ile oluşan hash değerininin başında 2 tane sıfır olması beklenmektedir.

Bekleyen işlemlere göre "mine" butonu ile işlemler mine edildiğinde zorluk seviyesinde başında kaç tane sıfır var ise hash değeri o sıfır sayısını bulana kadar devam etmektedir. Bu koşul sağlandıktan sonra yani belirtilen zorluk seviyesine göre hash değeri oluştuktan sonra blok zincire eklenebilmektedir.

Aşağıdaki ekran görüntüsünde kırmızı çerçeve ile belirtilen alanlarda elle istenilen zorluk seviyesi seçilerek "değiştir" butonuna basıldığında zorluk seviyesi belirtilen sayı kadar değişmiş olacak; bekleyen işlemlerden oluşan hash değerinin başında girilen seviye sayısı kadar sıfır oluşmuş olacaktır.



Şekil 8: *Simülatör Zorluk Seviyesi*

Zorluk seviyesi kullanıcı tarafından istenildiği şekliyle değiştirilebilmektedir. Böylece zorluk seviyesi değiştikçe işlemler baz alınarak oluşturulacak hash kodunun

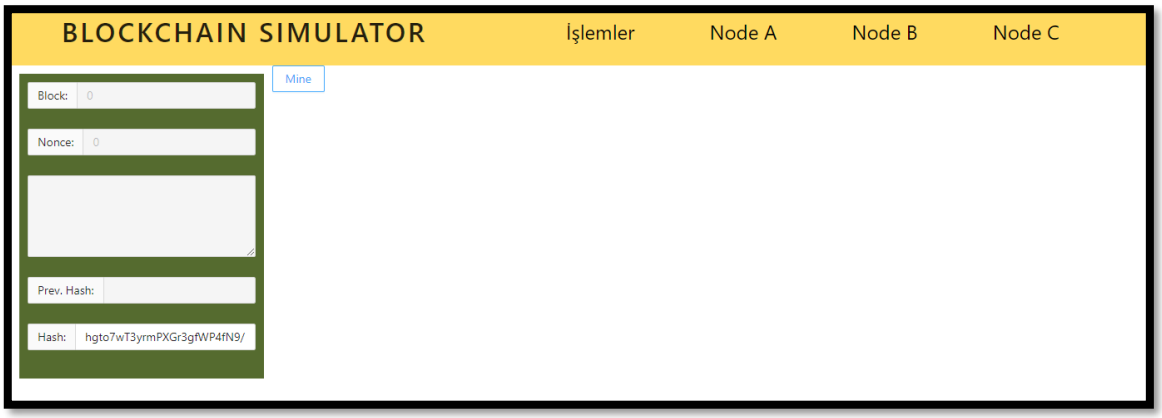
başında kaç tane sıfır olacağı bilgisi de değişecek ve bu da blokların oluşması ve zincire eklenmesi zorlayıcı bir unsur olarak göze çarpabilecektir.

3.4 Simülatörde İlk Bloğun (Genesis Blok) Oluşması

Simülatör ilk açıldığı zaman arka planda bir blok zincir oluşturulur. Oluşturulan blok zincirde ilk olarak bir "genesis" blok yaratılır. Burada "genesis" blok, blok zincirdeki ilk yaratılan bloktur. Zincire yeni bloklar eklenmesi için "genesis" blokun oluşması şarttır. Bu bloğa bir nevi "default blok" da denebilmektedir. Bu blok içerisinde herhangi bir işlem bilgisi bulunmamaktadır.

Yaratılan hash kodu işlem bilgisi içermeden uygulamanın SHA 256 algoritması kullanılarak oluşturduğu bir hash kodudur. Bu bloktaki hash kodu, işlem bilgisi barındırmadığından ve ilk blok olduğundan zorluk seviyesi kriteri bu blok için aranmamaktadır.

Oluşan ilk blokta blok numarası sıfır olarak atanmaktadır. Bu blokta içerisinde işlem barındırmadığından ve oluşan hash değerinde zorluk seviyesi aranmadığından nonce değeri 0 olarak atanmaktadır. İlk blok olduğu için "previous hash" yani bir önceki blokta bulunan hash bilgisi değeri de bulunmamaktadır çünkü bu blok zincirdeki ilk blok olduğundan ve öncesinde başka blok barındırmadığından bir önceki bloğun hash değeri bulunmamaktadır. Hash alanında ise içerisinde işlem barındırmayan, SHA 256 algoritması ile oluşmuş 32 karakterlik bir değer ortaya çıkmaktadır.



Şekil 9: *Simülatör Genesis Blok*

Simülatörde bloklar oluşurken oluşan hash oluşturulduğunda, hashin oluşması için SHA256 algoritması kullanılmaktadır. SHA yani Secure Hash Algorithm özet bir değer üretmektedir. Bu algoritmalar ile büyük verilerden daha küçük özet bilgiler çıkarılabilmektedir ve bu durum normalde kullanılan dijital bir parmak izi olarak düşünülebilmektedir. Hash değeri çözülmesi zor, tahmin edilmesi güç ve işlemlere özel bir koddur.

3.5. Simülatörde Blokların Oluşması ve Zincire Eklenmesi

Simülatör açıldıktan sonra uygulama tarafından bir blok zincir oluşturulur. Oluşturulan blok zincire ilk blok (genesis blok) eklenir. Aynı zamanda "işlemler" sayfasında gönderen kullanıcıdan alıcıya ne kadar miktarlık transfer olacağı bilgisi de girilir. Burada istenilen kadar işlem girilebilmektedir. Girilen işlemler ekle butonu ile "bekleyen işlemler" sayfasına yeni bir satır olarak eklenir.

Girilen işlemlerin bloklara eklenebilmesi ve bu blokların da blok zincire dahil olabilmesi için işlemlerin "mine" butonu ile aktif hale getirilmesi gerekmektedir. "mine" butonu ile girilen işlemler için bir hash kodu oluşturulur. Bu hash kodu "işlemler" sayfasında girilen zorluk seviyesine göre belirlenir. Burada zorluk seviyesi 2 olarak belirlendiğinde, işlemler baz alınarak oluşturulacak hash kodunun ilk iki hanesinin sıfır ile başlaması beklenir.

"mine" butonu işlemlerin bloklara dahil olmasını ve bloğun da zincire eklenmesini sağlar. Aynı zamanda oluşturulan bloğun tüm node (düğüm) sayfalarında da görünmesine olanak tanır. Çünkü işlemlerden oluşan ve "mine" edilen bloğun artık onaylandığı varsayılır ve bu onaylı bloklar tüm node'lara dağıtılır.

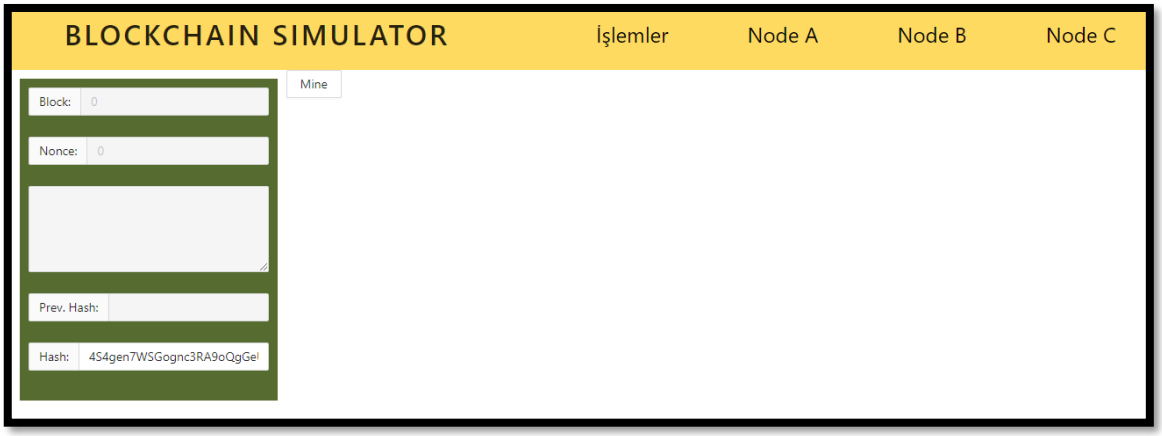
Hash kodunun zorluk seviyesine göre oluşmasını beklerken blok içerisinde "nonce "değeri de "mine" butonu çalıştırılarak görünür. "nonce" değeri belirtilen kriterlere ve girilen işlemlere göre oluşan hash kodunu döngüde kaçıncı sırada bulduğunu göstermektedir ve blok için tek ve özel bir değerdir.

İşlemler sayfasında girilen transactionlar (işlemler) "bekleyen işlemler" statüsünden blok içerisine eklenebilmesi için "mine" edilir. Bu durum "mine" butonu ile sağlanır. "mine" butonu "Node A" sayfasında bulunmaktadır. "Node A" sayfası IP

barındıran bir bilgisayar olarak düşünülmektedir. “Node A” sayfasında blok oluşturulursa simülatörde var olan “Node B” ve “Node C” sayfalarında da görünür. Burada “Node B” ve “Node C” sayfalarının da IP barındıran birer aygıt olduğu düşünülmekte ve görselleştirilmektedir.

Blok zincirin genel yapısı gereği dağıtık bir ağ yapısı olduğu düşünüldüğünde Node A, B ve C sayfalarının her birinin birer server gibi olduğu varsayılıp, blok zincirdeki bloklar bu nodelarda (düğümlerde) tutulabilmektedir. Yani Node A sayfasında oluşan blokların Node B ve C sayfalarında da görünür olması blok zincirin dağınık ağ yapısının görselleştirilmesin de etkisidir.

Simülatörün aşağıdaki ekran görüntüsünde işlemler sayfasından oluşan transactionlar için bir blok yaratılması için “mine” butonu gösterilmiştir. Burada işlemler sayfasında talep edilen kadar transaction girildikten sonra Node A sayfasına gidilir. Burada ilk blok (genesis blok) ilk ekran açıldığında görülmektedir. Ardından bu ekranda bulunan “mine” butonuna basılır.



Şekil 10: *“Mine” butonu görseli*

“Mine” butonuna basıldıktan sonra “işlemler” sayfasında girilen transactionlar için yeni bir blok oluşturulması sağlanır. Yeni oluşan blok ilk blok (genesis blok) un yanına eklenmektedir. Oluşan yeni blok içerisinde blok numarası bulunmaktadır. Zincire genesis bloktan sonra eklenen ilk blok olduğu için blok numarası 1 olarak atanmıştır. Blokların ortasında bulunan alanda “bekleyen işlemler” sayfasında bulunan işlemler listelenmektedir.

Liste gösterimi aşağıdaki gibidir:

[{"fromAddress":"Erdem
","toAddress":"Gizem","amount":100},{"fromAddress":"Ahmet","toAddress":"Ayşe
","amount":150},{"fromAddress":"Mehmet","toAddress":"Hasan
","amount":250},{"fromAddress":"blockchain","toAddress":"firstClient","amount":10}]

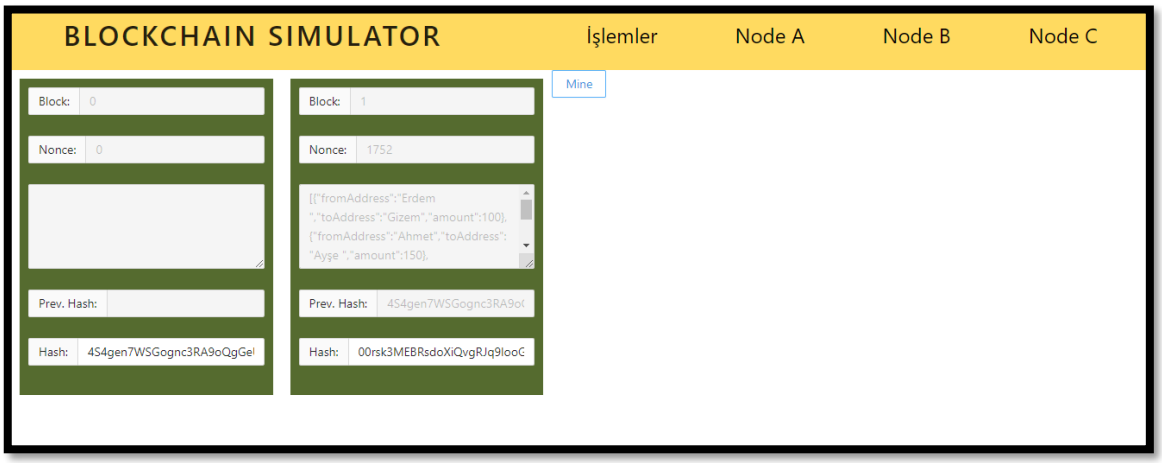
Liste gösterimde girilen her bir transaction “fromAddress … toAdress.. Amount “şeklinde gösterilmektedir. Ne kadar transaction girildiyse o kadar satır burada gösterilmektedir.

Tüm girilen ve gösterilen işlemlerin yanı sıra bir de bitcoin yapısında da olan ödül mekanizması işlemi gösterilmektedir. Mevcutta bitcoin madenciliğinde kullanıcılar işlemleri gerçek anlamda transfer edebilmek ve bitcoin kazıyabilmek için “mine” ettiklerinde ve bir blok oluşturduklarında bitcoin altyapısı tarafından “mine” edip bloğu oluşturulan kullanıcıya bitcoin ödül olarak verilir. Çünkü bu “mine” işleminde bilgisayarın işlem gücü kullanıldığından ve efor sarf edildiğinden bu çabanın bir karşılığı olarak ödül mekanizması bulunmaktadır. Simülatör aşamasında da bu ödül mekanizmasını “mine“butonuna basıldığında ve yeni bir blok oluşturulduğunda bloktaki mevcut transactionların altında yeni bir satır olarak görünmektedir. Buradaki gösterimde de “fromAddress":"blockchain","toAddress":"firstClient","amount":10” şeklinde gösterilmektedir. Amount simülatörde 10 olarak gelmektedir.

Yeni oluşturulan blokta “Previous Hash” alanı bulunmaktadır. Bu alan bir önceki blokta bulunan hash bilgisini göstermektedir. Bloklar arası iletişim ve bağlantı bu hash kodları ile olmaktadır. Aşağıdaki örnek ekran görüntüsünde “mine” butonu ile oluşturulan 1 numaralı blokta bulunan”Prev.Hash” alanı ilk bloğun (genesis blok) hash bilgisidir. Blok zincir uygulamasında güvenlik kontrolleri bir önceki bloğun hash bilgisinin, yeni yaratılan blokta da tutulması ile de sağlanır. Böylece zincire veya bloğa dışardan müdahale edilmek istendiğinde sıralı hash bilgisi bozulacağından güvenlik de bozulmuş olur. Bir önceki blok ile yeni blok arasındaki hash bağlantısı ile zincirdeki bloklar birbirine bağlanmış olur ve dışarıdan müdahale de zorlaşmış olmaktadır.

Hash değeri de girilen işlemlere göre uygulama tarafından oluşturulmuş ve SHA 256 algoritması ile ortaya çıkmış bir değerdir. Bu değer "işlemler" sayfasında seçilen zorluk derecesine göre oluşmaktadır. Simülatörde şu an zorluk derecesi 2 olarak seçili gelmektedir. Hash değeri işlemler sayfasında kaç tane işlem girildiyse onları baz alıp, ardından seçilen zorluk derecesine göre başında kaç tane sıfır olarak belirlendiyse o kadar olacak şekilde gelmektedir. Girilen işlemlerin yanısıra ödül mekanizması için oluşan transaction (işlem) da hash kodunu oluşturmak için algoritmaya dahil edilir. Uygulamada zorluk derecesi 2 olarak ayarlandığından işlemler ile oluşan hash bilgisi başında 2 adet sıfır olarak oluşmuştur. Bu hash kodu bloğa özgü bir kod olmuştur.

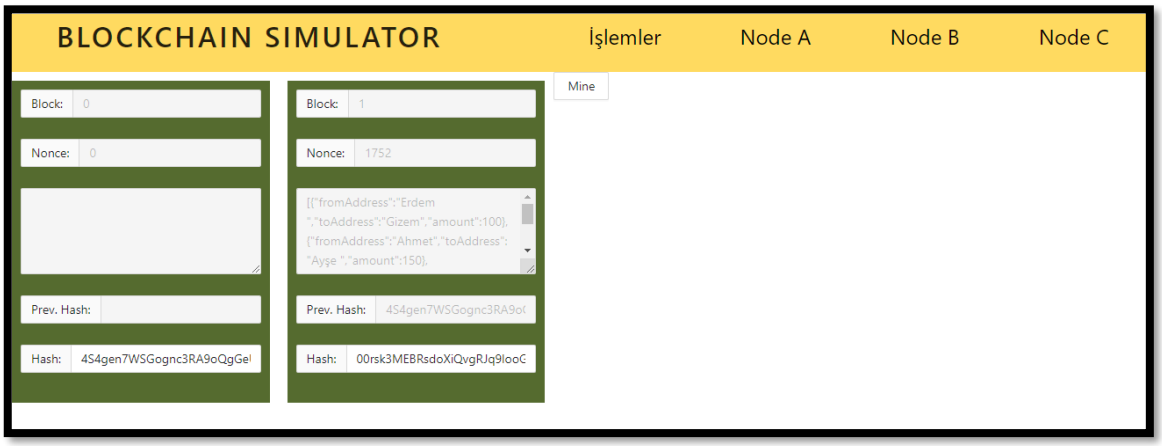
"Nonce" değeri, girilen işlemler ve zorluk seviyesine göre oluşması beklenen hash kodu "mine" edilirken bir döngü içerisinde kaçıncı seferde bulunduğunu gösteren, o bloğa özgü bir değerdir.



Şekil 11: *Blok oluşturulması*

1 numaralı blok oluştuğunda yani belirtilen kriterlere göre hash kodu oluşup, zincire eklendiğinde oluşan blok rengi yeşil olarak ilk bloğun (genesis blok) görünmektedir.

Oluşan 1 numaralı bloğun diğer nodelerda da görünür olması beklenmektedir. Bunun sebebi de Node A, Node B ve Node C sayfalarının simülatörde zincirde birer düğüm olarak düşünülmesi ve 1 numaralı blok da başarılı şekilde "mine" edilip, hash kodu ve nonce değeri oluşturduğu için onaylı olarak Node B ve Node C düğümlerine de yansıması olarak düşünülmektedir.

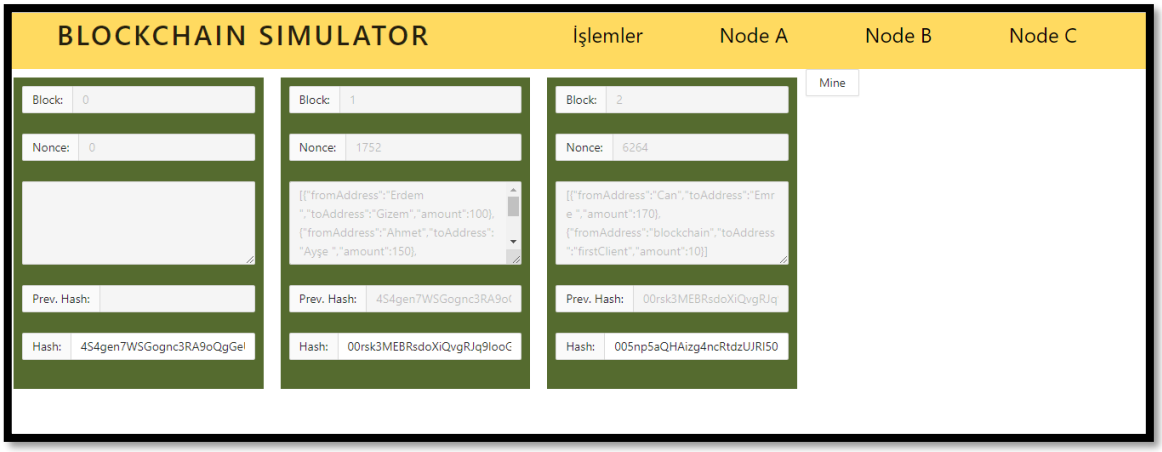


Şekil 12: *Oluşan Bloğun diğer düğümlerde gösterimi*

1 numaralı bloğun oluşması ve diğer düğümlere de gösterilmesinin ardından "işlemler" sayfasına yeniden girilip, yeni transaction (işlem) kayıtları yaratılabilmektedir.

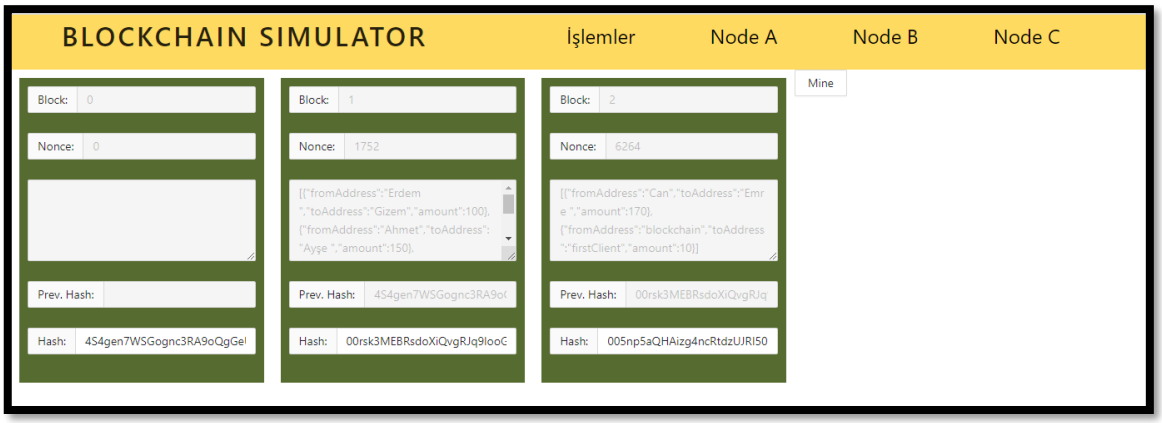
İşlemler sayfasında girilen işlemler de yeniden "bekleyen işlemler" adı altında toplanmaktadır. 1 numaralı bloğun oluşturulmasının ardından yeni girilen işlemler de "bekleyen işlemler" adımından transferin gerçekleşebilmesi için yeniden Node A sayfasında "mine" edilmesi ve yeni bir blok yaratılması gerekmektedir. Yaratılan bu bloğun da zincire eklenmesi beklenmektedir.

Aşağıdaki ekran görüntüsünde girilen işlemler baz alınarak yeni bir blok oluşturulmuştur. Oluşan bloğun numarası 2'dir ve bu blok sadece yeni girilen işlemleri ve ödül işlemini barındırmaktadır. Buradaki "prev. Hash" değeri, bir önceki 1 numaralı bloğun hash değeri bilgisidir. Her blokta, bir önceki bloğun hash değeri bilgisi de bulunmaktadır. Aynı şekilde yeni girilen işlem ve ödül transactionı (işlemini) de baz alarak zorluk seviyesine göre yeni bir hash kodu oluşturulmuştur. Bu hash kodu bulunurken oluşan "nonce" değeri 1 numaralı blokta bulunan nonce değerinden farklıdır çünkü bu nonce değeri her blok için farklıdır, tekil bir sayıdır. 2 numaralı bloktaki "nonce" değeri de girilen işlemler ve ödül mekanizmasına göre oluşan değerin döngüde kaçıncı denemede bulunduğunu gösterir.



Şekil 13: *Zincire yeni blok eklenmesi*

Oluşan 2 numaralı bloğun diğer nodelerda da görünür olması beklenmektedir.



Şekil 14: *Eklenen yeni bloğun diğer düğümlerde gösterimi*

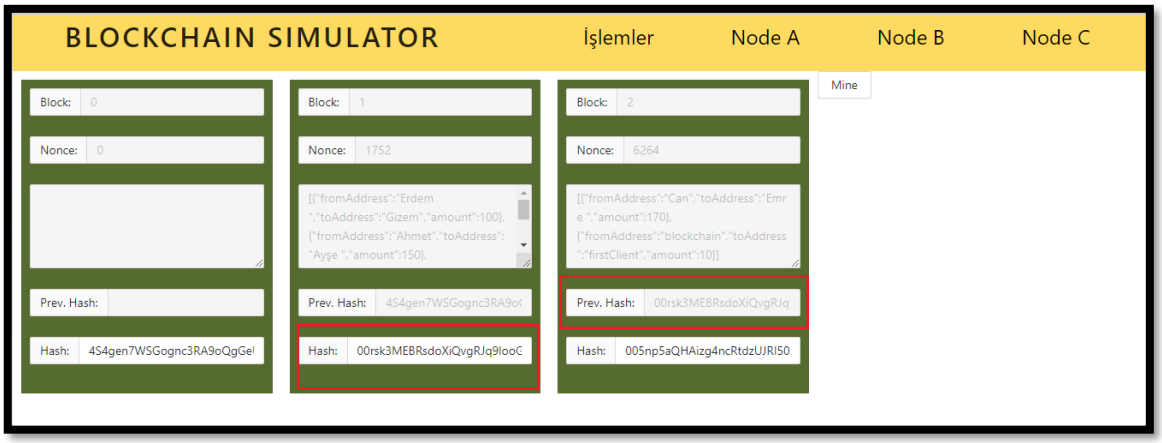
Simülatörde aynı döngü istenilen kadar yapılarak yani 2 numaralı blok oluştuktan sonra da işlemler sayfasında yeni işlemler girilip ardından Node A sayfasında bulunan "mine" butonu ile işlemler mine edilip, yeni blok oluşturduğunda yine zincire yeni bir blok numarası, işlem detayları, hash kodu ve nonce değeri ile eklenebilecektir. Prev.Hash alanı da yine bir önceki bloğun hash değerini alarak ilerleyebilecektir.

3.6. Simülatörde Bloğun Hash Koduna Müdahale Edilmesi

Blok zincire işlemler baz alınarak ve ardından mine edilerek oluşturulan bloklar eklenir. Bloklar eklenirken güvenlik ve aralarındaki ilişki hash kodları ile olmaktadır. Her bir blok, bir önceki bloğun hash kodunu kendi içerisinde tutmakta ve birbirleri arasında ilişki bu hash kodları ile oluşmaktadır.

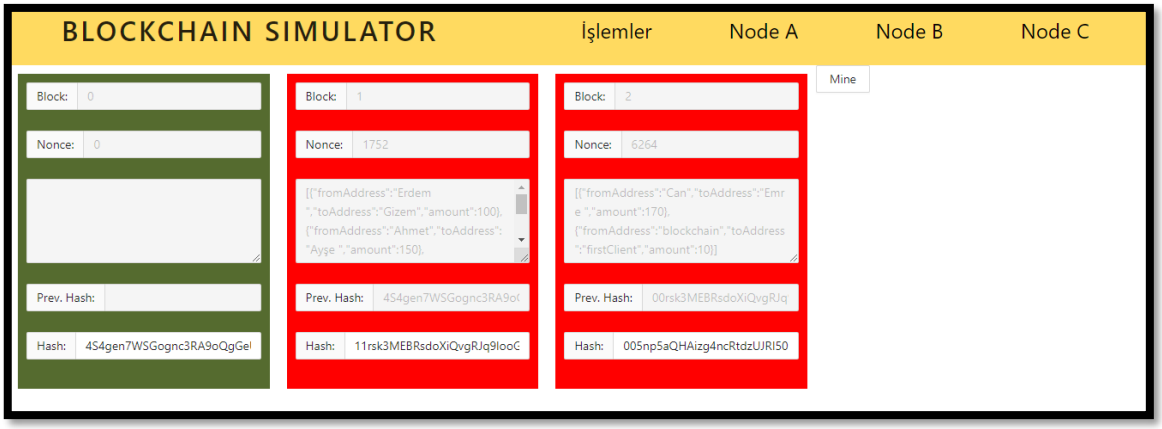
Eğer 1 ve 2 numaralı bloklar oluştuktan sonra 1 numaralı bloğun hash koduna elle müdahale durumu olursa 1 numaralı blok ve 2 numaralı blok bozulmuş olacak ve birbirleri arasındaki bağlantı kopmuş olacaktır.

Aşağıdaki ekran görüntüsünde 1 ve 2 numaralı bloklar mine edilerek oluşturulmuş ve 1 numaralı bloğun hash kodu, 2 numaralı blokta "prev.hash" alanına tutulmuştur.



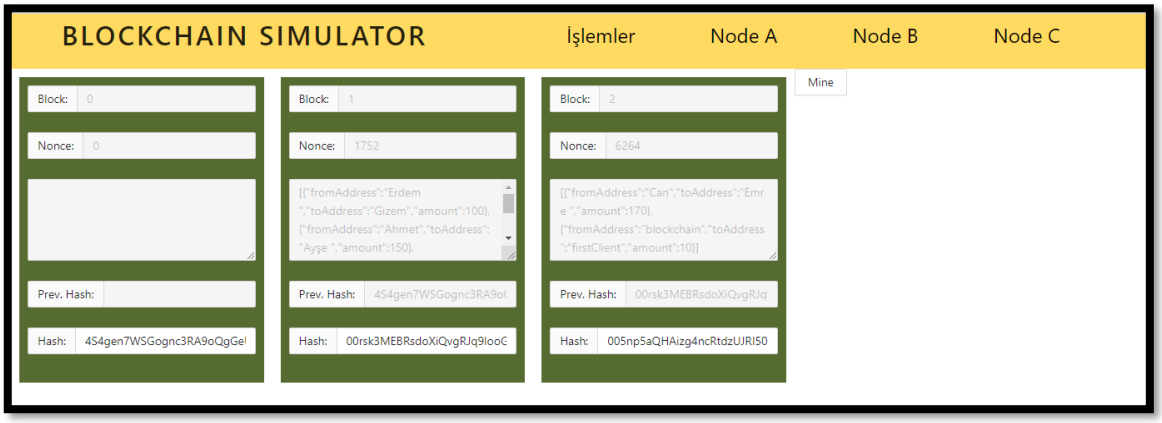
Şekil 15: *Bloklardaki hash kodu ilişkisi gösterimi*

Simülatörde hash koduna elle müdahale olduğunda ilgili bloğun rengi kırmızı olmakta ve bu da bloğun bozulduğu anlamına gelmektedir. İlgili blok bozulduktan ve kırmızı ile işaretlendikten sonra hash kodu diğer blokları da etkilediğinden kendisi ve kendisinden sonra gelen tüm blokların rengi kırmızıya dönmektedir.



Şekil 16: *Bloktaki hash koduna elle müdahale edilmesi*

Simülatörde Node A içerisinde bloklar elle müdahale ile bozulduğunda sadece o node (düğüm) için zincir bozulmuş olur. Diğer nodelar (düğümler) için zincir bozulmamış olur.



Şekil 17: *Node A'daki elle müdahalenin diğer düğümleri etkilememesi*

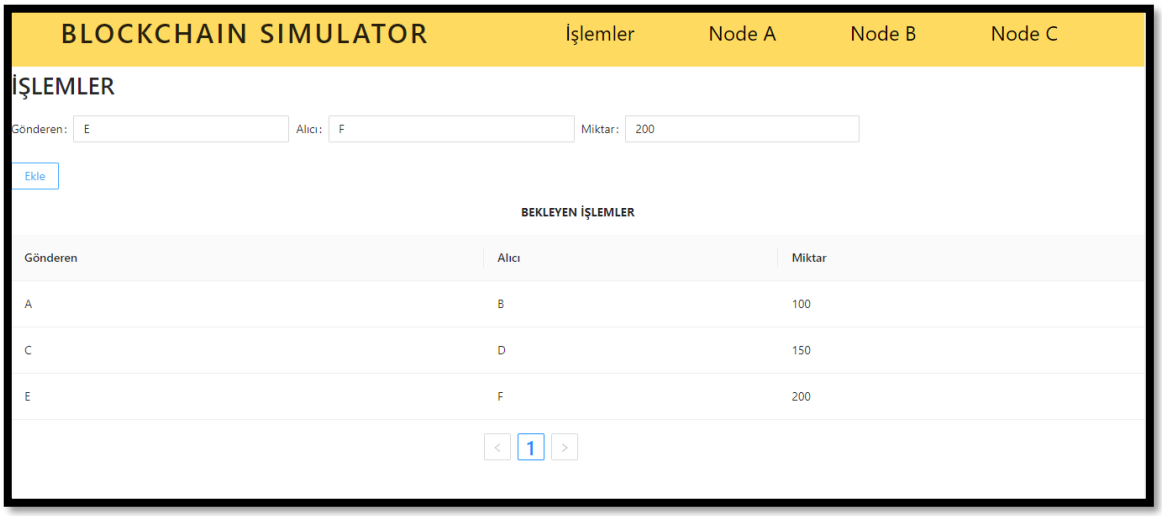
Bu durum blok zincir yapısında da bu şekildedir. Blok zincirde de bir düğümde var olan blok zincire ait bloklardan biri dışarıdan bir müdahale ile bozulduğunda kendisi ve ondan sonra gelen tüm bloklar da bozulmuş olur. Böylece birbirleri arasındaki bağlantı kopmuş olur. Fakat blok zincir altyapısında dışarıdan müdahale kolay bir işlem değildir. Bir şekilde güvenlik önlemleri aşılsa bile bir node üzerinde bloklara elle müdahale olduğunda blok zincir yapısı bozulduğu için elle müdahale edilen blokların tekrar doğrulanarak diğer nodelara dağıtılması diğer nodelarda da kısa süre içerisinde çok sayıda işlemler yapıldığı için zor bir ihtimaldir.

3.7. Simülatör Uygulama Örnekleri

Simülatörün çalışma mantığını göstermek ve görselleştirmek için çeşitli örnekler yapılmıştır.

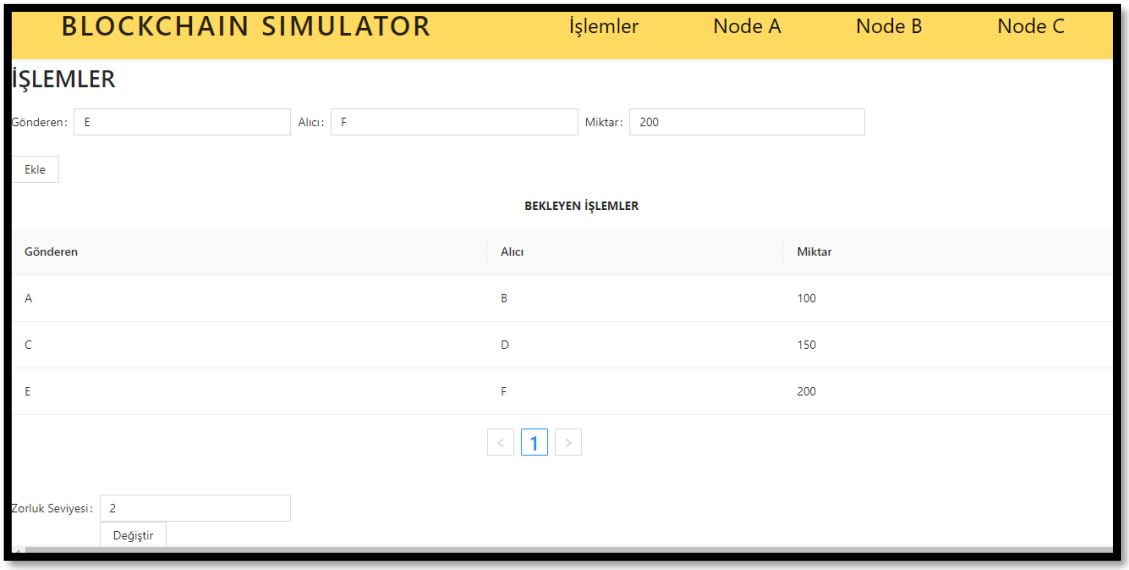
Örnek 1:

- Simülatörde "işlemler" sayfasına gidilir.
- İşlemler sayfasında Gönderen, Alıcı ve miktar alanları girilip ekle butonuna basılır.
    - Gönderen: A, Alıcı:B, Miktar: 100 olarak seçilir ve ekle butonuna basılır.
    - Gönderen: C, Alıcı:D, Miktar: 150 olarak seçilir ve ekle butonuna basılır.
    - Gönderen: E, Alıcı:F, Miktar: 200 olarak seçilir ve ekle butonuna basılır.



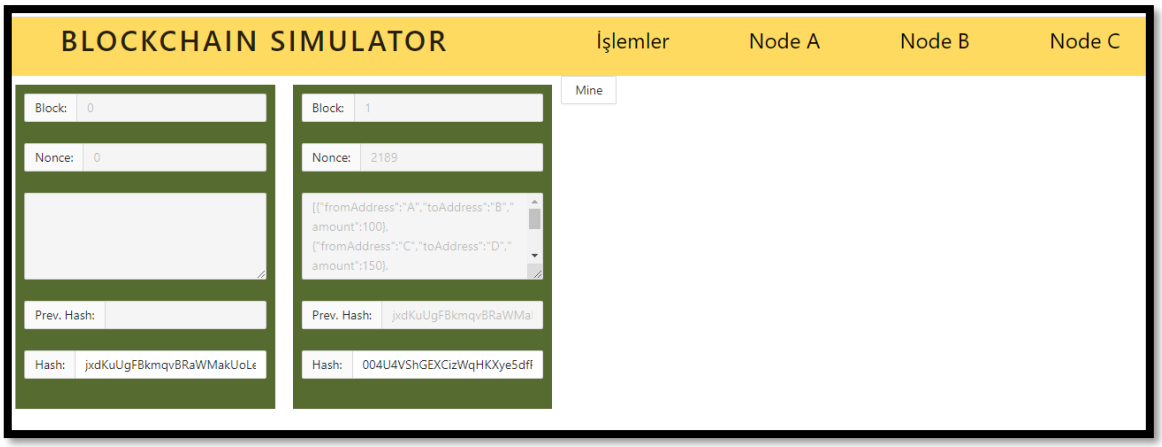
Şekil 18: *Örnek 1 işlem sayfası*

- Girilen 3 işlem "Bekleyen İşlemler" olarak ekranda görünür.
- "İşlemler" sayfasında zorluk seviyesi alanına 2 yazılır ve "değiştir" butonu ile işlemlerden oluşacak hash kodunun başında zorluk seviyesi 2 seçilerek iki tane sıfır oluşması talep edilir.



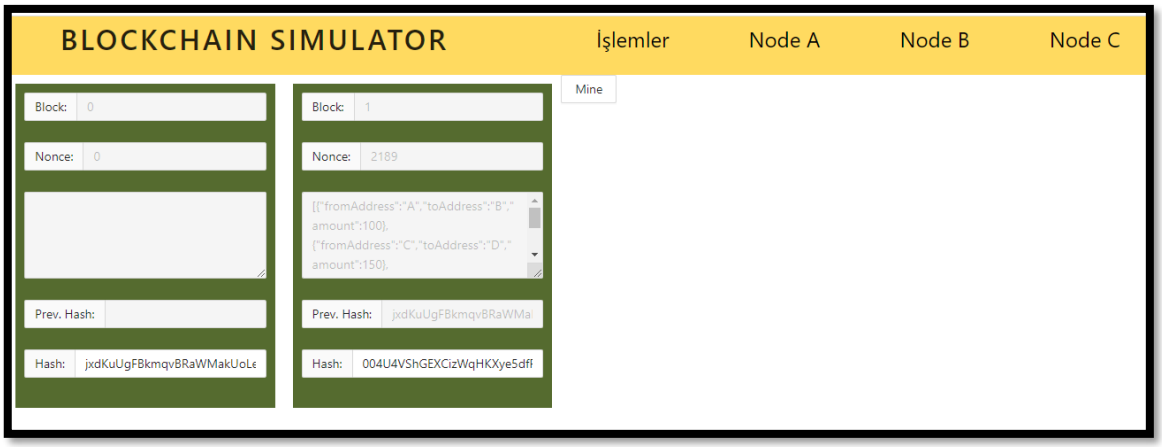
Şekil 19: *Örnek zorluk seviyesi alanı*

- "Node A" sayfasına gidilir ve ilk blok (genesis blok) görülür. İlk blok hash kodunun jxdKuUgFBkmqvBRaWMakUoLeLKpCD6U9 olarak oluştuğu görülür.
- "Node A" sayfasında "mine" butonuna tıklanarak işlemler sayfasında oluşan 3 işlemin bloğun içine dahil edilmesi sağlanır. İşlemlerin yanı sıra ödül işleminin de görüntülenmesi sağlanır.
    - [{"fromAddress":"A","toAddress":"B","amount":100},{"fromAddress":"C","toAddress":"D","amount":150},{"fromAddress":"E","toAddress":"F","amount":200},{"fromAddress":"blockchain","toAddress":"firstClient","amount":10}]
- Blok numarası yeni yaratıldığı için 1 olarak görünür.
- Hash kodu 004U4VShGEXCizWqHKXye5dfPuAGL95M olarak oluştuğu görülür.
- Yeni blokta "prev.hash" alanının jxdKuUgFBkmqvBRaWMakUoLeLKpCDU9 olarak ilk bloktaki hash kodu olduğu görülür.
- Nonce değerinin hash kodunun döngüde bulunma sayısı olarak 2189 olarak oluştuğu görülür.



Şekil 20: *Örnek 1 blok oluşturulması*

- Girilen blok bilgisinin diğer düğümlerde de (Node B ve Node C'de) aynı şekilde olduğu görülür.



Şekil 21: *Örnek blokların diğer düğümlerde gösterilmesi*

Örnek 2:

- Örnek 1'de oluşan blok üzerine yeni blok eklenmesi için simülatörde "işlemler" sayfasına gidilir.
- İşlemler sayfasında Gönderen, Alıcı ve miktar alanları girilip ekle butonuna basılır.

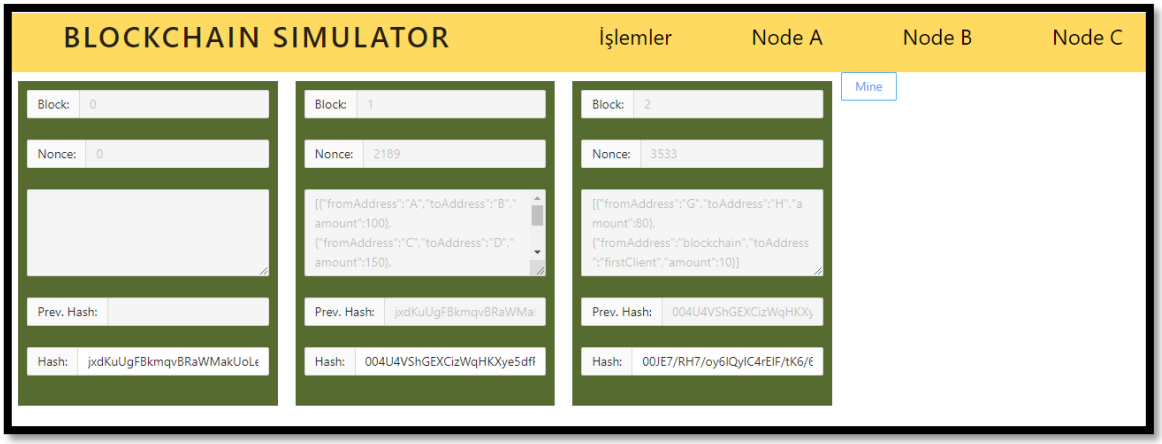
- Gönderen: G, Alıcı: H, Miktar: 80 olarak seçilir ve ekle butonuna basılır.



Şekil 22: *Örnek 2 işlem sayfası*

- Girilen işlem "Bekleyen İşlemler" olarak ekranda görünür.
- "Node A" sayfasında "mine" butonuna tıklanarak işlemler sayfasında oluşan 1 işlemin bloğun içine dahil edilmesi sağlanır. İşlemlerin yanı sıra ödül işleminin de görüntülenmesi sağlanır.
    - [{"fromAddress":"G","toAddress":"H","amount":80},{"fromAddress":"blockchain","toAddress":"firstClient","amount":10}]

- Blok numarası 2 olarak görünür.
    - Hash kodu 00JE7/RH7/oy6lQylC4rElF/tK6/6HY+ olarak oluştuğu görülür.
    - Yeni blokta "prev.hash" alanının 004U4VShGEXCizWqHKXye5dfPuAGL95M olarak ilk bloktaki hash kodu olduğu görülür.
    - Nonce değerinin hash kodunun döngüde bulunma sayısı olarak 3533 olarak oluştuğu görülür.

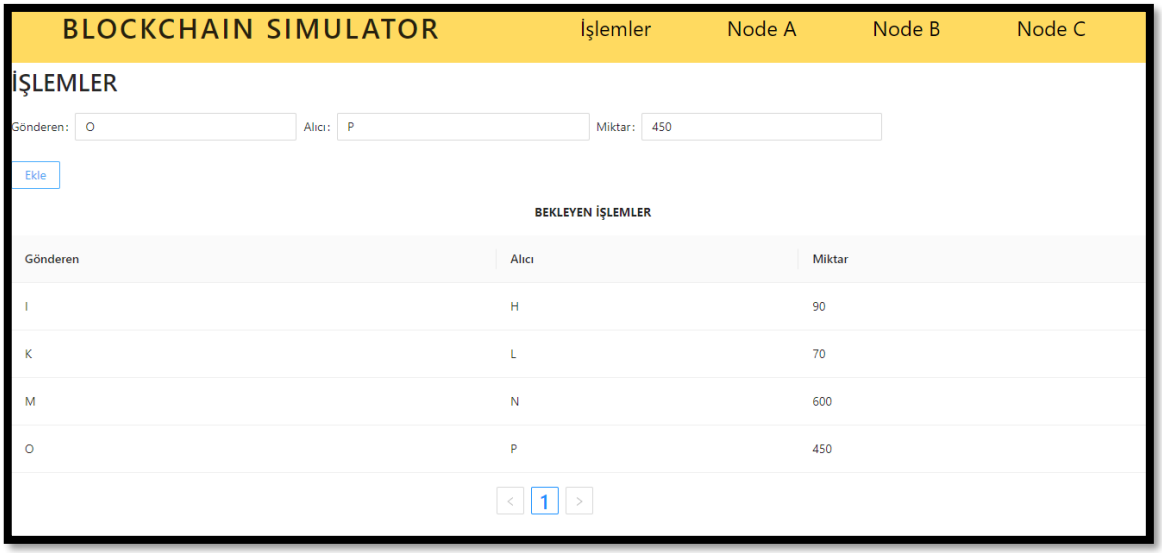


Şekil 23: *Örnek 2 blok oluşturulması*

- Girilen blok bilgisinin diğer düğümlerde de (Node B ve Node C'de) aynı şekilde olduğu görülür.

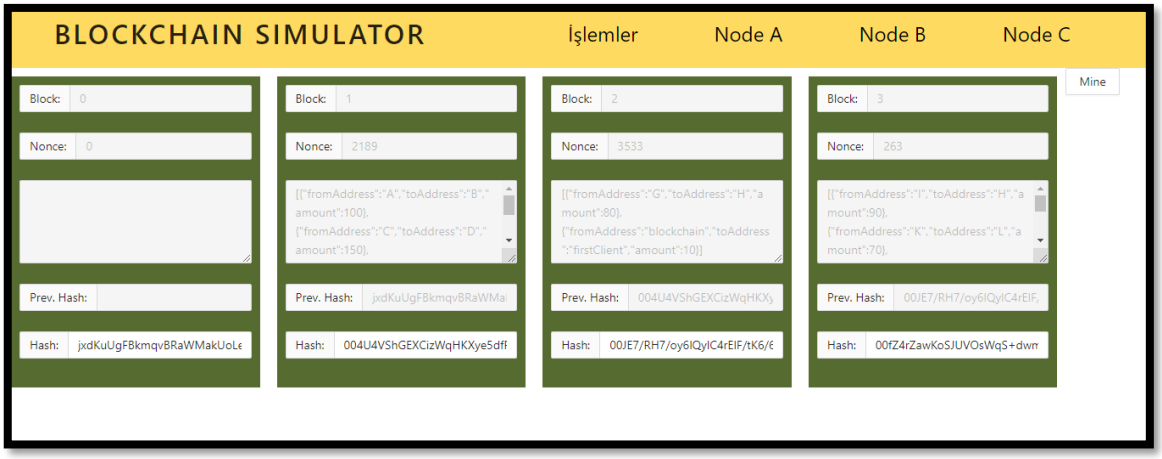
Örnek 3:

- Örnek 2'de oluşan blok üzerine yeni blok eklenmesi için simülatörde "işlemler" sayfasına gidilir.
- İşlemler sayfasında Gönderen, Alıcı ve miktar alanları girilip ekle butonuna basılır.
    - Gönderen: I, Alıcı: J, Miktar: 90 olarak seçilir ve ekle butonuna basılır.
    - Gönderen: K, Alıcı: L, Miktar: 70 olarak seçilir ve ekle butonuna basılır.
    - Gönderen: M, Alıcı: N, Miktar: 600 olarak seçilir ve ekle butonuna basılır.
    - Gönderen: O, Alıcı: P, Miktar: 450 olarak seçilir ve ekle butonuna basılır.



Şekil 24: *Örnek 3 yeni işlem sayfası*

- Girilen işlem "Bekleyen İşlemler" olarak ekranda görünür.
- "Node A" sayfasında "mine" butonuna tıklanarak işlemler sayfasında oluşan 4 işlemin bloğun içine dahil edilmesi sağlanır. İşlemlerin yanı sıra ödül işleminin de görüntülenmesi sağlanır.
    - [{"fromAddress":"I","toAddress":"H","amount":90},{"fromAddress":"K","toAddress":"L","amount":70},{"fromAddress":"M","toAddress":"N","amount":600},{"fromAddress":"O","toAddress":"P","amount":450},{"fromAddress":"blockchain","toAddress":"firstClient","amount":10}]
- Blok numarası 3 olarak görünür.
- Hash kodu 00fZ4rZawKoSJUVOsWqS+dwmFhMwYfsg olarak oluştuğu görülür.
- Yeni blokta "prev.hash" alanının 00JE7/RH7/oy6lQylC4rElF/tK6/6HY+ olarak ilk bloktaki hash kodu olduğu görülür.
- Nonce değerinin hash kodunun döngüde bulunma sayısı olarak 263 olarak oluştuğu görülür.

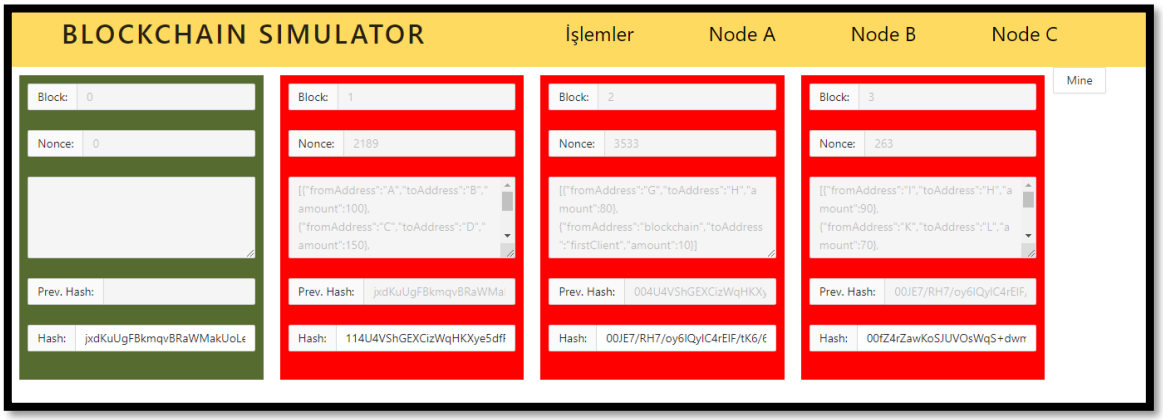


Şekil 25: *Örnek 3 blok oluşturulması*

- Girilen blok bilgisinin diğer düğümlerde de (Node B ve Node C'de) aynı şekilde olduğu görülür.

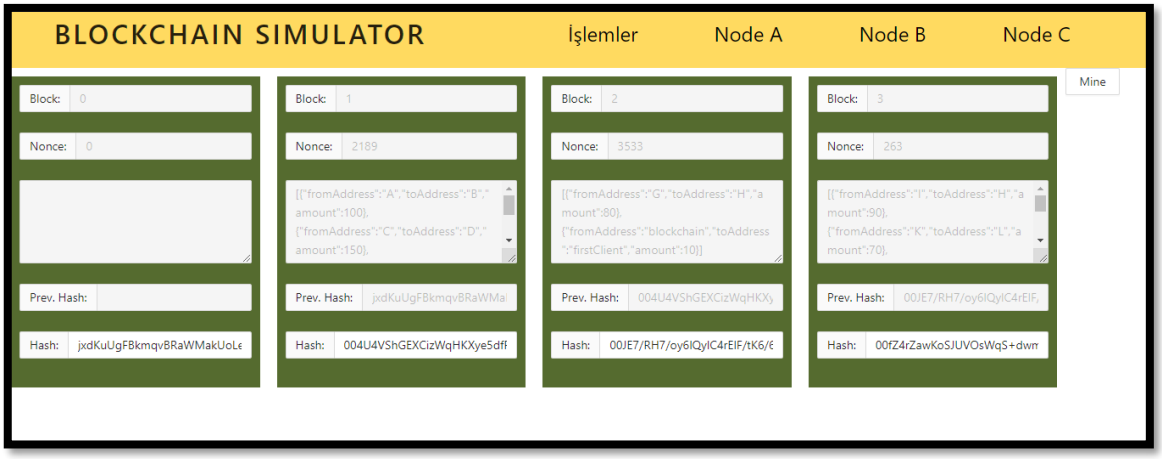
Örnek 4:

- Örnek 3'de oluşan işlemlerle beraber toplam ilk blok hariç 3 blok yaratılmıştır.
- Blok 1 içerisinde bulunan 004U4VShGEXCizWqHKXye5dfPuAGL95M hash kodunun ilk iki hanesindeki 00 değeri elle 11 olarak değiştirilir.
- Elle hash değeri değiştiğinde hash kodları bozulduğu için değişen blok ve sonrasında gelen 2 ve 3 numaralı blokların da etkilendiği ve rengi değiştiği görülür.



Şekil 26: *Örnek 4 blokta hash değerinin bozulması*

- Girilen blok bilgisinin diğer düğümlerde de (Node B ve Node C'de) aynı şekilde yeşil hali olduğu görülür.



Şekil 27: *Örnek 4'te blokta hash değerinin diğer düğümleri etkilememesi*

BÖLÜM 4. SONUÇ

Özet

Blok zincir ile ilgili yapılan araştırmalarda bu teknolojinin güvenilir, az masraflı ve hızlı olduğu görülmüştür. Geleneksel yapıda olan işlemlerde eski yöntem baz alınarak gidilmesindense bu teknoloji ile gitmenin faydalı olabileceği yapılan literatür araştırmaları kapsamında öngörülmektedir. Fakat bu teknoloji henüz çok yeni olduğu ve çok fazla kullanılmadığı için henüz çeşitli kanun ve kurallar açısından yetersiz olabilmektedir. Aynı zamanda tüm dünyada da bu teknolojinin çok bilinmemesinden kaynaklı olarak kullanıcılar arasında bir önyargı olabilmektedir.

Yapılan bu tez çalışması ile bu teknolojinin temel yapı taşları anlatılmış; detayları gösterilmiş ve en temel özellikleriyle bu yapı taşları arasındaki entegrasyon noktaları simülasyon aracılığı ile görselleştirilmiştir. Bu yapı simülatör üzerinde kurgulandıktan sonra, örnek işlemler yapılmış ve bir işlemin en başından sonuna kadar nasıl bir yol izlediği somut olarak görülebilmiştir. Bu somutlaştırma durumu ile birçok kullanıcının kafasında blok zincir nedir, ne şekilde bir akışı bulunmaktadır, temel bileşenleri nelerdir ve en temel özellikleriyle bir transactionın (işlemin) nasıl gerçekleştiği ile ilgili genel soruların cevap bulması beklenmektedir.

Bu sorular cevap bulduktan sonra birçok kullanıcı blok zincir konusunda bilgi sahibi olabilecek ve yapılacak olan ve temeli blok zincir teknolojisine dayanan uygulamalarda kolaylıkla ilerleyebileceklerdir.

Yargı

Kısa vadede finansal teknolojilerinin gelişimlerini hızla sürdüreceği görülmektedir. Bu alanda açılan birçok yeni kurum olacak ve yeni fikirler de doğacaktır. Bu alanda en çok kullanılacak teknolojilerden biri blok zincir teknolojisi olabilecektir. Çünkü bu alan gelişime çok açıktır ve altyapısı ve kurgulanma biçimiyle birçok kullanıcıya katkı sağlayacak şekilde görülmektedir. Fakat blok zincir teknolojisi de yeni olduğu için daha çok gelişmeye ihtiyacı vardır.

Kullanım alanları zamanla daha da artarsa ve etkileri daha çok görülürse hem güven ortamı sağlanmış olacak hem de yeni bir teknoloji birçok alanda kullanılmış olacaktır. Çalışma kapsamında yapılan simülatör ile blok zincirin temel yapı taşları gösterilmiş, bir işlemin en temel haliyle izlediği yol görselleştirilmiş ve blok zincirin temel kavramları simülatör ile daha somut hale gelebilmiştir.

Öneriler

Finansal teknoloji kuruluşlarının blok zincir teknolojisi konusunda daha çok geliştirme yapması ve bu konuyu girişimlerinde daha aktif kullanılmasıyla çoğu kişi bu duruma aşina olabilecektir. Böylece merkezi otoriterler için de blok zincir teknolojisi kullanımı için farkındalık oluşacak; kanuni olarak da birçok onayın yolunu açabilecektir.

Tez çalışması kapsamında yapılan simülatör ile blok zincir konusunda var olan kavramların somut olarak ele alınması sağlandığından blok zincir hakkında bilgi sahibi olmak isteyen kişiler için örnek olabilecektir.

KAYNAKÇA

Atabas, H. (2018). *Blokzinciri Teknolojisi. 1 ed*. İstanbul: Ceres Yayınları

Haddad, C., Hornuf, L. (2019). *The emergence of the global fintech market: economic and technological determinants. Small Bus Econ* 53, 81–105 Springer Press

Karahan, Ç. ve Tüfekçi, A. (2020). *Blok zincir teknolojisinin dijital kimlik yönetiminde kullanımı: bir sistematik haritalama çalışması.* Politeknik Dergisi, 23(2) : 483-496.

Usta, A. ve Doğantekin, S. (2017). *Blockchain 101. 1 ed.* İstanbul: Kapital Medya.

Çevrimiçi Kaynaklar

academy.binance.com: (2020). Blockchain'in Kullanım Alanları. 10.01.2022 tarihinde https://academy.binance.com/tr/articles/blockchain-use-cases adresinden e referans alınmıştır.

blockchain.com: (2021). Blok 704425. 10.01.2022 tarihinde https://www.blockchain.com/btc/block/000000000000000000036d2d80c0e1e21e324c13e6b4d93e8a267971c744e6c3 adresinden referans alınmıştır.

btcturk.com: (2020). Proof of Stake (Hisse Kanıtı) Nedir? Nasıl Çalışır? 10.01.2022 tarihinde https://www.btcturk.com/bilgi-platformu/proof-of-stake-hisse-kaniti-nedir-nasil-calisir/ adresinden referans alınmıştır.

economist.com.tr: (2019). Kredileri skorluyor. 10.01.2022 tarihinde https://www.ekonomist.com.tr/burcu-tuvay/kredileri-skorluyor.html adresinden referans alınmıştır.

fintechtime.com: (2019). Finansal Kurumların Radarındaki Finansal Teknolojiler 10.01.2022 tarihinde https://fintechtime.com/tr/2019/06/finansal-kurumlarin-radarindaki-finansal-teknolojiler/ adresinden edinilmiştir.

Günen, E. (2020). En Sade Anlatımla Blockchain Nedir, Nasıl Çalışır? 10.01.2022 tarihinde https://tr.cointelegraph.com/news/a-simple-explanation-of-what-is-blockchain-and-how-its-works adresinden referans alınmıştır.

Günen, E. (2020). Nonce nedir? Bitcoin Madenciliğinde Nonce Ne Demek? 10.01.2022 tarihinde https://tr.cointelegraph.com/news/what-is-nonce-what-is-the-meaning-of-cryptographic-nonce adresinden referans alınmıştır.

iyzıco.com: (2019). Fintech Nedir? Finans Sektöründeki Etkileri Nelerdir? 10.01.2022 tarihinde https://www.iyzico.com/blog/fintech-nedir-finans-sektorundeki-etkileri-nelerdir/ adresinden referans alınmıştır.

Nakamoto,S.: (2008). Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. 10.01.2022 tarihinde https://bitcoin.org/bitcoin.pdf adresinden referans alınmıştır.

researchgate.net: (2018). Bitcoin Blok Structure 10.01.2022 tarihinde https://www.researchgate.net/figure/Bitcoin-block-structure_fig1_343236094 adresinden referans alınmıştır.

Tubitak.gov.tr: (2017). Blokzincir Teknolojileri. 10.01.2022 tarihinde https://blokzincir.bilgem.tubitak.gov.tr/blok-zincir.html adresinden referans alınmıştır.

wikipedia.org: (2021). Merkle Ağacı. 10.01.2022 tarihinde https://tr.wikipedia.org/wiki/Merkle_a%C4%9Fac%C4%B1 adresinden referans alınmıştır.

Vargönen, (2020). SHA Secure Hashing Algoritması Nedir? 10.01.2022 tarihinde https://www.vargonen.com/blog/sha-secure-hashing-algoritmasi-nedir/ adresinden referans alınmıştır.