

**T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ**

**OYUN GELİŞTİRME PLATFORMLARINDA BLOKCHAIN
TABANLI ÖDEME SİSTEMLERİNİN GÜVENLİĞİ**

YÜKSEK LİSANS TEZİ

Seyyit Murat SEÇİLMİŞ

Bilgisayar Mühendisliği Anabilim Dalı

Siber Güvenlik Bilim Dalı

MART 2025

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

OYUN GELİŞTİRME PLATFORMLARINDA BLOKCHAIN
TABANLI ÖDEME SİSTEMLERİNİN GÜVENLİĞİ

YÜKSEK LİSANS TEZİ

Seyyit Murat SEÇİLMİŞ

Bilgisayar Mühendisliği Anabilim Dalı

Siber Güvenlik Bilim Dalı

Tez Danışmanı: Prof.Dr. Ünal ÇAVUŞOĞLU

MART 2025

Seyyit Murat SEÇİLMİŞ tarafından hazırlanan “Oyun Geliştirme Platformlarında Blockchain Tabanlı Ödeme Sistemlerinin Güvenliği” adlı tez çalışması 25.03.2025 tarihinde aşağıdaki jüri tarafından oy birliği/oy çokluğu ile Sakarya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Siber Güvenlik Bilim Dalı’nda Yüksek Lisans tezi olarak kabul edilmiştir.

Tez Jürisi

Jüri Başkanı : **Prof. Dr. Ahmet ZENGİN**
Sakarya Üniversitesi

Jüri Üyesi : **Prof. Dr. Ünal ÇAVUŞOĞLU** (Danışman)
Sakarya Üniversitesi

Jüri Üyesi : **Dr. Öğr. Üyesi Burak ARICIOĞLU**
Sakarya Uygulamalı Bilimler Üniversitesi



ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Sakarya Üniversitesi Fen Bilimleri Enstitüsü Lisansüstü Eğitim-Öğretim Yönetmeliğine ve Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Etiği Yönergesine uygun olarak hazırlamış olduğum “OYUN GELİŞTİRME PLATFORMLARINDA BLOCKCHAIN TABANLI ÖDEME SİSTEMLERİNİN GÜVENLİĞİ” başlıklı tezin bana ait, özgün bir çalışma olduğunu; çalışmamın tüm aşamalarında yukarıda belirtilen yönetmelik ve yönergeye uygun davrandığımı, tezin içerdiği yenilik ve sonuçları başka bir yerden almadığımı, tezde kullandığım eserleri usulüne göre kaynak olarak gösterdiğimi, bu tezi başka bir bilim kuruluna akademik amaç ve unvan almak amacıyla vermediğimi ve 20.04.2016 tarihli Resmi Gazete’de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince Sakarya Üniversitesi’nin abonesi olduğu intihal yazılım programı kullanılarak Enstitü tarafından belirlenmiş ölçütlere uygun rapor alındığını çalışmamla ilgili yaptığım bu beyana aykırı bir durumun ortaya çıkması halinde doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi beyan ederim.

(25/03/2025).

Öğrencinin Adı Soyadı





Sevgili AFU, Yasin Özçelik ve Prof.Dr. Ünal Çavuşoğluna



TEŞEKKÜR

Öncelikle bu yoğun çalışma dönemlerimizde, çalışmalarında hiçbir desteğini esirgemeyen AFU'ya ve danışmanlık desteği için Yasin Özçelik'e teşekkürlerimi sunuyorum.

Yüksek Lisans süresince her adımında destekçi rol oynayan danışmanım Prof.Dr. Ünal ÇAVUŞOĞLU'na teşekkürlerimi sunuyorum.

Seyyit Murat SEÇİLMİŞ



İÇİNDEKİLER

Sayfa

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ	v
TEŞEKKÜR	ix
İÇİNDEKİLER	xi
KISALTMALAR	xv
ŞEKİL LİSTESİ	xvii
ÖZET	xix
SUMMARY	xxi
1. GİRİŞ	1
2. LİTERATÜR TARAMASI	5
2.1. Literatür Taraması	5
3. TEMEL TANIMLAR	17
3.1. Web 2 & Web 3	17
3.1.1. Web 2.0	17
3.1.2. Web 3.0	17
3.1.3. Web 2.0'dan Web 3.0'a geçiş süreci	18
3.2. Oyun Geliştirme Platformları	18
3.2.1. PC ve konsol oyun platformları	18
3.2.2. Mobil oyun platformları	19
3.2.3. Web tabanlı oyunlar	19
3.3. Blockchain Teknolojisi	19
3.3.1. Blockchain tarihi ve evrimi	19
3.3.2. Blockchain türleri ve protokolleri	20
3.3.2.1. Blockchain türleri	20
3.3.2.2. Blockchain protokolleri	21
3.3.3. Blockchain çalışma mantığı ve bileşenleri	22
3.3.3.1. Blockchain yapısı ve işleyişi	22
3.4. Akıllı Sözleşmeler	25
3.5. Merkeziyetsizlik	26
3.5.1. Akıllı sözleşmelerde merkeziyetsizlik	27
3.6. Blockchainlerde Layer Kavramı	27
3.6.1. Layer 1	27
3.6.2. Layer 2	28
3.6.3. Layer 3	28
3.7. Blockchain Ağları	28
3.7.1. Ethereum blockchain ağı	28
3.7.2. Bitcoin blockchain ağı	29
3.7.3. Avalanche blockchain ağı	29
3.7.4. Cardano blockchain ağı	29
3.7.5. Solana blockchain ağı	30
3.7.6. Ripple blockchain ağı	30
3.7.7. Ağların karşılaştırılması	30

3.7.7.1. Hız ve ölçeklenebilirlik	30
3.7.7.2. İşlem maliyeti	31
3.7.7.3. Merkeziyetsizlik ve güvenlik	31
3.7.7.4. Kullanım alanları	31
3.7.7.5. Konsensüs mekanizmaları	31
3.8. Tokenler	31
3.8.1. Token nedir ve ne işe yarar?	31
3.8.2. Token türleri ve kullanım alanları	32
3.8.2.1. Hizmet tokenleri (Utility Tokens)	33
3.8.2.2. Menkul kıymet tokenleri (Security Tokens)	33
3.8.2.3. Varlık destekli tokenler (Asset-Backed Tokens)	34
3.8.2.4. Hisse senedi tokenleri (Equity Tokens)	35
3.8.2.5. Blockchain tokenlerinin kullanım alanları ve uygulamaları	35
3.9. Dijital Cüzdan	37
3.9.1. Dijital cüzdanların rolü ve türleri	38
3.9.1.1. Mobil cüzdanlar	39
3.9.1.2. Web tabanlı cüzdanlar	39
3.9.1.3. Donanım cüzdanlar	40
3.9.2. Dijital cüzdanlarda güvenlik önlemleri	41
4. MODEL MİMARİ	43
4.1. Solana Blockchain Altyapısının Entegrasyonu	44
4.2. Rust Kullanılarak Akıllı Sözleşme Geliştirme	44
4.3. React ile Web Tabanlı Kullanıcı Arayüzü	45
4.4. Phantom Dijital Cüzdan Entegrasyonu	45
4.5. Sistem Bileşenlerinin İletişimi	45
5. UYGULAMA	47
5.1. Program Tanıtımı ve Amaçları	47
5.1.1. Ana program modülü	47
5.1.2. initialize_program	47
5.1.3. process_payment	47
5.1.4. update_program_settings	49
5.1.5. freeze_program	49
5.1.6. blacklist_account	49
5.2. Solana Hesaplarının Temelleri ve Veri Yapıları	50
5.2.1. Signer	50
5.2.2. Account	50
5.2.3. ProgramState	50
5.2.4. PaymentState	51
5.3. Ortamının Yapılandırılması ve Güvenli Oturum Açma Geliştirmesi	51
5.3.1. Güvenli oturum açmanın implementasyonu	51
5.3.2. Express yapılandırması ve middleware	52
5.3.3. JWT konfigürasyonu ve güvenlik önlemleri	53
5.3.4. Token doğrulama middleware'i	54
5.3.5. Güvenli token gönderimi (HTTP-only cookie)	54
5.3.6. Token içeriği ve payload	54
5.3.7. Bakiye güncelleme işlemi ve yetkilendirme	55
5.3.8. Geliştirilen uygulamanın son hali	55
6. BİRİM TESTİ	57
6.1. Veri Doğrulama Eksikliği	57
6.2. Lamports Manipülasyonu	58

6.3. Aritmetik-Kayan Nokta Hatası.....	58
6.4. Rust Özel Sorunları	59
6.5. Test Sonuçları.....	59
7. SONUÇLAR	61
KAYNAKLAR	65
ÖZGEÇMİŞ.....	69





KISALTMALAR

DAO	: Decentralized Autonomous Organization
DApps	: Decentralized Applications
DeFi	: Decentralized Finance
EMV	: Europay Mastercard Visa
HTTP	: HyperText Transfer Protocol
HTTPS	: HyperText Transfer Protocol Secure
IOT	: Internet of Things
JWT	: JSON Web Token
NFC	: Near Field Communication
NFT	: Non Fungible Token
P2E	: Play to Earn
POS	: Point of Sale
QR	: Quick Response
TPS	: Transactions Per Second



ŞEKİL LİSTESİ

Sayfa

Şekil 4.1. Model mimari şeması	43
Şekil 5.1. Program yönetici yetkilerini ayarlayan kod parçası	47
Şekil 5.2. Ödeme sistemi ayarlayan kod parçası.....	48
Şekil 5.3. Admin fonksiyonlarını barındıran kod parçası	49
Şekil 5.4. Karaliste sistemi kod parçası	50
Şekil 5.5. JWT konfigürasyonu kod parçası	52
Şekil 5.6. Token doğrulama kod parçası.....	53
Şekil 5.7. HTTP ile token gönderimi	54
Şekil 5.8. JWT payload kod parçası.....	55
Şekil 5.9. Kullanıcı bilgileri getiren kod parçası	55
Şekil 5.10. Geliştirilen oyunun son hali.....	56
Şekil 6.1. Birim testinden bir kesit	60



ÖYÜN GELİŐTİRME PLATFORMLARINDA BLOCKHAIN TABANLI ÖDEME SİSTEMLERİNİN GÜVENLİĞİ

ÖZET

Oyun, geçmişten günümüze eğlencenin en önemli unsurlarından biri olmuştur. Sanal bir dünya ile alternatif evrenler sunan oyunlar, kendi içlerinde yarattıkları ekonomi sayesinde gerçek dünya ile maddi temas sağlayabilmektedir. Bu noktalardaki para kazanma yöntemlerinden biri de oyun içi kostüm, eşya, ikon ve benzeri edinimlerin gerçek dünya parası ile satılması ve gerçek dünyada bir varlık yaratılmasıdır. Blockchain teknolojileri sayesinde bu varlıklar son derece güvenli bir şekilde merkezsiz olarak saklanabilmektedir. Şifreleme yöntemleri ve dağıtık defter yapısı sayesinde bu teknoloji, kullanıcıların dijital varlıklarını üçüncü taraflara ihtiyaç duymadan güvenli bir ortamda saklamalarına olanak sağlıyor. Blockchain sadece oyun sektöründe değil, finans, sağlık, lojistik, eğitim ve daha birçok alanda devrim niteliğinde yenilikler sunan teknolojik bir gelişmedir. Özellikle verilerin değişmez ve şeffaf bir şekilde saklanmasını sağlayarak güvenilirliği artırıyor ve araçlara olan bağımlılığı azaltıyor. Bu sayede blockchain, dijital ekonomiden sosyal sistemlere kadar geniş bir alanda insan hayatını derinden etkileyen ve yeniden şekillendiren bir unsur haline gelmiştir.

P2E (Play to Earn), oyunlarda oynadıkça kripto varlıkları kazanmaya yönelik bir modeldir. Oyuncunun oyun oynama süresini kazanarak artırmayı hedefler. Bu da oyuna bağlı kripto varlıkların değerini artırır ve bir ekonomi yaratır.

Benzer şekilde, NFT (Non-Fungible Token) kazanıp satarak, blockchain teknolojisi oyunlarda gerçek dünya kazançları elde edilmesini sağlar.

Dijital varlıkların gerçek dünyadaki karşılığı yüksek güvenlik önlemleri gerektirir. Blockchain teknolojisi burada ana aktörlerden biridir.

Oyun geliştirme platformlarında blockchain tabanlı ödeme sistemlerinin güvenliği, işlem bütünlüğünü, kullanıcı gizliliğini ve varlık sahipliğini artırmaya odaklanan kritik bir araştırma alanıdır. Blockchaini teknolojisi, veri tahrifatı ve yetkisiz erişim gibi geleneksel ödeme sistemleriyle ilişkili riskleri azaltan merkezi olmayan bir çerçeveye sunar.

Bu çalışmada model mimari olarak Solana blockchain altyapısı entegre edilmiştir. Solana'nın yüksek hızlı ve düşük maliyetli işlem özelliklerinden yararlanılarak projenin temel gereksinimlerini karşılayacak bir sistem tasarımı gerçekleştirilmiştir. Akıllı sözleşmeler Rust programlama dili kullanılarak geliştirildi. Blockchain tabanlı ödeme sistemlerinin güvenilir ve verimli çalışmasını sağlamak için Rust'ın performans odaklı ve güvenli bellek yönetimi özellikleri tercih edildi.

Akıllı sözleşme geliştirme sürecinde işlem mantığı, veri doğrulama ve güvenlik önlemleri gibi unsurlar özenle tasarlandı. Ayrıca token transfer fonksiyonları ve kullanıcı yetkilendirme süreçleri Solana'nın Program Library standardı kullanılarak modellendi.

Web tabanlı kullanıcı arayüzü React kütüphanesi kullanılarak oluşturuldu. React'in bileşen tabanlı mimarisi ve dinamik veri yönetimi yetenekleri, kullanıcı deneyimini geliştirecek bir arayüz geliştirilmesini sağladı. Bu süreçte kullanıcıların dijital cüzdanları üzerinden sisteme güvenli bir şekilde erişebilmeleri için dijital cüzdan entegrasyonu gerçekleştirildi. Kullanıcıların blockchain işlemlerini kolayca gerçekleştirebilmelerini sağlayan Phantom, Sollet vb. gibi Solana uyumlu cüzdanlar tercih edildi.

Sistem bileşenleri detaylı olarak analiz edilmiş ve mimari tasarımın temel taşları olarak belirlenmiştir. Bu bileşenler arasında akıllı sözleşmeler, blokchaini ağı, kullanıcı arayüzü ve dijital cüzdanlar yer almaktadır. Ayrıca bu bileşenler arasındaki iletişim mekanizmaları tanımlanmış ve veri akışını optimize etmek için gerekli protokoller belirlenmiştir. Sistem, kullanıcıların işlem güvenliğini ve veri bütünlüğünü sağlamayı amaçlayan bir yapıda tasarlanmıştır.

Bu yöntem ve araçlar bir araya getirilerek, blockchain tabanlı ödeme sistemlerinin oyun geliştirme platformlarında uygulanabilirliğini değerlendiren bir model sunulmuş ve proje güvenlik açısından tartışılmıştır. Bu tez, akıllı sözleşmenin Rust ile ilgili güvenlik, giriş ve çıkış işlemleri, kullanıcı ve imzalayan kimliklerinin güvenli çalışması gibi güvenlik açıklarını ve avantajlarını inceleyerek oyun platformlarında blokchaini tabanlı ödeme sistemlerinin güvenliğine genel bir bakış sunmaktadır.

ON GAME DEVELOPMENT PLATFORMS BLOCKCHAIN BASED SECURITY OF PAYMENT SYSTEMS

SUMMARY

Gaming has been one of the most important elements of entertainment from past to present. Games, which offer alternative universes with a virtual world, can achieve material contact with the real world through the economy they create within themselves. One of the monetization methods at these points is to sell in-game costumes, items, icons and similar acquisitions with real-world money and to create an asset in the real world. Thanks to blockchain technologies, these assets can be stored decentralized in a highly secure manner. Thanks to its encryption methods and distributed ledger structure, this technology allows users to store their digital assets in a secure environment without the need for third parties. Blockchain is a technological development that offers revolutionary innovations not only in the gaming industry, but also in finance, health, logistics, education and many other fields. In particular, it enables data to be stored in an immutable and transparent way, increasing reliability and reducing dependency on intermediaries. In this way, blockchain has become an element that deeply affects and reshapes human life in a wide range of areas from the digital economy to social systems.

P2E (Play to Earn) is a model for earning crypto assets as you play in games. It aims to increase the player's playing time by earning. This increases the value of crypto assets tied to the game and creates an economy.

Similarly, by earning and selling NFT (Non-Fungible Token), blockchain technology enables real-world gains in games. The real-world equivalent of digital assets requires high security measures. Blockchain technology is one of the main actors here.

The security of blockchain-based payment systems in game development platforms is a critical area of research focused on increasing transaction integrity, user privacy and asset ownership. Blockchain technology offers a decentralized framework that mitigates the risks associated with traditional payment systems, such as data falsification and unauthorized access.

In this study, blockchain-based payment systems in games will be discussed, focusing on the benefits and vulnerabilities for users and systems.

In this study, Solana blockchain infrastructure is integrated as the model architecture. By taking advantage of Solana's high-speed and low-cost transaction features, a system design was realized to meet the basic requirements of the project. Smart contracts were developed using the Rust programming language. Rust's performance-oriented and secure memory management features were preferred to ensure reliable and efficient operation of blockchain-based payment systems.

During the smart contract development process, elements such as transaction logic, data validation and security measures were carefully designed. In addition, token

transfer functions and user authorization processes were modeled using Solana's Program Library standard.

The web-based user interface was built using the React library. React's component-based architecture and dynamic data management capabilities enabled the development of an interface that would enhance the user experience. In this process, digital wallet integration was realized so that users can securely access the system through their digital wallets. Solana-compatible wallets such as Phantom, Sollet, etc., which allow users to easily perform blockchain transactions, were preferred.

The system components were analyzed in detail and identified as the cornerstones of the architectural design. These components include smart contracts, blockchain network, user interface and digital wallets. In addition, the communication mechanisms between these components were defined and the protocols required to optimize the data flow were identified. The system is designed in a structure that aims to ensure users' transaction security and data integrity.

By combining these methods and tools, a model that evaluates the applicability of blockchain-based payment systems in game development platforms is presented and the project is discussed in terms of security. This thesis provides an overview of the security of blockchain-based payment systems in gaming platforms by examining the vulnerabilities and advantages of the smart contract, such as Rust-related security, input and output transactions, and the secure operation of user and signer identities.

As a result of this study, important findings have been obtained on the usability and security of blockchain-based payment systems on gaming platforms. The smart contract model, developed using the Solana blockchain infrastructure and the Rust programming language, provides a suitable solution for payment systems on gaming platforms with low cost and fast transaction capability.

The web-based demo was developed with the React library to provide a user-friendly interface and wallet integration, enabling easy digital payments. The system managed to optimize security by protecting users' payment data and authorization mechanisms, and showed positive results in test scenarios.

As a result of the performance tests, it was determined that the Solana infrastructure can provide a significant advantage over traditional centralized payment systems by meeting expectations, especially in micropayments and intensive transaction scenarios. In addition, the architectural design of the system ensured that the communication mechanisms between components work effectively and that security is prioritized in payment processes.

In the developed application, security weaknesses were tried to be prevented in 5 steps. These vulnerabilities can be named as signer control vulnerability, ownership control vulnerability, floating point vulnerability and program call vulnerability.

Future research in this field can focus on further optimizing the performance and security of blockchain-based payment systems in gaming environments. The evolution of blockchain technology and the integration of advanced cryptographic mechanisms could further strengthen digital asset protection. Additionally, interoperability between different blockchain networks could enhance the usability and accessibility of payment systems across multiple gaming platforms. The ongoing development in this area will significantly impact the way digital economies function within gaming ecosystems, providing more secure, transparent, and efficient transactions for users worldwide.

Moreover, regulatory developments and legal frameworks surrounding blockchain-based gaming transactions will play a crucial role in shaping the adoption of these technologies. Governments and financial institutions may implement policies to ensure consumer protection, mitigate financial risks, and enhance transaction transparency. These regulations could provide greater credibility and trust in blockchain-based payment systems, making them a preferred choice for game developers and players alike. Advancements in artificial intelligence and machine learning could further enhance blockchain security in gaming. AI-driven security protocols could be implemented to detect fraudulent activities, prevent unauthorized access, and ensure the integrity of digital transactions. As blockchain technology continues to evolve, integrating AI-based monitoring and security mechanisms may significantly improve the overall efficiency and reliability of payment systems in gaming platforms.

This study demonstrates that blockchain-based payment systems offer an efficient and secure solution for game development platforms. Different blockchain-based technologies have different transaction costs, speed, smart contract security, and vulnerabilities to other technologies they enable. For gaming platforms, blockchain-based systems stand out especially with the Play 2 Earn model. As user habits increase, security standards will emerge and blockchain-based payments will emerge as a strong preference. This study has enabled us to reach these conclusions by examining the security of a Solana-based system with the application demo we developed.



1. GİRİŞ

Oyun geçmişten günümüzün en önemli eğlence unsurlarından biri olmuştur. Sanal bir dünya ile alternatif evrenler sunan oyunlar, kendi içlerinde oluşturduğu ekonomi ile gerçek dünya ile maddi temas elde edebilmektedir.

Bu noktalarda parasallaştırma yöntemlerinden biri, oyun içi kostüm, eşya, ikon ve benzeri kazanımların gerçek dünya parası ile satılması ve oyun içi kazanımların gerçek dünya üzerinde bir varlık oluşturması üzerinedir.

Blokchain teknolojileri sayesinde bu varlıklar, yüksek güvenli bir şekilde merkeziyetsiz olarak saklanabilmektedir. Bu teknoloji, şifreleme yöntemleri ve dağıtık defter yapısı sayesinde, kullanıcıların dijital varlıklarını üçüncü taraflara ihtiyaç duymadan güvenli bir ortamda muhafaza etmelerine olanak tanımaktadır. Blokchain, yalnızca oyun sektöründe değil, finans, sağlık, lojistik, eğitim ve daha pek çok alanda devrim niteliğinde yenilikler sunan bir teknolojik gelişmedir. Özellikle, verilerin değiştirilemez ve şeffaf bir şekilde saklanmasını sağlayarak güvenilirliği artırmakta ve araçlara olan bağımlılığı azaltmaktadır. Bu sayede blokchain, dijital ekonomiden sosyal sistemlere kadar geniş bir yelpazede insan hayatını derinden etkileyen ve yeniden şekillendiren bir unsur haline gelmiştir.

P2E (Play to Earn), oyunlarda oynadıkça kripto varlıklar kazanmaya yönelik bir modeldir. Oyuncunun oyun süresini kazandırarak arttırılması hedeflenmektedir. Bu da oyuna bağlı kripto varlıkların değerini arttırmakta ve bir ekonomi oluşturmaktadır.

Benzer şekilde NFT üzerinden kazanımlar ve satışlar gerçekleştirilerek blokchain teknolojisi ile oyunlar içinde gerçek dünya kazanımları sağlanmaktadır.

Dijital varlıkların gerçek dünyada bir karşılığı olması, yüksek güvenlik önemlemleri gerektirmektedir. Blokchain teknolojisi buradaki ana aktörlerden bir tanesidir.

Oyun geliştirme platformlarında blokchaini tabanlı ödeme sistemlerinin güvenliği, işlem bütünlüğünü, kullanıcı gizliliğini ve varlık sahipliğini artırmaya odaklanan kritik bir araştırma alanıdır. Blockchain teknolojisi, verilerin tahrif edilmesi ve yetkisiz

eriřim gibi geleneksel ödeme sistemleriyle iliřkili riskleri azaltan merkezi olmayan bir çerçeve sunar [1].

Bu tezin amacı geliřmekte olan oyun endüstrisinde, yine genç bir dönemini yařayan blockchain teknolojilerini barındıran ödeme sistemleriyle oyun dünyası için güvenli ve gerçek dünyada maddi karřılıklar oluřturabilecek çözüm önerisinin geçerli bir çözüm olacađını göstermektir. P2E gibi modeller sayesinde oyuncuların oyun alışkanlıkları gelir modellerine dönüşebilecek; hantal, işlem ücretleri ve depolama bakımından oldukça maliyetli banka merkezli ödeme sistemleri yerini merkeziyetsiz sistemlere bırakacak.

Literatürde incelenen çalışmalarla yapın tezin gerekliliđi öne koyulmuřtur. Genellikle güvenlik odaklı çalışmalarda uygulama tarafından, uygulama odaklı olanlarda ise oyun yaklaşımlarında bir eksiklik gözükmemektedir. Bu sebepten yaptığımız geliştirme literatürde özel bir alan yakalamış ve katkı sağlamış olmaktadır.

Zolanvari ve arkadaşlarının (2018) “Security Services Using Blockchains: A State of the Art Survey” başlıklı çalışması blockchain teknolojisinin güvenlik hizmetlerindeki potansiyelini detaylı olarak ele almaktadır. Bu makale, blockchainin karar alma süreçlerinde dağıtılmış mutabakat mekanizmalarını kullanarak güvenliđi artırabileceđine dikkat çekmekte, ancak Ethereum ve Hyperledger gibi yaygın platformların gizlilik, ölçeklenebilirlik ve iletişim gecikmeleri gibi temel teknik sorunları bulunduđunu ortaya koymaktadır. Bu sorunlar, özellikle dinamik ve yüksek işlem hacimli oyun geliştirme ortamlarında önemli performans engelleri yaratmaktadır. Tez kapsamında, bu zorluklara karřı çözüm arayışında Solana gibi yüksek işlem kapasitesine sahip, düşük gecikmeli blokzincir teknolojileri tercih edilmektedir.

Min ve arkadaşlarının (2019) “Blockchain Games: A Survey” başlıklı makalesi, blockchain teknolojisinin oyun içi ekonomik modellerde ve oyuncu katılımında yarattığı dönüşümü kapsamlı biçimde incelemektedir. Özellikle oyun içi varlıkların mülkiyet haklarının blockchain ile tanımlanması ve dijital varlık ticaretinin sağlanması, oyuncular arasında yeni ekonomik fırsatlar yaratmaktadır. Ancak, bu çalışmada güvenlik ve işlem bütünlüğü konularının detaylandırılmamış olması, blockchain tabanlı oyun ödeme sistemlerinde güvenlik üzerine yapılacak arařtırmalar

iin bir boşluk bırakmaktadır. Bu tezin özgün katkılarından biri de, güvenlik boyutunu teknik ve kullanıcı algısı perspektifinden bütüncül olarak değerlendirmesidir.

Iqbal ve Matulevicius (2019) tarafından yürütölen “Blockchain-based Application Security Risks: A Systematic Literature Review” alışması, blockchain teknolojisinin sunduėu gçlü güvenlik özelliklerine rağmen yeni ortaya ıkan riskleri kapsamlı şekilde sınıflandırmaktadır. Bu alışma, özellikle Ethereum tabanlı DAO saldırısı gibi yüksek profilli güvenlik açıklarını örnek vererek, blockchain uygulamalarındaki reentrancy saldırıları gibi spesifik tehditlerin ciddi finansal kayıplara yol açabileceėini göstermektedir. Tez alışmasında, Rust dili kullanılarak geliştirilen ve Solana platformunda alışan akıllı sözleşmelerin, bu tür tehditlere karşı nasıl güvenli hale getirilebileceėi teknik olarak ele almaktadır.

Saha ve arkadaşlarının (2023) “Protecting the Decentralized Future: An Exploration of Common Blockchain Attacks and their Countermeasures” makalesi, blockchainin karşılaştıėı temel saldırı türleri arasında %51 saldırıları, çift harcama sorunları ve akıllı sözleşme açıklarını detaylı şekilde incelemektedir. Bu tür saldırılar, merkeziyetsiz yapıya rağmen sistemin bütünlüğünü ve güvenilirliğini tehdit etmekte, özellikle blockchain tabanlı ödeme sistemlerinde büyük riskler oluşturmaktadır. Tez alışması, bu saldırılara karşı gçlü konsensüs algoritmalarının kullanılması, akıllı sözleşmelerin düzenli denetimi ve güvenlik testlerinin önemi üzerinde durmaktadır.

İbrahim Halil Efendioėlu ve arkadaşlarının “The Mediating Effect of Blockchain Technology on the Cryptocurrency Purchase Intention” başlıklı alışması, blockchain teknolojisinin kullanım kolaylıėı ve sağladığı faydaların kullanıcıların kripto para satın alma niyetini artırdığını ortaya koymaktadır. Bu bulgu, blockchain tabanlı ödeme sistemlerinin oyun dünyasında benimsenmesinde kullanıcı algılarının ne denli kritik olduğunu göstermektedir. Bu alışma, algıları iyileştirecek arayüz tasarım ilkeleri ve kullanıcı deneyimi yaklaşımlarını da uygulama kapsamında ele alır.

Son olarak, Myles Lewis ve Chris Crawford’un (2024) “Architectural Design for Secure Smart Contract Development” makalesi, akıllı sözleşmelerin güvenliėinin sağlam yazılım mühendisliėi ilkelerine dayandığını ve kapsamlı test süreçlerinin zorunlu olduğunu belirtmektedir. Bu tezde, Rust ile yazılan akıllı sözleşmelerin mimari tasarımı, güvenlik açıklarını minimize edecek şekilde planlanacak ve Solana aėı üzerinde kapsamlı testlerden geçirilecektir.

Bu tez, literatürde genel anlamda blockchain teknolojisinin oyun sektörüne entegrasyonu, ekonomik etkileri ve genel güvenlik riskleri üzerine yoğunlaşan çalışmaların aksine, teknik altyapı detayları ve pratik uygulamalarla güvenlik risklerini doğrudan ele alan özgün bir araştırma sunmaktadır. Solana, Rust ve React teknolojilerinin birlikte kullanılması, yüksek performans ve güvenlik gereksinimlerini karşılayan modern bir çözümün prototipini ortaya koymaktadır. Aynı zamanda kullanıcı deneyimi ve güvenlik algısının oyun ödeme sistemleri üzerindeki etkisini de inceleyerek, hem teknik hem de kullanıcı perspektifinden güvenliğin artırılmasını hedeflemektedir.

Bu tez çalışması, öncelikle “Literatür Taraması” bölümü ile birlikte endüstride benzer çalışmaların incelenmesini içermektedir. "Temel Tanımlar" bölümünde ise blockchain ve ilgili teknolojilere dair kavramsal açıklamalara yer verilmiştir.

"Model Mimarisi" bölümünde, Solana tabanlı blockchain yapısının entegrasyonu, Rust diliyle akıllı sözleşme geliştirme süreci, React ile kullanıcı arayüzü oluşturulması ve cüzdan bağlama işlemleri gibi teknik konular ele alınmaktadır.

"Uygulama" bölümünde, belirtilen teknolojiler kullanılarak React tabanlı geliştirilen ve tıklama mekanizmasına dayalı bir blockchain oyununda ödeme sistemi ve güvenlik uygulamaları üzerinde durulmuştur.

"Birim Testi" bölümünde, geliştirilen uygulamanın test süreci detaylandırılmış ve elde edilen sonuçlar paylaşılmıştır.

Son olarak, "Sonuçlar" bölümünde yapılan tez çalışmasının literatüre katkısı değerlendirilmiş ve ulaşılan genel bulgular özetlenmiştir.

Sonuç olarak, bu çalışma oyun geliştirme platformlarında blockchain tabanlı ödeme sistemlerinin güvenliğinin sağlanmasına yönelik önemli bir katkı sunmakta ve gelecekte bu alanda yapılacak araştırmalar için bir perspektif oluşturmaktadır. Özellikle yüksek performanslı blockchain altyapıları ve güvenli akıllı sözleşme geliştirme yöntemleri, oyun sektörünün ihtiyaçlarını karşılayacak şekilde uyarlanmış ve test edilmiştir. Kullanıcı algısı ve deneyimi üzerine yapılan analizler ise sistemlerin benimsenmesini artıracak stratejilerin geliştirilmesine ışık tutmaktadır.

2. LİTERATÜR TARAMASI

2.1. Literatür Taraması

M. Zolanvari, A. Erbad, R. Jain ve M. Samaka tarafından 2018 yılında yazılan, "Security Services Using Blockchains: A State of the Art Survey" başlıklı makale, blockchain teknolojisinin güvenlik hizmetlerinde kullanılmasına ilişkin potansiyel ve zorlukları kapsamlı bir şekilde incelemektedir. Yazarlar, blockchainin yerel blockchain günlüklerini kullanarak karar alma mekanizmalarını nasıl kolaylaştırabileceğine ve bu sayede dağıtılmış mutabakata olan ihtiyacı nasıl ortadan kaldırabileceğine odaklanmaktadır. Bu yaklaşım, özellikle oyun geliştirme platformları gibi dinamik ortamlarda, blockchain tabanlı ödeme sistemlerinin güvenliği açısından son derece önemlidir.

Makale, blockchain teknolojisinin özellikle gerçek zamanlı uygulamalar bağlamında karşılaştığı birkaç kritik zorluğun altını çizmektedir. Yazarlar, Ethereum ve Hyperledger gibi platformların Bitcoin'in gecikme sorunlarını ele alma konusunda ilerleme kaydettiğini, ancak madencilik için gereken sürenin hâlâ oldukça yüksek olduğunu – iki ila üç saniye arasında değiştiğini – ve milisaniye düzeyinde yanıt süresi gerektiren uygulamalar için yetersiz kaldığını belirtmektedir. Bu gecikme, şifreleme ve güvenlik tekniklerinin getirdiği karmaşıklıklarla daha da ağırlaşmakta ve işlem sürelerini artırmaktadır. Yazarlar, bu zaman tüketimi sorunlarının yanı sıra, gizlilik, ölçeklenebilirlik ve iletişim yüküyle ilgili zorlukların, blockchainin güvenlik uygulamalarında etkili bir şekilde kullanılmasını önemli ölçüde engellediğini savunmaktadır.

Makalenin eleştirel bir değerlendirmesi, blockchainin güvenlik hizmetleri için teorik temellerini ve potansiyel uygulamalarını etkili bir şekilde özetlediğini, ancak son yıllarda kaydedilen ilerlemeleri yeterince vurgulamadığını ortaya koymaktadır. Layer 2 çözümlerinin ve diğer ölçeklenebilirlik iyileştirmelerinin geliştirilmesi gibi blockchain teknolojilerinin hızlı evrimi, belirtilen gecikme sorunlarına yönelik alternatif yollar sağlayabilir. Ayrıca yazarlar, teknolojik potansiyeller ile karşılaşılan

zorluklar arasında bir denge kurulması gerektiğini vurgulamakta ve gelecekteki arařtırmaların bu engellerin ařılmasına odaklanması gerektiğini önermektedir.

Açık anahtar řifrelemesi yoluyla kimlik doęrulama ve gizlilik konusundaki tartıřma, özellikle blockchain tabanlı ödeme sistemleri açasından oldukça önemlidir. Bu unsurlar, oyun geliřtirme platformlarında güvenli iřlemlerin saęlanması için kritik öneme sahiptir. Yazarlar, gizlilik ve ölçeklenebilirlięi birincil bileřenler olarak dikkate alan bir tasarım yaklařımını savunmaktadır ve bu, blockchain çözümlerini platformlarına entegre etmeyi planlayan geliřtiricilerin ihtiyaçlarıyla uyumludur [2].

T. Min, H. Wang, Y. Guo ve W. Cai tarafından 2019 yılında yazılan "Blockchain Games: A Survey" bařlıklı makale, blockchain teknolojisi ile dięital oyunların kesiřimini, özellikle ödeme sistemleri bağlamında, kapsamlı bir řekilde incelemektedir. Yazarlar, blockchainin sanal varlıkların yapısını nasıl dönüřtürdüęünü ve bunun çok oyunculu oyun ortamlarındaki etkilerini vurgulamaktadır.

Makalenin temel bulgularından biri, blockchain oyunlarının türlerine ve teknik platformlarına göre sınıflandırılmasıdır. Bu sınıflandırma, blockchainin oyun geliřtirme süreçlerine entegre edilebileceęi çeřitli yolları anlamak açasından önemlidir. Makalede, blockchainin oyun içi varlıkların mülkiyetini ve ticaretini kolaylařtırdıęı, bunun da oyuncu katılımını önemli ölçüde artırdıęı ve oyunlar içinde yeni ekonomik fırsatlar yarattıęı belirtilmektedir. Ancak bu entegrasyon, oyunculara güç katmanın yanı sıra, güvenlik ve ödeme sistemlerinde iřlem bütünlüęü açasından karmařıklıklar da doğurmaktadır.

Yazarlar, blockchain oyunları endüstrisindeki eğilimleri analiz etmek için istatistiksel bir yaklařım benimseyerek, gelecekteki teknolojik ve ticari geliřmeleri öngörmektedir. Bu ileri görüş, özellikle blockchain teknolojisinin geliřmeye devam etmesiyle ortaya çıkabilecek potansiyel büyüme alanlarını ve karşılaşılabilecek zorlukları vurguladıęından, oyun endüstrisindeki geliřtiriciler ve paydařlar için oldukça deęerlidir.

Bununla birlikte, makale blockchain entegrasyonunun faydalarını etkili bir řekilde özetlese de, blockchain tabanlı ödeme sistemlerinde ortaya çıkabilecek güvenlik risklerini daha derinlemesine inceleyebilirdi. Bu güvenlik boyutlarının daha ayrıntılı bir řekilde ele alınması, makalenin oyunlarda blockchain teknolojisi üzerine olan literatüre katkısını daha da artırabilirdi [3].

M. Iqbal ve R. Matulevicius tarafından 2019 yılında yazılan "Blockchain-based Application Security Risks: A Systematic Literature Review" başlıklı makale, blockchain teknolojisi etrafındaki güvenlik ortamını kapsamlı bir şekilde incelemekte ve özellikle bu dağıtık değiştirilemez defter sistemini kullanan uygulamalar bağlamında değerlendirmeler sunmaktadır. Yazarlar, blockchain tabanlı uygulamalarda güvenliğin çift yönlü doğasını vurgulamakta; merkezi sistemlerde hafifletilen risklerin yanı sıra blockchain ortamında ortaya çıkan yeni güvenlik açıklarına dikkat çekmektedir.

Makalenin temel fikri, blockchain teknolojisinin merkezi olmayan konsensüs mekanizması ve kriptografik temelleri sayesinde gelişmiş güvenlik özellikleri sunduğunu, ancak bunun risklerden tamamen arınmış bir teknoloji olmadığını belirtmektedir. Yazarlar, özellikle parasal varlıkları içeren blockchain uygulamalarında gözlemlenen belirli güvenlik tehditlerini detaylandırmaktadır. Örneğin, Ethereum tabanlı DAO akıllı sözleşmelerine yapılan tekrarlı giriş (reentrancy) saldırısı gibi önemli olaylara atıfta bulunarak, bu tür saldırıların önemli finansal kayıplara ve sistem güvenliğinin ihlaline neden olabileceğini açıklamaktadır.

Bu derlemenin önemli katkılarından biri, blockchain uygulamalarına özgü kapsamlı bir güvenlik riskleri listesinin belirlenmesidir. Yazarlar, bu riskleri blockchain teknolojisinin benimsenmesiyle hafifletilenler ve yeni ortaya çıkanlar olarak kategorize etmektedir. Bu sınıflandırma, blockchaine ödeme sistemlerinde kullanan oyun geliştirme platformları gibi geliştiriciler ve paydaşlar için oldukça önemlidir, çünkü bu, karşılaşılabilecekleri güvenlik ortamını daha net bir şekilde anlamalarına yardımcı olmaktadır.

Ayrıca makale, yalnızca riskleri sunmakla kalmayıp, bu güvenlik açıklarını hafifletmek için potansiyel önlemler de önermektedir. Bu proaktif yaklaşım, blockchain uygulamalarının güvenliğini artırmaya yönelik pratik stratejiler sunması nedeniyle alandaki uygulayıcılar için özellikle değerlidir. Yazarlar, bu alanda süregelen araştırmaların önemini vurgulayarak, mevcut ve yeni ortaya çıkan güvenlik tehditlerini daha ayrıntılı bir şekilde anlamanın, blockchain teknolojisinin sürekli evrimi için hayati olduğunu öne sürmektedir [4].

B. Saha, M. Mehedi Hasan, N. Anjum, S. Tahora ve yazarlar tarafından 2023 yılında yazılan "Protecting the Decentralized Future: An Exploration of Common Blockchain

"Attacks and their Countermeasures" başlıklı makale, blockchain teknolojisinin karşılaştığı güvenlik zorluklarını kapsamlı bir şekilde incelemektedir, özellikle de finansal hizmetler de dahil olmak üzere çeşitli endüstrilerdeki uygulamaları bağlamında. Yazarlar, blockchainin şeffaflık, değiştirilemezlik ve güvenlik gibi doğasında bulunan avantajlarını etkin bir şekilde ortaya koyarken, bu avantajlarla birlikte gelen güvenlik açıklarını da ele almaktadır.

Makalenin eleştirel bir değerlendirmesi, yazarların blockchain ağlarını tehdit eden çeşitli saldırı türlerini başarıyla belirlediğini ve kategorize ettiğini göstermektedir. Bunlar arasında %51 saldırıları, çift harcama saldırıları ve akıllı sözleşmelerle ilgili güvenlik açıkları yer almaktadır. Özellikle %51 saldırıları konusundaki tartışma dikkat çekicidir, çünkü bu, merkezi olmayan bir çerçevede merkezi kontrolün etkilerini vurgulamaktadır. Bu konu, blockchain tabanlı ödeme sistemlerinin, özellikle de merkeziyetsiz finans (DeFi) uygulamalarının giderek daha fazla entegre edildiği oyun geliştirme platformlarında karşılaşılabilecek potansiyel riskleri anlamak için önemlidir.

Yazarlar ayrıca, bu güvenlik açıklarını hafifletmek için karşı önlemlerin önemini vurgulamaktadır. Güvenliği artırmak için çeşitli stratejiler önermektedirler, bunlar arasında güçlü konsensüs mekanizmalarının uygulanması ve akıllı sözleşmelerin düzenli güvenlik denetimlerinin yapılması yer almaktadır. Bu, oyun geliştirme platformları için özellikle önemlidir, çünkü blockchainin işlem sistemlerini kullanan bu platformlarda sistemlerin bütünlüğü, kullanıcı güvenliğini sürdürmek ve kesintisiz bir oyun deneyimi sağlamak için kritik öneme sahiptir.

Ayrıca, makale blockchain güvenliği alanında süregelen araştırma ve geliştirmelerin gerekliliğini vurgulamaktadır. Teknoloji geliştikçe ve daha yaygın bir şekilde benimsendikçe, potansiyel tehditler hakkında bilgi sahibi olmak ve proaktif önlemler geliştirmek kritik olacaktır. Yazarlar, blockchain ağlarının güvenliğini artırmak için geliştiriciler, araştırmacılar ve endüstri paydaşları arasında iş birliği yapmayı savunmaktadır. [5]

S. Dong, K. Abbas, M. Li ve J. Kamruzzaman tarafından 2023 yılında yazılan "Blockchain technology and application: an overview" başlıklı makale, çeşitli blockchain türlerini kapsamlı bir şekilde inceleyerek, bunların özelliklerini, avantajlarını ve sınırlamalarını vurgulamaktadır. Tartışmanın önemli bir yönü,

özellikle güvenlik, verimlilik ve yönetim açısından konsorsiyum, halka açık ve özel blockchainler arasındaki farklardır.

Yazarlar, konsorsiyum blockchainlerinin, paylaşılan kontrol ve yüksek güvenlik sunduğunu belirtirken, şeffaflık ve anonimlik açısından zorluklar ortaya çıkarabileceğine dikkat çekmektedir. Bu ağlara erişim, önceden seçilen katılımcılarla sınırlıdır, bu da halka açık blockchainlere kıyasla şeffaflık eksikliği konusunda endişelere yol açmaktadır. Bu sınırlama, ödeme sistemlerinde kullanıcı güvenine ve açıklığa öncelik veren oyun geliştirme platformları için kritik bir faktördür. Sınırlı erişim, ayrıcalıklı bir algı yaratabilir ve geliştiricilerin ve oyuncuların daha geniş katılımını engelleyebilir.

Buna karşın, halka açık blockchainler, izinli olmayan doğasıyla merkeziyetsiz yönetim sunmaktadır. Ancak yazarlar, bu sistemlerin oyun geliştirme gibi hızlı tempolu ortamlarda gerekli olan ölçeklenebilirlik ve hızla ilgili zorluklarla karşılaştığını belirtmektedir. Halka açık blockchainlerin sınırlı ölçeklenebilirliği, hızlı işlem işleme gerektiren ödeme sistemlerinin etkinliğini engelleyebilir.

Makale, özel blockchainlerin daha iyi verimlilik ve ölçeklenebilirlik sunduğunu vurgulamaktadır, çünkü erişimleri sınırlıdır. Bu özellik, kontrol edilmiş bir ortamda hızlı ve güvenilir işlemler sağlamak isteyen oyun geliştirme platformları için avantajlı olabilir. Ancak, bunun bir dezavantajı olarak şeffaflık azalabilir, bu da ödeme sisteminin güvenilirliğine ilişkin kullanıcı güvenini etkileyebilir.

Makale, blockchain güvenliğinin önemini vurgulayarak, yetkisiz erişim ve veri ihlallerine karşı koruma sağlayan stratejiler üzerinde durmaktadır. Temel odak alanları arasında bütünlük, gizlilik ve ağ kullanılabilirliği yer almakta olup, bu unsurlar, ödeme sistemlerinde kullanıcı güvenliğini sürdürmek için kritik öneme sahiptir. Yazarlar, blockchain teknolojisinin, bilgi etkileşimlerini korumak için merkeziyetsiz işlemler, konsensüs mekanizmaları ve değiştirilemezlik gibi özellikleri kullandığını belirterek, bu özelliklerin oyun geliştirme platformlarındaki ödeme sistemlerinin güvenliğini sağlamak adına önemli olduğunu vurgulamaktadır. [6]

M. Lewis ve C. Crawford tarafından 2024 yılında yazılan "Architectural Design for Secure Smart Contract Development" başlıklı makale, özellikle akıllı sözleşmelerdeki kritik güvenlik açıklarına odaklanarak blockchain altyapılarındaki önemli zayıflıkları ele almaktadır. Yazarlar, blockchain teknolojisinin finans ve sağlık gibi çeşitli

sektörlerde giderek daha fazla kullanılmasına dikkat çekerken, bu benimsemenin önemli güvenlik ihlalleri ile gölgelendiğini vurgulamaktadır. Makale, DAO saldırısı, bZx saldırıları ve Parity Multisignature Cüzdan Çift Saldırısı gibi yüksek profilli saldırıları inceleyerek, bu olayların önemli finansal kayıplara ve hassas bilgilerin ifşasına yol açtığını belirtmektedir.

Yazarlar, blockchain sistemlerinde iletilen hassas bilgilerin kapsamlı bir incelemesini yaparak, güçlü güvenlik önlemlerinin gerekliliğini vurgulamaktadır. Akıllı sözleşmelerdeki yaygın yazılım güvenlik açıklarının analizleri, blockchain teknolojilerine duyulan güvensizliğe yol açan sistematik zayıflıkları ortaya koymaktadır. Bu eleştirel değerlendirme, özellikle oyun endüstrisinde blockchain tabanlı ödeme sistemlerinin entegrasyonu kullanıcı deneyimini iyileştirebilse de, düzgün yönetilmediği takdirde ciddi güvenlik riskleri taşıdığı için geliştiriciler için son derece önemlidir.

Lewis ve Crawford, akıllı sözleşme geliştirme için güvenlik standartlarını iyileştirmeye yönelik kapsamlı bir model önerir. Bu model, blockchain teknolojilerinin daha geniş bir şekilde benimsenmesi için son kullanıcılar arasında güven tesis etmeyi amaçlamaktadır. Akıllı sözleşme geliştirme sürecini detaylandırarak ve potansiyel tuzakları tanımlayarak, yazarlar daha güvenli blockchain uygulamaları oluşturmak isteyen geliştiriciler için değerli bir çerçeve sunmaktadır. [7]

Sally M. Gainsbury ve Alex Blaszczynski tarafından 2017 yılında yayımlanan "How blockchain and cryptocurrency technology could revolutionize online gambling" başlıklı makale, blockchain teknolojisinin çevrimiçi kumar alanındaki potansiyelini kapsamlı bir şekilde ele almaktadır. Makalenin ana fikri, blockchain protokollerinin, kalıcı kayıtları güvenli bir şekilde saklama kapasitesi, kısmi anonimlik sağlarken aynı zamanda işlem ve veri şeffaflığı ve doğrulaması sunması gibi avantajları üzerinde yoğunlaşmaktadır.

Yazarlar, blockchainin, bilgisayar gücünü kullanarak bir olayın gerçekleştiğini doğrulayan dağıtılmış bir ağ üzerinde güvenli bir şekilde çalıştığını vurgulamaktadır. Bu yapı, çevrimiçi kumarın en büyük sorunlarından biri olan güven eksikliğini ele alma potansiyeline sahiptir. Makaleye göre, güven eksikliği, çevrimiçi kumarın en büyük dezavantajlarından biri olarak tarihsel olarak öne çıkmaktadır ve bu durum, insanların çevrimiçi kumar oynamaktan kaçınmalarına neden olmaktadır. Bu

bağlamda, yazarlar, güvenli işlemleri garanti altına alacak ve riskleri azaltacak mekanizmaların kurulmasının gerekliliğini belirtmektedir.[8]

Blockchain teknolojisi, merkezi olmayan bir defter olarak tanımlanmakta ve bu sayede üçüncü taraf aracılara olan bağımlılığı ortadan kaldırarak, açık, güvenilir ve şeffaf işlemler gerçekleştirilmesine olanak tanımaktadır. Akıllı sözleşmeler aracılığıyla, kullanıcılar arasında doğrudan ve güvenli işlemler yapılması mümkün hale gelmektedir. Bu durum, çevrimiçi kumar platformlarının daha güvenli hale gelmesini sağlayarak, kullanıcıların güven duygusunu artırabilir. Ancak, makalenin ele aldığı bazı noktalar eleştirel bir değerlendirme gerektirmektedir.

Öncelikle, blockchain teknolojisinin uygulanabilirliğinin yanı sıra, bu teknolojinin benimsenmesinin önündeki potansiyel engellerin de dikkate alınması önemlidir. Örneğin, kullanıcıların teknolojiyi anlaması ve benimsemesi, güvenlik endişeleri ve yasal düzenlemeler gibi faktörler, bu sistemlerin etkinliğini etkileyebilir. Ayrıca, blockchain teknolojisinin sunduğu güvenlik avantajları ile birlikte, siber saldırılara karşı ne kadar dayanıklı olduğu konusunda daha fazla araştırmaya ihtiyaç vardır.[9]

W Yang, S Garg, A Raza, DP Herbert ve BH Kang tarafından 2018 yılında yayımlanan "Blockchain: trends and future" başlıklı makale, blockchain teknolojisinin güvenliğini ve veri dağıtımındaki rolünü kapsamlı bir şekilde ele almaktadır. Yazarlar, blockchainin, güvenilir bir varlık olmadan işlemlerin güvenli bir şekilde dağıtılmasını sağlama yeteneği ile dikkat çektiğini belirtmektedir. Bu özellik, günümüz internetinin karşılaştığı güvenlik ve gizlilik sorunlarının çözümünde blockchain teknolojisinin potansiyelini ortaya koymaktadır.

Makalenin ana fikri, blockchainin veri geçerliliğini takip etme kabiliyeti ve merkezi bir otoriteye ihtiyaç duymadan işlemleri doğrulama yeteneğidir. Yazarlar, Bitcoin gibi merkeziyetsiz para birimlerinin, her bir işlemi merkeziyetsiz bir biçimde doğrulayarak kaydettiğini ifade etmektedir. Bu durum, oyunlarda blockchain tabanlı ödeme sistemlerinin güvenliğini artırma potansiyelini göstermektedir. Oyun içi işlemlerde, kullanıcıların güvenliğini sağlamak için blockchainin sunduğu şifreleme ve dağıtım özellikleri oldukça değerlidir.

Makalenin ele aldığı konular, blockchain teknolojisinin güvenlik ve gizlilik özelliklerinin yanı sıra, dağıtık defterlerin, güven ve gizlilik sorunlarını nasıl hafifletebileceği üzerinde durmaktadır. Ancak, makalede blockchain teknolojisinin

sınırlamaları ve potansiyel zayıflıkları hakkında daha fazla bilgi verilmesi, okuyucuların bu teknolojiye dair daha kapsamlı bir anlayış geliştirmesine yardımcı olabilir. Ayrıca, oyun endüstrisindeki spesifik uygulamalara dair örneklerin verilmesi, okuyucuların bu konudaki pratik etkileri daha iyi kavramalarına olanak tanıyabilir. [10]

PJ Taylor, T Dargahi, A Dehghantanha, RM Parizi ve KKR Choo tarafından 2020 yılında yayımlanan "A systematic literature review of blockchain cyber security" başlıklı makale, blockchain teknolojisinin siber güvenlik alanındaki uygulamalarını sistematik bir şekilde incelemektedir. Makale, blockchainin güvenliğini artırmak amacıyla yapılan akademik çalışmaları derleyerek, bu alandaki mevcut literatürü kapsamlı bir şekilde analiz etmektedir.

Makalenin ana fikri, blockchain teknolojisinin güvenli, merkeziyetsiz ve güvenilir işlemler sağlama kapasitesidir. Özellikle, Bitcoin blockchainin 2008'de tanıtılmasından bu yana, çeşitli kamuya açık ve özel erişim sağlayan blockchain sistemlerinin ortaya çıktığına değinilmektedir. Bu sistemlerin artışı, blockchainin dünya genelindeki popülaritesini artırmış ve finansal saldırılar ile yasadışı karanlık ağ pazarlarının yayılmasına zemin hazırlamıştır. Bu bağlamda, makale, blockchainin sunduğu "güvenilmez katılımcılar arasında güvenilir işlemler" gerçekleştirme yeteneğinin, farklı endüstriler tarafından nasıl değerlendirildiğini göstermektedir.

Makale, blockchain teknolojisinin siber güvenlik uygulamaları için sunduğu fırsatları ve zorlukları ele alırken, aynı zamanda güvenli ve merkeziyetsiz uygulamaların geliştirilmesi için gereken temel unsurları da vurgulamaktadır. Özellikle, blockchainin merkeziyetsiz uygulamalar için bir temel oluşturabileceği ve internet güvenliği altyapılarının anahtar unsurlarını destekleyebileceği ifade edilmektedir. Bu durum, oyunlarda blockchain tabanlı ödeme sistemlerinin güvenliği açısından kritik bir öneme sahiptir. Çünkü oyun endüstrisi, kullanıcıların güvenliğini sağlamak ve dolandırıcılık gibi siber tehditlere karşı koruma sağlamak amacıyla blockchain teknolojisinden yararlanabilir.

Blockchain teknolojisi, çeşitli endüstrileri devrim niteliğinde dönüştürme potansiyeline sahipken, bu teknolojinin sunduğu merkeziyetsiz yapının sağladığı şeffaflık, değişmezlik ve güvenlik gibi avantajlar, aynı zamanda çeşitli zorlukları da beraberinde getirmektedir. [11]

Bilash Saha ve diğer yazarlar tarafından 2023 yılında kaleme alınan "Protecting the Decentralized Future: An Exploration of Common Blockchain Attacks and their Countermeasures" adlı makalede, blockchain ağlarının maruz kaldığı çeşitli saldırılar ve bunların güvenlik üzerindeki etkileri detaylı bir şekilde ele alınmaktadır.

Makalede, blockchain sistemlerinin 51 saldırıları, çift harcama saldırıları ve akıllı sözleşme zafiyetleri gibi çeşitli saldırılara karşı ne kadar savunmasız olduğu vurgulanmaktadır. Örneğin, Ethereum Classic'in maruz kaldığı çok sayıda çift harcama saldırısının sonucunda 6.7 milyon dolardan fazla bir kayıp yaşanmıştır. Ayrıca, Poly Network'ün akıllı sözleşmesine yapılan bir saldırıda 611 milyon dolarlık kripto para çalınmıştır. Bu tür olaylar, blockchain sistemlerinin siber saldırılara karşı ne kadar açık olduğunu göstermektedir. Özellikle, Binance gibi büyük kripto para borsalarının da saldırılara maruz kalması, bu teknolojinin güvenlik açıklarının ciddiyetini ortaya koymaktadır [12].

Makalede, blockchain teknolojisinin yaygınlaşmasıyla birlikte bu tür saldırıların anlaşılmasının ve önlenmesinin önemine vurgu yapılmaktadır. Yazarlar, kötü niyetli faaliyetlerin analizinin, güvenlik endişelerine yanıt vermek için pratikteki uygulayıcılara yardımcı olabileceğini belirtmektedir. Bu bağlamda, blockchain tabanlı ödeme sistemlerinin güvenliği için, saldırı türlerinin ve bu saldırılara karşı alınabilecek önlemlerin detaylı bir şekilde incelenmesi gerekmektedir. [13]

İbrahim Halil Efendioğlu ve arkadaşları tarafından gerçekleştirilen "The Mediating Effect of Blockchain Technology on the Cryptocurrency Purchase Intention" başlıklı çalışma, kripto para satın alma niyetinde blockchain teknolojisinin rolünü incelemektedir. Çalışmanın temelinde, merkezi bir otoriteye ihtiyaç duymayan ve blockchain altyapısı ile güvenli dijital varlık transferlerine olanak tanıyan kripto paraların artan popüleritesi yatmaktadır. Ancak, tüketicilerin bu teknolojiyi nasıl algıladığı ve satın alma sürecindeki etkileri henüz tam olarak anlaşılmamıştır.

Araştırma, algılanan kullanım kolaylığı ve faydanın, müşteri hizmetleri, düşük maliyetler, verimlilik ve güvenlik gibi faktörler üzerindeki etkilerini incelemektedir. Elde edilen bulgular, algılanan kullanım kolaylığının ve faydanın, satın alma niyetini artırmada aracılık ettiğini göstermektedir. Bu durum, oyunlarda blockchain tabanlı ödeme sistemlerinin güvenliği açısından önemli bir perspektif sunmaktadır. Zira,

kullanıcıların kripto paraları kullanma konusundaki algıları, bu sistemlerin benimsenmesi ve güvenilirliği üzerinde doğrudan etkili olabilir.

Çalışmada kullanılan SPSS Process Macro programları ile elde edilen veriler, blockchain teknolojisinin sağladığı güvenliğin ve düşük maliyetlerin, kullanıcıların satın alma niyetlerini artırdığına işaret etmektedir. Bu bulgular, oyun endüstrisinde blockchain tabanlı ödeme sistemlerinin güvenliğinin artırılmasına yönelik stratejilerin geliştirilmesi için önemli bir temel oluşturmaktadır. Özellikle, oyun içi satın alımlarda kullanıcıların güvenlik algıları ve kullanım kolaylığına verdikleri önem, bu sistemlerin başarısını doğrudan etkileyebilir.[14]

Myles Lewis ve Chris Crawford'un 2024 yılında yayımlanan "Architectural Design for Secure Smart Contract Development" başlıklı makalesi, blockchain sistemlerinde akıllı sözleşmelerin güvenliği üzerine önemli bilgiler sunmaktadır. Makale, blockchain sistemlerinin mevcut akıllı sözleşme güvenlik araçlarını kullanarak gelecekteki blockchain geliştirmeleri için kavramsal bir güvenlik protokolü tasarımı oluşturabileceğini vurgulamaktadır. Bu bağlamda, güvenlik protokollerinin yazılım güvenlik standartlarının belirlenmesinde kritik bir rol oynadığına dikkat çekilmektedir.

Makalenin temel noktalarından biri, güvenli bir akıllı sözleşme inşa etmenin, sağlam yazılım mühendisliği ilkelerine dayalı dikkatli bir tasarım ve uygulama süreci gerektirdiğidir. Ayrıca, akıllı sözleşmelerin, blockchain ağında dağıtılmadan önce potansiyel zayıflıklar açısından kapsamlı bir şekilde test edilmesi gerektiği belirtilmektedir. Bu, kullanıcıların akıllı sözleşmelere olan güvenini artırmak için hayati öneme sahiptir. Makalede, blockchain bileşenleriyle ilgili sorunların (konsensüs algoritmaları, kriptografi, kamu defterleri gibi) saldırganların ağı hedef alması için gerekli bilgileri sağlayabileceği ifade edilmektedir.

Blockchain platformunun güvenliğinin, akıllı sözleşmelerin güvenliğine katkıda bulunduğu vurgulanmaktadır. Eğer blockchain ağı kendisi güvenli değilse, bu durum, o ağda çalışan akıllı sözleşmelerin tehlikeye girmesini kolaylaştırabilir. Akıllı sözleşmelerin güvenli ve değiştirilemez bir şekilde yürütülmemesi, kullanıcıların bu sözleşmeleri kullanma konusundaki isteksizliklerini artırabilir ve bu da sözleşmelerin faydasını ve benimsenmesini sınırlayabilir. Bu nedenle, blockchain ağlarının güvenliği önceliklendirmesi gerektiği, böylece o ağlarda çalışan akıllı sözleşmelerin bütünlüğü ve güvenilirliğinin sağlanabileceği sonucuna varılmaktadır.[15]

Oyunlarda blockchain tabanlı ödeme sistemlerinin güvenliği üzerine yapılan literatür taraması; yapılan çalışmaların çoğu son 10, özellikle 5 sene içerisinde yapmışmış olduğunu göstermektedir. Bunun ana sebebi, blokchain teknolojisinin günümüzde önemli bir yer kazanmış olması sebebiyledir. Yalnızca oyun odağında olmamakla beraber bir çok alanda, Finans Teknolojileri, sağlık, mobil uygulamalar gibi, kullanım alanları oluşmaktadır.

Bu teknolojinin sağladığı yenilikçi avantajların yanı sıra karşılaştığı zorlukları kapsamlı bir şekilde incelemektedir. Blockchain'in sunduğu kalıcı kayıtlar, anonimlik ve şeffaflık gibi özellikler, online kumar ve diğer işlemlerde güvenli işlemler sağlama potansiyelini artırmaktadır. Bununla birlikte, blockchain sistemlerinin güvenliği, farklı saldırı türleri ve bunlara karşı alınabilecek önlemlerle doğrudan ilişkilidir. Merkeziyetsiz yapısıyla güvenliği öne çıkmaktadır fakat kullanıcı taraflı, şüpheler tam olarak giderilememiştir

Bu çalışmada, bir oyun platformu örneklenerek, Solana ağı tabanlı bir ödeme sisteminin tasarlanması, ödeme işlemlerinin güvenli bir şekilde gerçekleştirilmesi ve sistemin güvenlik unsurları ele alınarak incelenmesi amaçlanmaktadır.



3. TEMEL TANIMLAR

3.1. Web 2 & Web 3

3.1.1. Web 2.0

Web 2.0 terimi, internet uygulamaları ve web gelişimi için kullanılan bir terimdir. Bu teknoloji, kullanıcıların içerik oluşturmalarını, düzenlemelerini ve paylaşmasını sağlamak için tasarlanmıştır. Ayrıca etkileşimli web siteleri, bloglar, sosyal medya platformları ve wikiler gibi örnekler de bulunmaktadır. Web 2.0 teknolojileri, internetin statik yapısını aşarak kullanıcıların daha aktif bir rol oynamasına imkan tanımaktadır.

Web 2.0'ın temel özelliklerinden biri kullanıcı odaklı içeriktir. Bu teknoloji, aynı zamanda zengin internet uygulamaları, veri odaklı servisler, kullanıcı deneyimini geliştiren web arayüzleri ve kolay paylaşılabilir içerik gibi özelliklere sahiptir. Ayrıca Web 2.0, web tabanlı yazılım uygulamalarının gelişimine de olanak tanımaktadır.

Web 2.0 teknolojilerinin örnek platformları arasında Facebook, Twitter, YouTube, Wikipedia ve Blogger gibi popüler sosyal medya ve içerik paylaşım siteleri bulunmaktadır. Bu platformlar, kullanıcıların içerik oluşturmalarına, düzenlemesine ve paylaşmasına imkan tanımakla birlikte, farklı etkileşim ve işlevsellik özellikleri sunmaktadır.

3.1.2. Web 3.0

Web 3.0, internetin evriminin bir sonraki aşamasını temsil eder. Bu aşama, internetin mevcut durumunun ötesine geçerek daha akıllı, daha bağlantılı ve kullanıcı odaklı bir deneyim sunmayı hedefler. Web 3.0'ın temel özelliği, verilerin anlamlı bir şekilde ilişkilendirilmesi ve anlamlı bir biçimde işlenmesidir. Bu sayede internet, insanlar arası etkileşim ve bilgi alışverişi konusunda daha etkili olacaktır.

Web 3.0'ın temel özellikleri arasında semantik web, yapay zeka, makine öğrenmesi, blockchain teknolojisi ve nesnelerin interneti gibi konseptler bulunmaktadır. Semantik web, verilerin anlamlı ilişkilendirilmesini ve anlamlı biçimde işlenmesini sağlayarak bilgi ve içerik erişimini kolaylaştırır. Yapay zeka ve makine öğrenmesi ise internet

deneyimini kişiselleştirme ve optimize etme konusunda önemli rol oynar. Blockchain teknolojisi ise veri güvenliği ve bütünlüğü konusunda çığır açan bir gelişmedir.

Web 3.0 kavramı, farklı uzmanlar ve kuruluşlar tarafından çeşitli şekillerde tanımlanmıştır. Kimi tanımlara göre, Web 3.0, bireylerin veri üzerindeki kontrolünü artıran bir yapının oluşumunu ifade ederken, kimilerine göre ise daha entegre, daha akıllı ve daha bağlantılı bir internet deneyimini temsil eder. Bu farklı tanımlar, Web 3.0'ın geniş ve çeşitli bir kavram olduğunu gösterir.[16]

3.1.3. Web 2.0'dan Web 3.0'a geçiş süreci

Web 2.0'dan Web 3.0'a geçiş süreci, teknoloji dünyasında büyük bir dönüşümü beraberinde getirmektedir. Bu süreç, nesnelerin interneti, yapay zeka, büyük veri analizi, blockchain gibi yeni teknolojik gelişmelerin entegrasyonunu içermektedir. Web 3.0'ın temelini oluşturan bu teknolojik ilerlemeler, internetin daha akıllı, kişiselleştirilmiş ve etkileşimli bir deneyim sunmasını sağlayacaktır. Bu bağlamda, Web 3.0'a geçiş süreci, mevcut web altyapısının dönüşümünü ve yeni teknolojilere adapte olma sürecini ifade etmektedir.

Web 3.0'a geçiş sürecinde yaşanan teknolojik gelişmeler ve inovasyonlar, internetin geleceğini şekillendirecek önemli faktörlerden biridir. Nesnelerin interneti (IoT), yapay zeka, makine öğrenmesi, dağıtık hesaplama sistemleri gibi yenilikler, Web 3.0'ın altyapısını oluşturmaktadır. Ayrıca blockchain teknolojisinin güvenilir veri depolama ve transferi konusundaki potansiyeli, Web 3.0'ın temel teknolojik gelişmelerinden biridir. Bu inovasyonlar, internetin daha verimli, güvenli ve kullanıcı odaklı hale gelmesine olanak sağlayacaktır.[17]

3.2. Oyun Geliştirme Platformları

3.2.1. PC ve konsol oyun platformları

PC ve konsol oyun platformları, bilgisayarlar ve oyun konsolları için oyun geliştirmek isteyen geliştiricilere hizmet veren platformlardır. Bu platformlar genellikle geliştirme araçları, dağıtım ve satış hizmetleri, oyun motorları ve altyapı desteği gibi çeşitli hizmetler sunmakta ve konsol oyun platformları, geliştiricilere oyunlarını farklı platformlarda piyasaya sürmeleri için gereken destek sağlamaktadır.

3.2.2. Mobil oyun platformları

Mobil oyun platformları, akıllı telefonlar ve tabletler gibi mobil cihazlar için oyun geliştirmek isteyen geliştiricilere hizmet veren platformlardır. Bu platformlar genellikle mobil oyun geliştirme araçları, pazarlama ve dağıtım hizmetleri, analiz ve geri bildirim araçları gibi çeşitli hizmetler sunmaktadır. Mobil oyun platformları, geliştiricilere oyunlarını başarılı bir şekilde piyasaya sürmeleri için gereken altyapıyı sağlamaktadır.

3.2.3. Web tabanlı oyunlar

Web tabanlı oyunlar, internet tarayıcıları üzerinden oynanan oyunlardır ve genellikle mobil cihazlardan da erişilebilir olmaktadır. Bu tür oyunlar genellikle web tarayıcıları için optimize edilmiş oyunlar olduğundan, oyun geliştirme platformları da genellikle web teknolojileri ve çeşitli tarayıcılarla uyumluluk gibi konularda destek sağlamaktadır. Web tabanlı oyunlar, genellikle kolay erişilebilirlik ve paylaşılabirlik gibi avantajlar sunmaktadır. Fakat saldırılara karşı diğer platformlara nazaran daha savunmasızdır.

3.3. Blockchain Teknolojisi

3.3.1. Blockchain tarihi ve evrimi

Blockchain teknolojisinin gelişimi, 2008 yılında Satoshi Nakamoto'nun kaleme aldığı Bitcoin makalesiyle başlamıştır. Bu makale, dağıtılmış defter tutma sisteminin ilk temellerini atmış ve teknolojinin seyrini değiştirmiştir. 2017 yılına kadar genelde kripto para birimleriyle özdeşleşen blockchain, son yıllarda farklı sektörlerde de kendine yer bulmaya başlamıştır. Bu evrim, teknolojinin nasıl bir yolculuk yaptığını ve her aşamada hangi yeniliklerin ortaya çıktığını gözler önüne sermektedir. Blockchain'in büyüme süreci, potansiyelini keşfetmek isteyenler için çeşitli fırsatlar sunmaktadır.

Blockchain terimi, 1991 yılında Stuart Haber ve W. Scott Stornetta'nın öncülüğünde hayat bulmuştur. Ancak bu teknolojinin gerçek anlamda tanınması, Satoshi Nakamoto'nun 2008 yılında sunduğu Bitcoin makalesi ile mümkün olmuştur. Burada, blokların bir zincir şeklinde birbirine bağlı olduğu bir yapıdan bahsedilmektedir. Bu kavram, blockchain teknolojisinin temelini oluşturan ve dağıtık defter sisteminin

işleyişini ortaya koyan bir göstergedir. Blockchainin sunduğu bu yapı, veri güvenliğini ve şeffaflığı artırma potansiyeli ile dikkat çekmektedir. Ancak, bu potansiyelin tam anlamıyla gerçekleşebilmesi için daha fazla güven ortamının oluşturulması gerekmektedir. Bu nedenle, blockchain dünyası, kendini sürekli olarak geliştirmeye ve bu alandaki olumsuz algıları aşmaya çalışmaktadır. [18]

3.3.2. Blockchain türleri ve protokolleri

Blockchain teknolojisi, hayatımızın birçok alanında kendine yer bulma çabası içerisinde. Bu alanlardan ilki, herkesin erişimine açık olan kamu blockchainleridir; merkeziyetsiz yapıları sayesinde şeffaflık ve güvenilirlik sunarak önemli fırsatlar yaratmaktadır. Özel blockchainler ise, belirli bireyler veya kuruluşlar için tasarlanmış, erişim kısıtlamaları barındıran daha kapalı bir yapı sunmaktadır. Bu tür sistemler, gizlilik ve kontrol arayışında olanlar için ideal bir çözüm imkanı tanımaktadır. Diğer yandan, konsorsiyum blockchainleri, belirli bir grup tarafından yönetilmekte olup, bu grubun ihtiyaçlarına göre şekillendirilen bir yapıya sahiptir. Her bir blockchain türünün kendine has avantajları ve dezavantajları mevcut olsa da, her biri farklı ihtiyaçlar ve kullanım senaryoları doğrultusunda tercih edilmektedir. Bu çeşitlilik, teknolojiye olan ilgiyi artırmakta ve uygulama alanlarının genişlemesine olanak sağlamaktadır.

3.3.2.1. Blockchain türleri

Kamu blockchainleri

Kamu blockchainlerinin yapısına bakıldığında, merkeziyetsiz bir sistemin sunduğu avantajları görmekteyiz. Bu tür platformlar, Bitcoin gibi kripto paraların güvenli bir şekilde işlem gördüğü alanlar olarak geniş bir kullanım alanına sahiptir. Merkezi bir otoritenin yokluğu, veri manipülasyonu endişelerini azaltsa da, şeffaflık açısından önemli bir ortam oluşturmaktadır. Ancak, bu durum bazen güven eksikliği yaratabilmektedir. Kullanıcılar, sistemin merkeziyetsiz doğasında var olan riskler nedeniyle, dikkatli olmak zorundadır. Blockchain teknolojisi, sunduğu güvenlik unsurlarıyla, zamanla daha fazla benimsenme potansiyeline sahiptir.

Özel blockchainler

Özel blockchainler, belirli kişi veya kurumların erişimine açık olan ve genellikle merkezi bir yapıya sahip olan blockchain türüdür. Finans kurumları veya şirketlerin iç

işlemlerini yönetmek için kullanılan özel blockchainler, katılımcıların belirlendiği ve erişim haklarının sınırlandırıldığı özel ağlar oluşturabilmektedir. Bu sayede, güvenlik ve gizlilik odaklı kullanım senaryolarına uygun çözümler sunmaktadır.

Konsorsiyum blockchainleri

Konsorsiyum blockchainlerinin özelliklerine bakıldığında, belirli bir grup tarafından oluşturulmuş ve bu grup tarafından yönetilen bir yapı ile karşılaşmaktayız. Bu yapılar, çeşitli paydaşların ortak bir platform oluşturmasını sağlayarak, belirli bir sektörde veya endüstride iş birliğini teşvik etmektedir. Özellikle finans, lojistik ve tedarik zinciri yönetimi gibi alanlarda bu tür blockchainlerin kullanımı giderek yaygınlaşmaktadır; çünkü bu sektörlerde iş birliği ve veri paylaşımı, gün geçtikçe daha da kritik bir hale gelmektedir. Ancak bu gelişmelerin yanı sıra, paydaşların güvenini sağlamanın da önemli bir unsur olduğu unutulmamalıdır.

3.3.2.2. Blockchain protokolleri

İş kanıtı (proof of work)

İş kanıtları (Proof of Work), blockchain protokollerinin güvenliğini sağlamak için kullanılan bir mekanizmadır. Bu mekanizma, madencilerin kriptografik işlem gücünü kullanarak blokları onaylamasını ve zincire eklemesini sağlar. Bu süreçte, madencilerin yoğun bir hesaplama gücüne ihtiyaç duyması ve bu işlemi gerçekleştirirken enerji tüketimi yüksek olması, blockchain sisteminin güvenliğini artırır. Ancak, bu durum çevresel etkiye neden olduğu için günümüzde çevreci alternatifler araştırılmaktadır.

İş ispatları (proof of stake)

İş ispatları (Proof of Stake), blockchain protokollerinin güvenliğini sağlamak için kullanılan bir diğer mekanizmadır. Bu mekanizma, katılımcıların sahip oldukları kripto paraya göre blokları onaylayarak zincire eklemesini sağlar. Bu sayede, enerji tüketimi azalır ve çevre dostu bir yaklaşım benimsenmiş olur. Ayrıca, iş ispatları mekanizması sayesinde, blokları onaylamak için yüksek hesaplama gücüne ihtiyaç duymadan katılımcılar arasında adaletli bir seçim yapılır ve blockchain ağının güvenliği korunmuş olur.[19]

3.3.3. Blockchain çalışma mantığı ve bileşenleri

Blockchain teknolojisi, verilerin değişmezliğini sağlamak için kriptografik güvenlik kullanan yenilikçi bir dağıtılmış defter teknolojisidir. Basitçe bir blockchainin veri içeren ve kriptografik bir hash ile tanımlanan bir bloklar zinciri olduğu söylenebilir. Uygulanan teknoloji hakkında bir şeyler söyler çünkü tasarım mevcut bloğu önceki ve sonraki bloklarla ilişkilendirir. Her blok bir önceki bloğun kriptografik bir karmasını, bir zaman damgasını ve işlem verilerini içerir. Kriptografik bir hash üretmek için blockchain, bloğun ham verilerini sabit uzunlukta dijital dizelere dönüştürmek için karmaşık algoritmalar kullanır. Bloкта herhangi bir değişiklik yapılırsa, orijinal bloğun kriptografik hash'ini etkiler ve kripto para birimi ağı boyunca tutarsızlıklar yaratır. Bu nedenle, doğrulandıktan sonra zinciri tersine çevirmek veya bloğun herhangi bir unsurunu değiştirmek neredeyse imkansızdır ve sistemin güvenliğini ve bütünlüğünü sağlar. Şu anda dünyamız, bankalar ve özel işletmeler gibi sunucular üzerinde çalışan merkezi sistemler aracılığıyla işlemektedir. Merkezi sistemler, blockchaini teknolojisinin temel yönlerinden biridir. Merkezi bir sunucu yoktur ve tüm veriler ağ üzerinde sonsuza kadar saklanacaktır. Her şeyi denetleyen bir şirket olmadığından, sistem eşit haklara ve söz hakkına sahip belirli bir grup insan içinde çalışacaktır - bu insanlar genellikle 'düğümler' olarak adlandırılır.

Blokchaini terimi, işlemlerin veya dijital verilerin kaydedildiği ve kamuya açık veya özel olarak doğrulandığı ve zincire kalıcı olarak eklendiği bu yapıdan kaynaklanmaktadır. Düğümler ağ için son derece önemlidir çünkü esasen blockchainin verilerinin bekçileridirler. Blockchainin çalışmasına ve bütünlüğünü korumasına yardımcı olan değerli verileri tutarlar. Halka açık blockchainleri, özel blockchainleri ve konsorsiyum blockchainleri de dahil olmak üzere farklı blockchain türleri de vardır.

Herkese açık blockchainleri açık kaynaklı ağlardır ve merkezi değildir; bu nedenle, işlemleri doğrulamak için birkaç katılımcı arasında fikir birliği gerektirirler. Blockchaini teknolojileri, çeşitli endüstrilerdeki ve devlet faaliyetlerindeki çeşitli rolleri görev bilinciyle dönüştürebilir veya yenilerini yaratabilir. [20]

3.3.3.1. Blockchain yapısı ve işleyişi

Blockchain yapısının, merkeziyetsiz bir ağ içerisinde nasıl bir dağıtık defter işlevi gördüğünü anlamak mümkündür. Bu ağ içerisinde yer alan tüm bilgiler, bloklar

halinde düzenlenmekte ve her bir blok, kendisinden önceki bloğun kriptografik bir özeti olan hash değerini taşımaktadır. Her yeni blok eklendikçe, önceki bloklarla bağlantılı bir zincir oluşturmaktadır ve bu süreç ile blokların güvenilirliği sağlanmaktadır. Bu nedenle, her bireyin erişim sağlayabileceği ve gözlemleyebileceği bu yapı, blockchain'in güvenilirlik ve şeffaflık açısından dikkate değer olma özelliğini taşımaktadır. Sonuç olarak, bu yenilikçi teknoloji, veri güvenliği ve bütünlüğü konularında devrim niteliğinde bir yaklaşım sunmakta ve birçok sektörde kullanılmakta olan umut verici bir çözüm olarak öne çıkmaktadır. Blockchainindeki bir blok, blok başlığı ve blok gövdesi olmak üzere iki ana bölümden oluşur.

Blok başlığı

Blok başlığı, meta veriler ve bloğa özgü bilgileri içerir. Önceki blok karması, zincir bütünlüğünü sağlamak için hemen önceki bloğun hash değerini içerir. Bu yapı, herhangi bir işlem değişikliğinin tüm zinciri etkilemesine neden olur. Zaman damgası, bloğun oluşturulma zamanını belirtir ve geçerli olması için daha önceki blokların medyan zamanından büyük olmalıdır. Merkle kökü, blok gövdesindeki işlemlerin hash değerlerini özetler ve işlemlerdeki bir değişiklik yeni bir Merkle kökü oluşturur. Nonce ise iş kanıtı zorluğunu karşılamak için kullanılan 32 bitlik rastgele bir sayı olup, her farklı nonce değeri yeni bir blok hash'i üretir.[21]

Blok gövdesi

Blok gövdesi işlemlerin bir listesini içerir. Teknik olarak, işlemlerin yapısı üzerinde herhangi bir kısıtlama yoktur. Çoğu ana akım blockchaini sistemi, tüm işlemleri bir Merkle ağacı şeklinde birleştiren bir veri yapısı kullanır; bu, ağaç için bir kök hash üretilinceye kadar alt düğümlerin tekrar tekrar hashlenmesiyle oluşturulan ikili bir ağaçtır. Böylece bir işlemler ağı, bir blokta tek bir Merkle kök değeri olarak kısaca temsil edilebilir. Bir Merkle ağacı, işlemleri işlem düzeyinde düzenler ve belirli bir bireysel işlemin bloğa dahil edilip edilmediğini belirlemek için verimli bir kanıt sistemini destekler. Bir Merkle ağacının yüksekliği $\log_2 n$ 'dir, burada n işlem sayısını gösterir. Dolayısıyla, bir blok sabit ve sınırlı bir boyuta sahiptir. Bir sistem uygun bir blok boyutu seçtiğinde, işlem işleme hızı ile blok yayılımının verimliliği arasındaki ödünleşimi ele alır. [22]

Dağıtık defter teknolojisi

Bir blokchaini sistemi, işlemlerin özdeş kayıtlarını saklayan ve paylaşan, ağ genelinde durumların ortak bir görünümünü oluşturan eşler arası bir düğüm ağı olan dağıtılmış defter teknolojisinin temelleri üzerine kurulmuştur. Dağıtılmış bir defter, klasik merkezi defterin aksine, varsayılan olarak yedekli, şeffaf ve tahrifata karşı dirençlidir ve teknolojinin doğasında bulunan ademi merkeziyetçilikten yararlanan varlıklar için işlemlerin ve geçmişin denetlenebilir bir günlük kaydını sağlar. Merkezi veritabanlarında kayıtların tek başına depolanmasıyla karşılaştırıldığında, dağıtık defter teknolojisi önemli ölçüde artırılmış kullanılabilirlik, esneklik ve depolama sunarak özellikle güvene dayalı olmayan işlem senaryolarında çeşitli avantajlar sağlar. Doğal bir güven ilişkisi olmayan sistemlerde gerçekten faydalı olma potansiyeline sahiptir ve kontrollerin desteklenmesini, dolandırıcılığın azaltılmasını ve çifte harcamaların önlenmesini sağlar.

Dağıtılmış defter teknolojisi tipik olarak bir blokchaini, defterin eşler arası dağıtımında düğüm adı verilen her katılımcıyı birbirine bağlayan bir ağ üzerinde çalışan bir protokol ve özgünlük ve bütünlük doğrulaması için bir sistem içerir. Sistem, işlemleri doğrulamak için merkezi bir otoriteye ihtiyaç duymaz ve bunları kriptografik karmalar kullanarak saklar. Bu nedenle veri bloklarının ve blokchaininin oluşturulması, katılımcı düğümler arasında çoğaltılmış bir geçmişin oluşturulmasına ve paylaşılmasına dayanmaktadır. Tek bir otoritenin verileri kontrol ettiği geleneksel veri tabanlarından farklı olarak, dağıtık defter teknolojisi mutabakat algoritmaları kullanır ve her düğüm eşit katılım hakkına sahiptir. Sonuç olarak, dağıtık defter teknolojisi süreçleri güven ve güvenlik ile güçlendirmeye hizmet edebilir. Birkaç popüler kullanım örneği, insanlar arası borç verme, tarım, enerji ve finans piyasalarını içermektedir. Bu uygulamalar geleneksel sektörlerle yeni bir soluk getirmektedir. Dağıtık defter teknolojisinin kullanımı mevcut sistemlerin yeniden tasarlanması anlamına gelmektedir. Teknoloji henüz erken aşamadadır, bu nedenle birçok durumda geçiş henüz tam olarak uygulanmamıştır. [23]

Konsensüs mekanizmaları

Daha önce de belirtildiği gibi, blokchaini değişmez, dağıtılmış bir işlem defteridir. Blokchainine yeni bir blok eklenmesi söz konusu olduğunda, yeni bloğun geçerliliğinin ağ katılımcıları tarafından doğrulanması zorunludur. Ancak, tüm

katılımcıların aynı fikirde olması için, hepsinin henüz zincire eklenmemiş olan bu yeni blok hakkında aynı bilgiye sahip olması gerekir. Sonuçta, zincirdeki yeni bir blok aynı şekilde geçerli ya da geçersiz kabul edilebilir. İşte bu noktada mutabakat mekanizması devreye girer. Mutabakat mekanizması, tüm ağın tüm işlemler üzerinde doğru sırada mutabık kalmasını sağlamaktan sorumludur. Bu, olası çifte harcama saldırılarını önler. Dünya çapında çeşitli blockchaini teknolojileri tarafından kullanılan bir dizi farklı mutabakat algoritması vardır.

En iyi bilinen ve yaygın olarak kullanılan mutabakat algoritması Proof of Work'tür. Diğerleri ise Proof of Stake ve Delegated Proof of Stake'tir. Bu mutabakat algoritmalarının her birinin enerji kullanımı, merkezileşme ve güvenlik açısından kendine özgü avantajları ve dezavantajları vardır. Çeşitli mutabakat algoritmaları blockchaini performansı ve ölçeklenebilirliğinde de önemli bir rol oynamaktadır. Bu nedenle, mutabakat sağlamanın önemsiz bir mesele olmadığını kabul etmek önemlidir. Ancak, daha önce de vurgulandığı üzere, tüm blockchaini önceki işlemler üzerine inşa edilmiştir ve bu işlemler mutabakat ile doğrulanmaktadır. Dolayısıyla, böyle bir mutabakat sağlanamazsa, önceki işlemlerin doğruluğuna artık herhangi bir güven ya da itimat olamayacağından, tüm blockchaini çözülmeye başlar. Pratik, gerçek dünyadan bir örnek olarak, Bitcoin yaklaşık her 10 dakikada bir blockchainine yeni bir blok ekler. Bu yeni blokların her biri, bir Bitcoin'in çifte harcanma olasılığını sona erdirmeyi amaçlayan şiddetli bir rekabetin konusudur. [24]

3.4. Akıllı Sözleşmeler

Akıllı sözleşmeler, blockchain ağlarında otomatik olarak yürütülen ve kodlanmış kuralları içeren dijital sözleşmelerdir. Bu sözleşmeler, blockchainde yer alan taraflar arasında güvenli ve şeffaf bir şekilde işlem yapılmasını sağlar. Akıllı sözleşmeler, herhangi bir merkezi otoriteye ihtiyaç duymadan otomatik olarak çalışabilir ve taraflar arasındaki anlaşmazlıkları çözebilir. Bu nedenle, akıllı sözleşmeler blockchain teknolojisinin en önemli bileşenlerinden biridir.

Akıllı sözleşme kavramı, ilk defa 1990'larda Nick Szabo tarafından ortaya atılmıştır. Bu kavram, Ethereum blockchaini platformu sayesinde popülerlik kazanmış ve akıllı sözleşme kavramı üzerine birçok akademik çalışma ve teknolojik gelişme gerçekleştirilmiştir.[25]

3.5. Merkeziyetsizlik

Akıllı sözleşmeleri, avantajlarını ve dezavantajlarını ve olası sorunlarda akıllı sözleşmeleri değiştirmek için blokchaini kodunu yeniden yazma alternatiflerini anlamak için blokchaini teknolojisinde uygulanan ademi merkeziyetçilik kavramının tanınması gerekir. Ademi merkeziyetçilik, siyasi, ekonomik ve idari otoritenin en alt seviyelere kadar dağıtılması anlamına gelmektedir. Yetki ve kontrolün bir sistemin yapısı boyunca dağıtılmasına dayanan sosyal ve teknolojik bir paradigmayı tanımlar. Bu, teknolojinin kontrolünü ve yönetimini herkesin erişebileceği ve kullanabileceği bir temele kaydırır. Bilgisayar biliminde ademi merkeziyetçilik, kaynakların birçok bilgisayara dağıtılması anlamına gelir. Dağıtık yazılım sisteminin en yaygın alternatifi merkezileştirmedir, ancak hibrit dağıtık sistemler gibi başka paradigmlar ve alternatifler de vardır.

Merkezi olmayan sistemlerin birden fazla avantajı vardır. Çoğunlukla saldırılara karşı daha dayanıklıdır çünkü merkezsizleştirme tek bir güvenlik açığını veya tek bir kontrol noktasını ortadan kaldırır ve ağdaki düğümlerin veya bilgisayarların tamamen tehlikeye atılmasını daha zor hale getirir. Bu avantaj hizmet kalitesinin düşürülmesi durumunda da geçerlidir. Saldırılarda veya diğer olaylarda olduğu gibi, merkezi olmayan bir ağın performansını tamamen düşürmek daha zordur çünkü hizmetler ve veri sağlama tek bir ana bilgisayara bağlı değildir. Merkezi olmayan sistemlerin güvenliği artıran bir diğer özelliği de savunmasızlıktır. Ek olarak, merkezi olmayan sistemler daha güvenli olma eğilimindedir çünkü daha resmi güvenlik kanıtları ve sistemleri değerlendirmek için daha fazla gözü teşvik eden açıklık için fırsatlar sağlayarak daha açıktırlar. Merkeziyetsizliğin ana ödünleşimi ölçeklendirme zorluğudur ve en iyi durumda iletişim ek yükünde daha az verimli olduğu düşünülmektedir. Merkezi olmayan ağlarda ne kadar çok ana bilgisayar olursa, paylaşım ve senkronizasyon o kadar yavaş olacaktır. Bulutlarda bu ek yük, iletişimin Katman-2 üzerinden kısa devre yaptırılmasıyla azaltılır. Ekonomik olarak, merkeziyetsizleştirme, değeri temsil eden tokenlar sunarak faaliyetlerin paraya çevrilmesine dayalı eş ekonomisi sağlayan geçerli bir değiştirme alternatifi önermektedir. [26]

3.5.1. Akıllı sözleşmelerde merkeziyetsizlik

Blockchain teknolojisi kripto para biriminin temelidir ve merkezsizleştirmeyi ilk nokta haline getirir. Akıllı bir sözleşme, bir sözleşmeyi uygulamak yerine, insanlar arasındaki müzakere şartlarını uygulamak için bir yol sağlar. Bir sözleşme, her şey kodda olduğu için herhangi bir karmaşıklık seviyesine sahip olabilir ve bir sözleşmenin veri depolaması değişmezdir; kod blockchainine yerleştirildikten sonra kimse onu değiştiremez. Merkezi olmayan dijital sözleşmeler, ilk halka açık, izinsiz blockchaininin piyasaya sürülmesinden bu yana önemli ölçüde gelişti ve büyük ilgi gördü. Bu, bir dizi işlemin kriptografik karmalarının sıralanması için kurcalamaya karşı korumalı destek sağlar. Bununla birlikte, defterde çifte harcama olmamasına rağmen, asıl sorun sistemin kurcalamaya karşı dayanıklı olan defterlerde yanlış durumlar yapmasını önlemektir. Bu sorunları gidermek için dijital sözleşmeler araçların rolünü üstlenebilir, ancak yine de adil bir sözleşme seçmek için sözleşme destekçilerine güven duyulmasını gerektirir. Bir sözleşmeyi doğrulamak için ödeme yapılması gereken ve aynı zamanda iletişimi yavaşlatabilecek araçlar kullanmak yerine, dijital sözleşmeler doğrulama işini gerçekleştirmek için merkezi olmayan bir ağ üzerinde etkileşime girer ve önemli verileri depolar. Gerçek dünyada, merkezi olmayan sistemlere olan ilgi, web'den bile daha hızlı büyüdükleri için giderek artmaktadır. Bu bize temel katmana erişmek için üstte bir izinler katmanı olan bir sistem verir. Dijital sözleşmelerin gerçek dünyada basit bir güvenilir noterlik hizmetinden kendi kendini yönetebilen sözleşmelere kadar pek çok uygulaması olabilir. [27]

3.6. Blokchainlerde Layer Kavramı

3.6.1. Layer 1

Layer 1, bir blockchain ağının ana protokol katmanıdır. Bu katman, blockchainin temel altyapısını ve güvenliğini sağlar. Layer 1 ağları, işlemleri doğrudan işleyen, konsensüs mekanizmaları kullanarak ağın güvenliğini sağlayan katmandır. Bitcoin Blockchain Ağı, Ethereum Blockchain Ağı, Solana Blockchain Ağı, Cardano Blockchain Ağı Layer 1 ağlarındandır.

Layer 1 ağları, doğrudan işlem onayları ve blok üretimiyle güvenlik, merkeziyetsizlik ve şeffaflık sağlar; ancak ölçeklenebilirlik genellikle sınırlıdır (örneğin, Bitcoin ve Ethereum'un erken sürümlerinde).[28]

3.6.2. Layer 2

Layer 2, Layer 1 ağlarının üzerine inşa edilen, genellikle işlem hızını ve ölçeklenebilirliği artırmak amacıyla kullanılan ikinci katmandır. Layer 2, Layer 1 ağındaki işlemleri hızlandırmak ve maliyetleri düşürmek için yan zincirler, kanal tabanlı sistemler gibi farklı teknikler kullanır.

3.6.3. Layer 3

Layer 3, blockchain tabanlı uygulamaların (DApps, akıllı sözleşmeler) çalıştığı ve merkeziyetsiz finans (DeFi), oyunlar ve NFT platformları gibi endüstriyel ve ticari uygulamaları içeren uygulama katmanıdır.

3.7. Blockchain Ağları

Farklı Blockchain ağları, farklı avantaj ve dezavantajlara sahiptir. Bu kısımda; Ethereum, Bitcoin, Avalanche, Cardano, Solana ve Ripple gibi blockchain ağlarının genel özellikleri, hızları, işlem kapasiteleri ve maliyetleri üzerine bir karşılaştırma sunulmaktadır. Karşılaştırmada, her bir ağın teknik detayları objektif bir şekilde ele alınarak, bu verilere dayalı olarak analiz ve değerlendirmeler yapılmaktadır. Yöntemoloji olarak, her bir ağın performansını ve özelliklerini belirlemek için karşılaştırmalı bir analiz yöntemi kullanılmakta ve bu analizlerden bir sonuç çıkarılmaktadır.

3.7.1. Ethereum blockchain ağı

Ethereum'un genel özellikleri arasında, açık kaynak kodlu bir platform olması, akıllı sözleşmelerin ve merkezi olmayan uygulamaların geliştirilebilmesi için uygun bir ortam sunması, diğer blockchain ağları üzerinde token çıkarılabilmesine imkan vermesi gibi özellikler bulunmaktadır. Hız ve işlem kapasitesi bakımından saatte 15 işlem kapasitesine sahiptir. Bu durum Ethereum'un işlem hızını etkileyebilmektedir. Maliyet ve ücretlendirme kısmında ise işlem başına ücretlendirme sistemi kullandığı için işlem büyüklüğüne göre değişen bir ücretlendirme politikası bulunmaktadır.

3.7.2. Bitcoin blockchain ağı

Bitcoin, blockchain ağının en eski ve en bilinen üyelerinden biridir. Teknik özellikleri arasında cüzdan türleri, işlem hızı, blok boyutu, işlem maliyeti ve ücretlendirme politikası yer almaktadır. Merkeziyetsiz yapısı, kriptografik güvenliği, sınırlı arzı ve açık kaynaklı kod yapısı, ağın güvenilirlik ve güvenliği üzerinde önemli etkiler yaratmaktadır.

Bitcoin'in işlem hızı ve kapasitesi, blok boyutu ile blokların oluşturulma sıklığına bağlı olarak değişkenlik göstermektedir. Özellikle yoğun işlem dönemlerinde ağda gecikmeler yaşanabilir ve bu durum performansı olumsuz etkileyebilir.

Güvenlik ve işlem doğrulama süreçleri, Bitcoin ağı için belirli bir maliyet oluşturmaktadır. Ücretlendirme politikası ve madencilere yapılan ödüller, ağın ekonomik yapısının önemli bir parçasıdır ve kapsamlı bir şekilde değerlendirilmelidir.

3.7.3. Avalanche blockchain ağı

Avalanche, ölçeklenebilirlik, güvenlik ve esneklik gibi özellikleriyle dikkat çeken, yüksek hızlı bir blockchaini platformudur. 4500+ işlem/saniye kapasitesi ve düşük işlem onay süreleri sayesinde kullanıcıların hızlı ve verimli işlem yapmasını sağlar. Aynı zamanda düşük işlem ücretleri ve ekonomik modelleriyle kullanıcı dostu bir yapı sunarak geniş bir kullanım alanına hitap etmektedir. Karmaşık uygulamaları destekleme esnekliği ve farklı blockchaini işlemlerini bir araya getirebilme yeteneği, platformun öne çıkan özellikleri arasındadır.

3.7.4. Cardano blockchain ağı

Cardano, yüksek güvenlik, sağlamlık ve sürdürülebilirlik gibi temel özellikleriyle öne çıkan, merkeziyetsiz bir ekosistem sunan gelişmiş bir blockchaini platformudur. Ouroboros konsensüs protokolü sayesinde güvenilirlik ve dayanıklılık sağlarken, çok katmanlı yapısı paralel işlem gücüyle geniş ölçekli işlemleri hızlı ve verimli bir şekilde gerçekleştirebilir. Bu özellikler, merkezi olmayan uygulamaların etkili çalışmasına olanak tanır. Cardano, düşük maliyetli ve adil bir ücretlendirme modeliyle kullanıcılarına ekonomik bir deneyim sunar, bu da platformun kullanıcı dostu ve rekabetçi bir seçenek olmasını sağlar.

3.7.5. Solana blockchain ağı

Solana, yüksek performanslı bir blockchain ağı olup, Proof of History (Tarih Kanıtı) konsensüs mekanizmasıyla dikkat çeker. Bu yenilikçi mekanizma ve zaman damgası ekleme yeteneği, ağın hızını ve işlem verimliliğini artırır. Solana, merkeziyetsiz uygulamalar ve finans projeleri için hızlı, düşük maliyetli ve güvenli işlemler sunan açık kaynaklı bir platformdur.

Ağ, saniyede 65.000 işleme kadar yüksek bir kapasiteye sahip olmasıyla rakiplerinden ayrılır ve kullanıcılara hızlı, verimli ve ekonomik bir deneyim sunar. Ayrıca düşük işlem ücretleri ve dengeli ödül mekanizması sayesinde güvenli ve istikrarlı bir yapı sağlar. Geliştiricilere sunduğu esneklik ve ölçeklenebilirlik, Solana'nın geniş bir kullanım alanına hitap etmesini sağlar.

3.7.6. Ripple blockchain ağı

Ripple, merkezi olmayan finansal işlemler için düşük enerji tüketimi, yüksek ölçeklenebilirlik ve hızlı işlem onaylarıyla öne çıkan bir platformdur. XRP tokeni üzerine kurulu olan ağ, hızlı ve düşük maliyetli transferleri mümkün kılar. Ortalama 4 saniyelik işlem onay süresi, Ripple'ı diğer blockchain ağlarından ayıran hızlı ve verimli bir yapı sunar.

Platform, düşük işlem ücretleri ve ekonomik transfer imkanı sağlayarak kullanıcı dostu bir deneyim sunar. Merkezi olmayan yapısı, yüksek hız ve ölçeklenebilirlik özellikleriyle Ripple, hem bireysel hem kurumsal kullanıcılar için güçlü bir finansal altyapı oluşturur. [29]

3.7.7. Ağların karşılaştırılması

3.7.7.1. Hız ve ölçeklenebilirlik

Solana ve Avalanche en hızlı blockchain ağlarıdır ve yüksek TPS sayesinde çok ölçeklenebilir. Ethereum Layer 1 seviyesinde sınırlıdır ancak Layer 2 çözümleri ile ölçeklenebilirliği artırır. Bitcoin, ölçeklenebilirlikte en zayıf olanıdır, çünkü ağ tasarımı itibarıyla güvenlik ve merkeziyetsizliğe öncelik verir.

3.7.7.2. İşlem maliyeti

Ripple, neredeyse sıfıra yakın işlem maliyetleriyle uluslararası ödemelerde liderdir. Ethereum, yoğun kullanımda işlem ücretlerinin artmasıyla bilinir; bu durum, kullanıcıları Layer 2 çözümlerine yönlendirmiştir. Solana ve Avalanche düşük işlem maliyetleriyle öne çıkar. [30]

3.7.7.3. Merkeziyetsizlik ve güvenlik

Bitcoin, merkeziyetsizlik ve güvenlik açısından endüstri standardı olarak kabul edilmektedir. Cardano, Ouroboros konsensüsü ile enerji verimliliğini artırırken merkeziyetsizliği korur. Solana, yüksek hız için merkeziyetsizliği bir miktar feda ettiği eleştirisi almaktadır.

3.7.7.4. Kullanım alanları

Ethereum, DeFi ve NFT sektörlerinde en büyük ekosisteme sahiptir. Ripple, özellikle bankalar ve finansal kurumlar tarafından uluslararası ödemeler için kullanılmaktadır. Cardano ve Avalanche, yenilikçi finansal uygulamalar için geniş bir potansiyele sahiptir. Bitcoin, daha çok değer saklama aracı ve dijital altın olarak kabul edilir. [31]

3.7.7.5. Konsensüs mekanizmaları

Bitcoin'in, Proof of Work ile ,daha güvenli ancak enerji tüketimi yüksektir. Ethereum ve Cardano'nun, Proof of Stake ile, enerji verimliliği sağlanarak, ölçeklenebilirliği artırır. Avalanche, Consensusla; Solana, Proof of History ile, düşük gecikme süreleri sunar. [32]

3.8. Tokenler

3.8.1. Token nedir ve ne işe yarar?

Tokenlar, bir blokchaini ağında, ağın sunduğu hizmetlere veya ürünlere erişimi temsil eden dijital varlıklar olarak işlev görür. Blokchaini ekonomisinin temel taşlarından biri olan tokenlar, farklı fikir birliği mekanizmalarında kullanılarak blokchainlerinin varlık ve pazarlar olarak anlaşılmasını kolaylaştırır. Tokenlar, ticaret gibi çeşitli eylemler için kullanılır ve çeşitlilik sunar. Çoğu kişi token ve coin arasındaki farkları tartışsa da, genel olarak tokenlar ödemeler için, coin'ler ise alım satım işlemleri için kullanılır.

Bu ayrımın temel nedenlerinden biri, maliyet ve nadirlik gibi faktörlerin token veya coin'lerin işlem sırasında güvenliğini sağlamasıdır. Tokenların kullanım alanları her

geçen gün genişlemekte ve birçok sektör, dijital paralardan ziyade tokenları benimsemektedir. Blockchain endüstrisi, tokenları işletmelerin üretimini ve yapısını iyileştirmek için bir araç olarak geliştirmiştir.

Dijital tokenlar, merkezi olmayan pazarlar, oyunlar ve çeşitli sektörler için temel standartlar haline gelmiştir. Tokenlar, değerli varlıkların sayısallaştırılması ve dijitalleştirilmesi amacıyla kullanılmakta, bu da özellikle blockchain pazar yerlerinde önem kazanmaktadır. Ayrıca, tokenların piyasa borsalarındaki geniş kullanım alanları, blockchainlerinin farklı formlarının benimsenmesini artırmıştır.

Tokenlar, kripto paraların ilham verdiği topolojik gelişmelerle ivme kazanmış, insan odaklı projelere katılımı mümkün kılmıştır. Tüm bunlara rağmen, kripto endüstrisi hala en fazla token çeşitliliğini barındıran alan olmaya devam etmektedir. [33][34]

3.8.2. Token türleri ve kullanım alanları

Tokenler, altında yatan doğalarına ve amaçlanan kullanım alanlarına göre farklı kategorilere ayrılabilir. Ancak, tokenlerin sınıflandırılmasının kesin veya nihai olmadığını unutmamak önemlidir; teknolojideki sürekli ilerlemeler zamanla yeni türlerin ortaya çıkmasına yol açabilir. Günümüzde en yaygın olarak bahsedilen token türleri arasında hizmet (utility) tokenleri, menkul kıymet (security) tokenleri, varlık destekli (asset-backed) tokenler ve öz sermaye (equity) tokenleri yer alır. Bir blockchaini girişimi perspektifinden hangi tür tokenlerin çıkarılması gerektiğine karar verirken, projenin altında yatan teknoloji, amacı, yasal bağlamı ve kullanım alanı gibi çeşitli faktörler göz önünde bulundurulmalıdır. Aynı blockchaini projesi için birden fazla türde token kullanıldığında, bu tokenler hibrit özelliklere sahip tokenler olarak birleştirilir ve teorik olarak, bahsedilen tüm bu token türlerine topluca kullanım tokenleri (usage tokens) adı verilir.

Hizmet tokenlerinin (utility tokens) temel özelliği, birçok durumda ihraççı ile token sahipleri arasında finansal bir karşılık bulunmamasıdır. Hizmet tokenleri, geleneksel finansal işlemleri düzenleyen yasalarda açıkça tanımlanmadıkları için detaylı düzenlemelere tabi değildir. Birisi bir akıllı sözleşme yazmaya ve merkezi olmayan bir ağda yeni bir projeye ait tokenler oluşturmaya başladığında, sanal projenin yüklü rezervi teminat oluşturmak için kullanılır. Daha sonra yeni token konsepti sisteme tanıtılır ve bu tokenlere likidite sağlayan kullanıcılara coinler dağıtıldıktan sonra tokenlerin sayısı artar.[35]

3.8.2.1. Hizmet tokenleri (Utility Tokens)

Hizmet tokenleri, bir hizmete veya ürüne erişim sağlayan lisanslar olarak işlev görür. Bu şekilde, oyun oynama hakları, indirimler alma veya bir ürün ya da hizmetin kullanımına ödeme yapma gibi haklar sunarak tüketici odaklı bir amaç taşırlar. Bu tasarımın sonucunda, müşteriler verilen hizmeti diğer blokchaini dışı alternatiflere kıyasla kullanmaya teşvik edilir ve kullanıcı ağının bir parçası olan tüm tüketiciler, ağ etkisi sonucunda yeni kullanıcılar çekmek için ödüller veya ödeme alacak şekilde motive edilirler. Hizmet tokenleri çıkaran projelerin amacı, ağda daha fazla büyüme ve aktiviteyi teşvik etmektir; burada yatırım, gelecekteki karlar için bir hak yaratmaz, ancak ağın değeri zaman içinde arttıkça tokenin değerinin de artacağı beklentisiyle yatırımı teşvik eder.

Blokchaini teknolojisi ilk ortaya çıktığından beri yayılmaya devam etti ve daha fazla sayıda girişim, ICO'lar (Initial Coin Offerings) aracılığıyla sermaye toplamak için bu teknolojiyi kullanmaktadır. Bu durum, hizmet tokenlerine olan talebin giderek artmasına yol açmıştır. Bu talep, sağlık hizmetleri, veri ve pazarlama gibi çeşitli hizmetlere dijital erişim elde etmeye çalışan bireylerin sayısındaki artışa bağlanabilir. Hizmet tokenlerinin, menkul kıymet tokenleri gibi doğrudan bir değeri olmasa da, yine de talep görmektedirler. Ancak, 2017'nin sonlarına doğru, bazı projeler düzenleyici otoriteler tarafından, hizmet tokenlerinin menkul kıymet olarak sınıflandırılıp sınıflandırılmayacağı konusunda incelemeye alınmıştır. [36]

3.8.2.2. Menkul kıymet tokenleri (Security Tokens)

Menkul kıymet tokenleri, bir varlığın mülkiyetini temsil eder ve sahiplerine bir işletmenin bir parçasına sahip olma hakkı sunar. Bu, yalnızca ihraççının topluluğunda geçerli olan belirli bir ürün veya hizmet sunan düzenlenmemiş hizmet tokenlerinden farklıdır. Menkul kıymet tokenleri, geleneksel menkul kıymetlerin ihraç ve ticaret sistemindeki belirli maliyetleri ihraççıdan yatırımcıya kaydırarak, emlak, özel şirketlerin öz sermayesi ve borçları, yatırım fonları gibi varlık sınıflarında sahiplik sunar. Bu tokenler, likit olmayan varlıkları daha kolay ticaret yapılabilir hale getirirken, geleneksel varlıkları dijitalleştirir. Bugün birçok menkul kıymet tokeni, özel şirketlerin hisseleri veya gayrimenkul mülkleridir.

Menkul kıymet tokenleri, menkul kıymet yasalarıyla düzenlenir. Yatırım amacıyla satılan her şeyin menkul kıymet olduğu kabul edilen klasik test nedeniyle, bu tokenlerin belirli bir finansal otoriteye kaydedilmesi veya kayıttan muaf tutulması

gerekir. Menkul kıymet ihraç eden kişi veya kuruluşlar, menkul kıymetlerin özelliklerini ve kısıtlamalarını belirten bir bölüm eklemek zorundadır. Kısıtlanmış menkul kıymet tokenlerinin nasıl ticaret yapılabileceği, ikincil arz olarak bilinir. Yatırımcılar, tokenlerin birden fazla yargı bölgesinde ve bağımsız borsalarda ticaret yapabilme yeteneğinden heyecan duymaktadır. Ancak menkul kıymet tokenleri ile ticaret yapanlar, düzenleyici otoritelerin müdahalesi konusunda büyük bir yasal belirsizlik içindedir. Şu an için menkul kıymet tokenlerini kaydettirmenin tek yolu, bir Menkul Kıymet Tokeni Arzı (STO) yapmaktır. İlk STO'lar, blockchaini projeleri için yapılmış olup, başlangıçta 300 milyon dolardan daha az fon toplandı ancak belirli bir tarihe kadar faaliyet göstermeyen yatırımcılara para iade edilmiştir. [37]

3.8.2.3. Varlık destekli tokenler (Asset-Backed Tokens)

Varlık destekli tokenler, dijital varlıklar alanında blockchaininde somut varlıkların tokenleştirilmesiyle ilgili yeni bir trenddir. Bu tür tokenler, fiziksel varlıklar üzerinde mülkiyet veya gelir paylaşım hakları sunar ve değerlerini arkasındaki somut varlıklardan alırlar. Emlak, altın ve gümüş gibi emtialar, sanat eserleri gibi birçok varlık türü tokenleştirilebilir. Yatırımcılar, hisse senetleri ve tahviller gibi geleneksel finansal varlıkların yanı sıra somut varlıkları da içeren çeşitlendirilmiş bir portföy sahibi olmak isterler. Bu tür varlıklara yatırım yapmak için genellikle önemli miktarda sermaye gereklidir. Varlık destekli tokenler, her iki problemi de çözme potansiyeline sahiptir. Blockchaininde çıkarıldıkları için likidite sunar ve bir kişiden diğerine internet üzerinden transfer edilebilir. Ayrıca, bu tokenleştirme süreci, söz konusu varlıkların paylaştırılmış mülkiyetini mümkün kılar. İhraççılar için bu, büyük bir anlaşmaya yatırım yapmak için çok sayıda insanın bir araya gelmesini sağlar.

Ancak, aktif olarak işlem görmeyen varlıklar için başlıca endişe, değerlemedir. Bir diğer sorun ise düzenlemelerdir. İhraççılar, projelerinin her bir katılımcının bulunduğu her yargı bölgesindeki düzenlemelere uygun olmasını sağlamalıdır. Düzenleyici ortam hala gelişmektedir ve çok az sayıda varlık destekli token, bu aşamayı geçebilmiştir. Bu engeller nedeniyle gelecekteki olasılıkları değerlendirmek zordur. Başarılı bir proje, yalnızca kripto yatırımcılarına değil, geleneksel finans geçmişine sahip yatırımcılara da hitap etmelidir. Getiriler, ideal olarak, arkasındaki varlıklara yapılan doğrudan yatırımla orantılı olmalıdır. Başarılı bir proje, bu yöntemi kullanarak geleneksel yatırımcılara ulaşabilir ve böylece daha geniş kitlelere benimsenme sağlayabilir. [38]

3.8.2.4. Hisse senedi tokenleri (Equity Tokens)

Geleneksel finansman modellerinde, hisse senetleri bir şirketteki kısmi mülkiyeti temsil eder ve sahipleri, şirket işlerinde oy verme haklarıyla birlikte bir mülkiyet payına sahiptir. Bu nedenle, hisse senedi tokeni sahipleri, girişimcilerle veya diğer token sahipleriyle kar ve zarar haklarını paylaşacaklardır. Haklar açısından benzerlik gösteren hisse senedi tokenleri, geleneksel finansman şekillerinin sınırlamaları nedeniyle tanıtılmıştır. Hisse senedi tokeni yaklaşımı ile girişimci şirketler, yatırımcıların, hizmet sağlayıcıların ve token kullanıcılarının şirketin katkılarına yatırım yapma yeteneğini demokratikleştirmiştir. Hisse senedi tokenleri kullanmak, blokchaini ekonomisine yatırım yapma yeteneğini demokratikleştirir ve girişim sermayesi finansmanı zorluklarına çözüm getirir. Blokchaini, tamamen yatırımın demokratikleştirilmesine doğru bir adım atma fırsatı sunmuştur.

Ayrıca, blokchaini teknolojisinin, işlem maliyetlerini düşürerek ve şeffaflığı artırarak bireysel yatırımcılara girişim sermayesi fonlamasının önünü açabileceği, girişim sermayesi toplama işlemlerinde uygulandığına dikkat edilmelidir. Hisse senedi tokenlerinin fonları, bulundukları ülkenin yasal düzenlemelerine uymalı ve ilgili denetleyici otoriteler tarafından yönlendirilmelidir. Token satışı etkinliği genellikle ekonomik ve yatırım forumları aracılığıyla gerçekleşir. Bu etkinlik, token meraklılarının kişisel olarak ya da bağlı oldukları etkinlik üzerinden iletişim kurulabileceği bir fırsattır. Bu eyleme başlamak, pazar yerinin gelişmeye başlamasına olanak tanır. Kişisel yatırımcılar, genellikle en sadık üyeler arasında paylaşılan bir token ön satışına katılabilir. İlk token arzına katkıda bulunan üyeler, ek teşviklerle, indirimler, ücretlerde azalma ve diğer bonuslarla hisse senedi tokeni edinme hakkına sahip olurlar. [39]

3.8.2.5. Blockchaini tokenlerinin kullanım alanları ve uygulamaları

Blokchaini tokenleri, bir blokchaininde barındırılan dijital varlıklar veya değer temsilidir. Bu tokenler, genellikle ilk coin arzları yoluyla satılır veya merkeziyetsiz finans sistemlerinde uçtan uca işlemleri kolaylaştırmak için kullanılır. Dijital tokenlerin kullanım alanları oldukça geniştir ve birden çok farklı uygulama alanına hitap edebilir. Tokenlerin önemli bir özelliği, blokchainindeki algoritmik konsensusa dayalı olarak değer taşımalarıdır. Bazı blokchainleri, dijital tokenlerin hemen barındırılabilmesini sağlayarak, kullanıcıların dijital varlıkları yaratmalarını

kolaylaştırır. Bu, tokenlerin oluşturulması için tüm kodlamayı yapmaya gerek kalmadan dijital varlıkların hızlı bir şekilde inşa edilmesine olanak tanır.

Blockchaini tokenlerinin kullanım alanları

- **Tedarik zinciri yönetimi**

Tedarik zinciri yönetiminde, tokenler, ürünlerin üretimden nihai tüketiciye kadar olan süreçlerini izlemek ve şeffaflık sağlamak için kullanılabilir. Bu kullanım, tedarik zincirinde güveni artırırken, süreçlerin daha verimli hale gelmesini sağlar.

- **Kimlik doğrulama**

Dijital tokenler, bireylerin kimliklerini doğrulamalarını sağlayan kolay ve güvenli bir yol sunar. Mobil uygulamalarda bir düğmeye tıklayarak kimlik kanıtı sunmak tokenler ile mümkün hale gelir.

- **Kayıbı olmayan tasarruf oyunları**

Merkeziyetsiz finans (DeFi) ve oyun dünyasında, tokenler kayıp yaşanmayan tasarruf oyunları yaratmak için kullanılabilir. Bu oyunlar, kullanıcıların kazançlarını artırmak için çeşitli finansal mekanizmalar sunar.

- **Paylaştırılmış mülkiyet**

Blokchaini tokenleri, mülkiyetin parçalara bölünmesini sağlar. Örnek olarak, bu bir gayrimenkul veya değerli bir varlık, tokenleştirilerek daha geniş bir yatırımcı kitlesine sunulabilir.

- **Merkeziyetsiz finans (DeFi)**

Blokchaini tokenleri, geleneksel bankacılık sistemlerinin dışında finansal işlemleri gerçekleştirmenizi sağlayan DeFi uygulamalarının temelini oluşturur. Bu, finansal sistemdeki güveni artırır ve erişimi daha geniş bir kitleye yayar.

- **Risk yönetimi**

Tokenler, finansal risklerin yönetilmesinde de kullanılabilir. Yatırımcılar, risklerini çeşitlendirmek ve minimize etmek için tokenler aracılığıyla daha güvenli yatırım fırsatları yaratabilir.

Bazı blockchaini tokenleri yalnızca bir değer birimini temsil etmekle kalmaz, aynzamanda çok daha karmaşık işlevlere sahiptir. Örneğin, açık kaynak mimarilerinin finansmanında veya oyun mekaniklerinde kullanılabilirler. Çevrimiçi oyunlar gibi uygulamalarda, tokenler finansal bütünlüğü izlemek için kullanılabilirken, akademik kimliklerin doğrulanması gibi işlemler de tokenler aracılığıyla yapılabilir. [40]

3.9. Dijital Cüzdan

Dijital cüzdanlar, e-cüzdanlar olarak da bilinir, kripto para birimlerinin gönderilmesine, alınmasına ve depolanmasına yardımcı olur. Bunlar, belirli blockchaini tabanlı kripto para birimlerinde varsayılan olarak mevcuttur ve güvenli ve merkezi olmayan oldukları bilinmektedir. Ancak, dijital cüzdan uygulamaları varlık portföylerine çok şey basitleştirir. Günümüzün dijital çağında, küresel olarak artan talep ve teknolojik gelişmeler nedeniyle, bankacılık sektörü, e-ticaret ve bu kripto para birimlerinin ticaret değeri hızla artmaktadır. Dijital cüzdan uygulamasının kullanıcı kullanımı, şahsen yapılan mağazaların, şirket portallarının ve e-ticaret sitelerinin ötesinde sayısız işlemle sonuçlanmaktadır. Dijital platformların, özel sektörün satışlarının yaklaşık %90'ını yalnızca dijital kanallara kaydıracağı önemli alanlar olacağı kanıtlanmıştır. Böyle bir ortamda, elektronik cüzdanlar, aşırı kolaylık, güvenlik ve hız nedeniyle Hindistan pazarındaki işlemlerin değerini artırmada önemli bir rol oynamaya hazırdır.

Dijital cüzdanlar, kripto para birimlerini depolamaya, göndermeye, almaya veya satın almaya yardımcı olan yazılım tabanlı sistemler veya mobil uygulamalardır. Değişen müşteri davranışları ve teknolojik gelişmeler sırasında ortaya çıktılar. Giderek artan sayıda insan, dijital cüzdan kullanarak bankacılık işlemlerini gerçekleştiriyor ve finansal işlemlerini yönetiyor. Finansal katılım için de önemli bir rol oynuyorlar. Düşük maliyetler ve dijitalleşme talebine dayanarak, hükümet ve diğer politika yapıcı kurumlar bundan faydalıyor. Burada, dijital cüzdan hakkında ayrıntılar, nasıl çalıştıkları, türleri ve diğer bilgiler tartışılıyor. Dijital cüzdan web sitesine kaydolarak, cüzdana para ekleyerek ve bunu banka hesabına aktararak elektronik cüzdan oluşturulabilir. Geçerli, aktif ve doğrulanmış bir cep telefonu numarasına ve internet bağlantısına sahip bir kullanıcı dijital cüzdan oluşturabilir. İnternet ve akıllı telefon kullanımının artmasıyla birlikte, giderek daha fazla tüketici artık işlemlerinde dijital cüzdanlar kullanıyor. E-cüzdanlar için pazar büyüklüğü hızla artıyor. Bunun nedeni,

tüketicilere tek bir tıklamayla, her yerde ve her zaman işlem yapmaları için hızlı ve modern bir yol sunmasıdır. Çevrimiçi, mobil ve satış noktası sistemleri, e-cüzdanlara doğru bu yükselen eğilimin başarısından sorumludur. Bir tüccarın kredi veya banka kartlarıyla ödeme kabul etmesi kolay ve güvenlidir ve ürün veya hizmetler için gerçek zamanlı işlemlere izin veren bir POS sistemi sunar. [41]

3.9.1. Dijital cüzdanların rolü ve türleri

Dijital cüzdanlar çeşitli biçimlerde ve türlerde gelir. Kullanıldıkları platform, işlevsellik veya bağlama göre kategorilere ayrılabilirler. Bir yandan, platform türüne göre düzenlenebilirler, yani mobil cüzdanlar, tarayıcı tabanlı ve bilgisayar tabanlı cüzdanlar ve donanım cüzdanları. Öte yandan, farklı uygulama ayarlarında işlevleri ve kullanımları açısından çeşitli türlerde olabilirler.

Mobil cüzdanlar. Bu cüzdanlar akıllı telefonlar için tasarlanmıştır ve mobil telefon kullanıcılarının cihazlarını kullanarak ödeme veya satın alma yapmalarını kolaylaştırmayı amaçlar. Kullanıcıların yalnızca ödeme yapmalarına izin vermekle kalmaz, aynı zamanda bir akıllı telefon ile herhangi bir alıcı ödeme terminali arasında iletişim kurmak gibi diğer hizmetleri veya işlevleri de entegre eder. Bu tür işlevlerde yaygın olarak çeşitli mobil ödeme hizmetleri kullanılır. Tarayıcı tabanlı web cüzdanları veya uzantıları, tamamen tarayıcı uzantıları üzerine kurulu belirli cüzdan uygulamalarına benzer. Cüzdan uygulaması, istemci uygulamasından bağımsız olarak çalışabilir. Sonuç olarak, web cüzdanları, kullanıcı tarafından birden fazla yetkilendirmeye ihtiyaç duymadan karmaşık iş süreçlerini çözerken birden fazla işlem veya yardımcı program işlemi gerçekleştirebilir. Tarayıcılara dayalı bilgisayar tabanlı cüzdanlar, dağıtılmış ağlarda oy kullanma yollarının yanı sıra kullanıcı gereksinimlerini yönetmeye yardımcı olabilir. Kullanıcılar, bu tür cüzdanlarda paralarını ve jetonlarını kullanabilir ve yalnızca kullanıcı parolalarını gösteren internet tarayıcılarını kullanarak etkileşim kurabilirler. Donanım cüzdanları, kullanıcının gizliliğinin diğer endişelerden daha önemli olduğu dağıtılmış ve merkezi olmayan bir bulut bilişim ortamında dağıtım gereksinimlerini karşılar. Herhangi bir heterojen platformda tasarlanabilen gizliliğe duyarlı bağlamsal uygulamalar için kullanıcıdan cihaza kimlik doğrulamasını desteklerler. Her hizmet sağlayıcının akıllı kartları ve güvenilir bileşenleridir. Her sağlayıcı, müşterilerine hizmet verirken donanım cüzdanı

için uygun veri birimleri sağlamalıdır. Bu cüzdanlar yazdırılabilir değildir ve çoğunlukla kripto paraların depolanması için tercih edilir.

3.9.1.1. Mobil cüzdanlar

Mobil cüzdanlar, mobil para, dijital cüzdanlar veya e-cüzdanlar olarak da bilinir, nakitsiz ve kağıtsız işlemler arasında prestijlerini oluşturmuştur. Mobil cüzdan, kullanıcıların akıllı telefonlarında veya dijital cihazlarında ödeme yapabilecekleri ve banka hesaplarını veya kredi/banka kartı bilgilerini güvenli bir şekilde saklayabilecekleri ve gerekli işlemlerini gerçekleştirebilecekleri geleneksel bir cüzdanın dijital biçimidir. Hızlı bir ödeme kanalı sunmayı ve işlem sürecini sorunsuz ve zahmetsiz hale getirmeyi amaçlamaktadır. Akıllı telefonlar ve bunların öncü teknolojileri, mobil cüzdanların omurgasını oluşturur - 2013'te işlem rekoru kıran ve küresel bilişim teknolojileri, finans ve eğlence sektörünü şekillendiren önemli bir rakam.

Mobil cüzdanlarda dijital nakit işlemleri, mobil ticaret satın alımları, mobil bankacılık ve diğer dijital pazarlama faaliyetleri gibi farklı işlevler mevcuttur. Biletler, biniş kartları veya seyahat kartları, lisanslar veya kimlik kartları, tesis erişim kartları ve bazı hasta sağlık kayıtları gibi fiziksel öğeler de mobil cüzdanlarda tutulabilir. Mobil ticaret faaliyetleri, özellikle e-ticaret dünyasında her geçen gün artmaktadır ve bu ödeme süreçlerini tamamlamak için mobil cüzdanlara sürekli talep vardır. Mağaza içi ödemeler, QR kodlarını tarayarak veya temassız ödemeler kullanarak dijital cüzdanlar aracılığıyla tamamlanabilir. Temassız ödemeler artık NFC ve EMV çip teknolojisi kullanılarak yapılabilir. Pandeminin mevcut yayılımı göz önüne alındığında, dijital ödemeler yapmak temassız ödemeler için en güvenli moddur. Bu, kartı dokundurarak veya işlemleri milisaniyeler içinde tamamlamak için mobil cüzdan cihazını POS ödeme terminali cihazlarının yakınına yerleştirerek yapılabilir. [42]

3.9.1.2. Web tabanlı cüzdanlar

Dijital cüzdan terimi geçtiğinde, kullanıcıların zihninde genellikle yalnızca mobil cihazlarla erişilebilen ödeme sistemleri canlanır. Ancak, web tabanlı dijital cüzdanlar da dijital finans dünyasında önemli bir yer edinmektedir. Temel yapıları itibarıyla web tabanlı cüzdanlar, uygulamalara entegre şekilde çalışır ve tarayıcılar, çeşitli finansal işlemleri yönetmek için ana kullanıcı etkileşim platformu olarak hizmet eder.

Web tabanlı cüzdanlar, hesaplara bir web tarayıcısı üzerinden erişilebilir. kullanıcılar, birden fazla banka hesabını yönetebilme avantajından yararlanabilirler. Akıllı telefon uygulamalarıyla entegre olmasının yanı sıra, yalnızca bir bilgisayar kullanılarak da ödeme yapılabilir. Web uygulaması üzerinden sunulan hizmet, temel bir web sitesi aracılığıyla da sağlanabilir. Bu da erişilebilirliği artırır.

Güvenlik, bu tür cüzdanlarda büyük önem taşır; çünkü veri alışverişi büyük veri formatında farklı platformlar arasında gerçekleşir. İki faktörlü kimlik doğrulama ve veri şifreleme, işlemleri daha güvenli hale getiren ileri düzey güvenlik önlemlerindendir.

E-ticaretin hızla yaygınlaşmasıyla, web tabanlı dijital cüzdanlar dijital ödeme çözümlerinin merkezi haline gelmiştir. Hassas bilgilere güvenli erişim hızlı ve kolay bir şekilde sağlanabilirken, kullanıcılar daha önce kaydedilen ödeme yöntemlerini de kullanabilir. Arka uç sistemleri, dijital sistemlerin yönetimini ve müşteri hizmetlerini kolaylaştırır. Şirketler, internet üzerinden ödeme ve dijital ödeme sistemlerini destekleyen e-ticaret siteleri ve alışveriş sepetleri geliştirmektedir. Kullanıcı, web tabanlı bir cüzdana giriş yaparak ödeme ağ geçidini senkronize eder. Böylece satıcı ve internet tüccar hesabı, kullanıcının cüzdanından yapılan ödemeyi tamamlar.

Bununla birlikte, birden fazla kripto para, coin veya token içeren işlemler için akıllı sözleşmelere ihtiyaç duyulabilir. Web tabanlı dijital cüzdanlar, dijital ödeme biçimi olarak hızla yaygınlaşmaktadır. Online perakendeciler tarafından yaygın olarak kullanılmaktadır ve popüler örnekleri arasında resmi web siteleri bulunmaktadır. [43]

3.9.1.3. Donanım cüzdanlar

Donanım cüzdanları, kripto paraların güvenli bir şekilde saklanması için kullanılan özel bir cüzdan türüdür. Bu cüzdanlar, temelde çevrimdışı olmaları ve diğer cüzdan türlerinden farklılıklarıyla öne çıkar. Donanım cüzdanlarının en büyük avantajı, dijital varlıklarınızı internetten uzak tutarak hırsızlık gibi riskleri azaltmasıdır.

Donanım cüzdanları genellikle USB bellek veya kredi kartı formunda olabilir; ancak en yaygın olanları USB tipi cüzdanlardır. Bu tür cüzdanları kullanırken, fonlarınıza erişimi geri yüklemek için kullanım kılavuzunu takip etmek önemlidir. Donanım cüzdanlarını benzersiz kılan iki temel özellik vardır: güçlü şifreleme ve yedekleme yapabilme yeteneği. Bu özellikler, cüzdan kaybolduğunda veya çalındığında, mevcut boş cihazlara aynı verileri yükleyerek cüzdanın kurtarılmasını mümkün kılar.

Genel bakışta, donanım cüzdanları, en güvenli kripto para cüzdanı türlerinden biri ve büyük yatırımlar için en iyi seçeneklerden biri olarak kabul edilir. Donanım cüzdanları sadece güvenli bir saklama aracı sunmakla kalmaz, aynı zamanda kullanım kolaylığı sağlar. İki temel kullanıcı arayüzü mevcuttur: düğmeler veya dokunmatik ekran. Dokunmatik ekranlı cüzdanlar, daha iyi güvenlik sağlayarak, telefon veya bilgisayar tabanlı işlemleri sık sık yapan kullanıcılar için ideal bir seçenek sunar.

Kripto paralara olan ilginin artmasıyla birlikte donanım cüzdanlarına olan talep de istikrarlı bir şekilde artmaktadır. Önemli dijital varlıkları kontrol eden ve sık saldırılara maruz kalan kullanıcılar, kötü niyetli aktörlere karşı fonlarını güvenceye almak için üst düzey bir donanım cüzdanı tercih etmelidir. Bu cüzdanlar, kullanıcı dostu özellikleriyle daha hızlı ve kolay kullanım imkânı sunarak da tercih edilir.

Donanım cüzdanları, yatırımcılar için güçlü güvenlik önlemleriyle birlikte kullanım kolaylığı ve dayanıklılık sağlayarak dikkat çekici bir seçenek olmaya devam etmektedir. [44]

3.9.2. Dijital cüzdanlarda güvenlik önlemleri

Bir dijital cüzdan sağlayıcısında hesap oluşturduğunuzda, sağladığınız hassas finansal bilgiler şifrelenmelidir, böylece yetkisiz erişim mümkün olmaz. Büyük dijital cüzdan şirketlerinden bazıları, güvenli bağlantılar sağlamak için büyük bankalarla aynı teknolojiyi kullanır. Şifrelenmiş bilgiler, USB bellekler, hafıza kartları, dizüstü bilgisayarlar, akıllı telefonlar, televizyonlar veya diğer mobil cihazlar gibi çeşitli medya türlerinde saklanabilir.

Dijital cüzdanlar, karmaşık bir veri güvenlik yöntemi olan şifreleme ile korunabilir. Bu koruma, bir şifre veya PIN ve kullanıcı kimliğini doğrulayan iki faktörlü kimlik doğrulama yöntemlerini içerir. Şifre veya PIN yalnızca kullanıcı tarafından bilinir ve iki faktörlü kimlik doğrulama yöntemleri genellikle kullanıcının bildiği, sahip olduğu veya olduğu bir şey olarak kategorize edilir. Bu yöntemler, kullanıcının bu benzersiz tanımlayıcılardan iki veya daha fazlasını sağlamasına dayanır.

Bilgiler, dijital cüzdan kaybolursa veya çalınrsa bile yetkisiz erişim riskini ortadan kaldıracak şekilde şifrelenir. Dijital cüzdana giriş yaptıktan sonra, ikinci bir şifre daha girilmesi gerekebilir. Bir dijital cüzdan hesabı oluştururken, gerçek zamanlı işlem bildirimlerini ve izleme hizmetlerini e-posta veya kısa mesaj yoluyla almayı

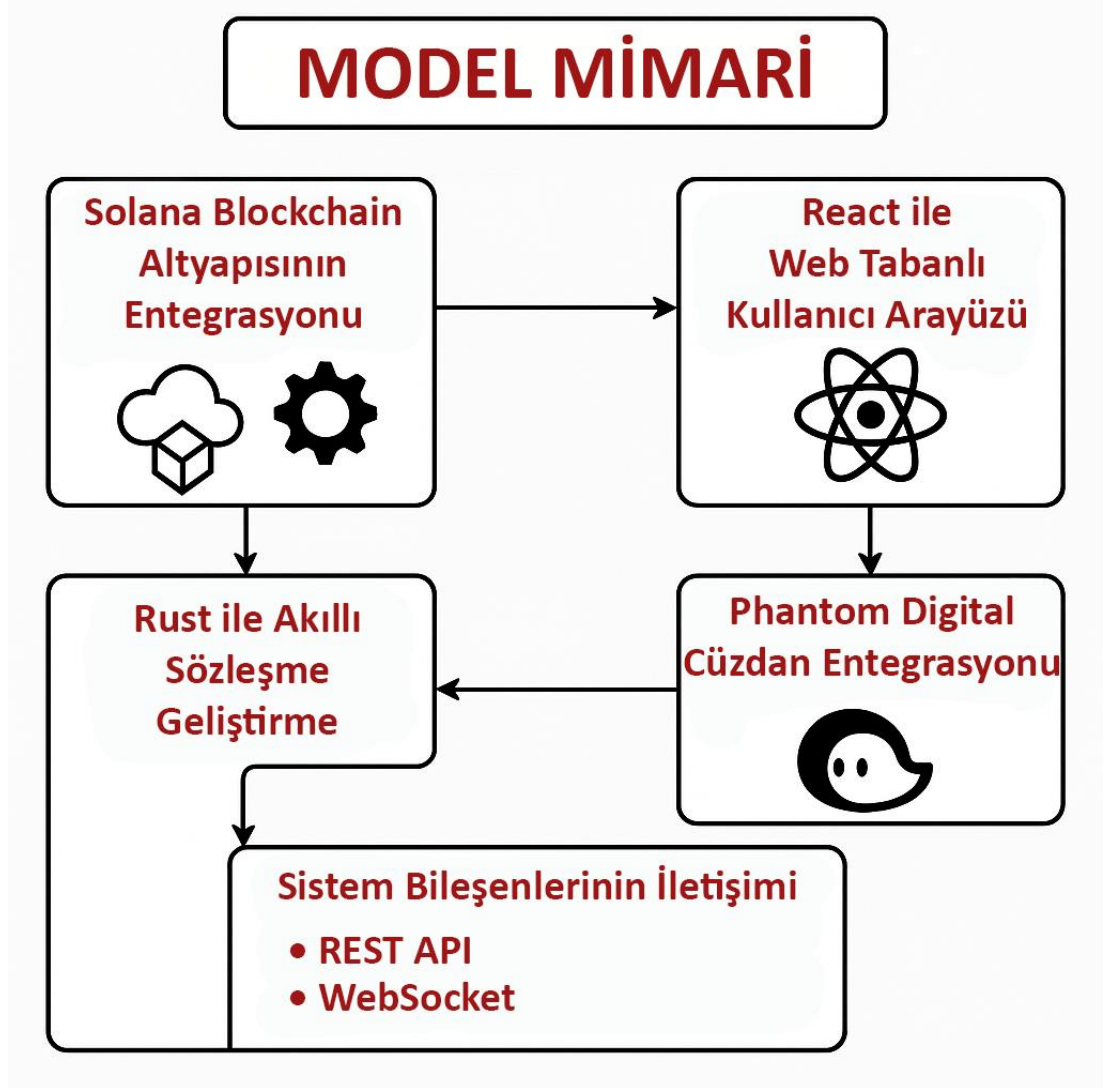
yetkilendirebilirsiniz. Mobil uygulama veya sistem bildirimleri de aynı uyarı hizmetlerini sağlar.

Bazı dijital cüzdanlarda, yüksek tutarlı işlemler için bildirimler gibi ek güvenlik özellikleri bulunur. Dijital cüzdanların korumalı ve güvenli olması sayesinde, ödeme yöntemlerinizi bu cüzdanlarda saklayabilir ve ihtiyaç duyduğunuzda güvenle para transferi gerçekleştirebilirsiniz. [45]



4. MODEL MİMARİ

Bu bölümde, geliştirilen blockchain tabanlı ödeme sisteminin teknik altyapısı ve bileşenleri ayrıntılı olarak açıklanmıştır. Sistem mimarisi; Solana blockchain ağına entegre edilen akıllı sözleşmeler, Rust programlama dili ile geliştirilen backend modülü, React ile oluşturulan kullanıcı arayüzü ve Phantom dijital cüzdan entegrasyonundan oluşmaktadır. Her bir bileşen, sistemin genel işleyişine katkı sağlayacak şekilde yapılandırılmıştır. Ayrıca, bileşenler arası iletişim protokolleri tanımlanarak, sistemin bütünsel çalışması sağlanmıştır.



Şekil 4.1. Model mimari şeması

4.1. Solana Blockchain Altyapısının Entegrasyonu

Solana, yüksek işlem kapasitesi ve düşük işlem ücretleri ile öne çıkan merkeziyetsiz bir blockchain platformudur. Bu projede, Solana ağı tercih edilerek yüksek verimlilikte, ölçeklenebilir ve güvenli bir altyapı oluşturulmuştur. Solana'nın mimarisinde yer alan Proof of History (PoH) konsensüs mekanizması, zaman damgalı işlemler sayesinde işlem sırasını önceden belirleyerek yüksek doğrulama hızı sağlar. Solana ağına entegrasyon, Solana tarafından sağlanan Solana Web3 SDK, Anchor Framework ve CLI araçları kullanılarak gerçekleştirilmiştir. Bu araçlar sayesinde sistemde; token transferleri, cüzdan doğrulama, sözleşme çağrılar ve ağ üzerinde veri kayıt işlemleri gibi temel fonksiyonlar uygulanabilir hale gelmiştir. Entegrasyon sürecinde, öncelikle yerel ağ (devnet) üzerinde test işlemleri gerçekleştirilmiş; sistem kararlılığı sağlandıktan sonra ana ağa (mainnet) dağıtım yapılmıştır. Bu aşamada, ağ bağlantısı ve veri akışı test edilerek, Solana zinciriyle senkronize çalışan bir uygulama yapısı elde edilmiştir.

4.2. Rust Kullanılarak Akıllı Sözleşme Geliştirme

Solana üzerinde çalışan programlar, diğer blockchain platformlarının aksine EVM tabanlı olmayıp, Rust programlama dili ile yazılmaktadır. Rust'ın sahip olduğu bellek güvenliği, yüksek performans ve tip güvenliği özellikleri sayesinde akıllı sözleşmeler daha güvenilir ve hataya kapalı şekilde geliştirilebilmektedir. Bu projede geliştirilen akıllı sözleşme; ödeme işlemlerini yönetmek, kullanıcı doğrulaması sağlamak ve token transferlerini gerçekleştirmek üzere yapılandırılmıştır. Sözleşme geliştirme süreci, öncelikle Cargo, lib.rs, Anchor.toml ve programs/ dizininden oluşan program iskeletinin oluşturulmasıyla başlamıştır. Ardından, cüzdanlar arası token transferi, işlem kayıtları ve kullanıcı rol yönetimi gibi iş mantığını (business logic) oluşturan fonksiyonlar geliştirilmiştir. Bu fonksiyonların doğruluğunu ve güvenilirliğini sağlamak amacıyla birim testleri yazılmış ve sözleşme, Anchor framework kullanılarak yerel ağı taklit eden test ortamlarında (localnet/devnet) test edilmiştir. Testlerin başarıyla tamamlanmasının ardından sözleşme Solana ağına deploy edilerek uygulamayla entegre hale getirilmiştir.

4.3. React ile Web Tabanlı Kullanıcı Arayüzü

Kullanıcı etkileşimlerinin sağlandığı ön yüz, modern web teknolojilerinden biri olan React kütüphanesi kullanılarak geliştirilmiştir. React'in bileşen tabanlı yapısı sayesinde kullanıcı arayüzü esnek, yeniden kullanılabilir ve sürdürülebilir modüllerle tasarlanmıştır. Arayüzde, Phantom cüzdan üzerinden kimlik doğrulamanın sağlandığı bir giriş/çıkış sistemi, kullanıcının bakiyesini görüntüleyebilmesi ve belirli adreslere token transferi yapabilmesini mümkün kılan bir transfer modülü, blockchain üzerinde gerçekleşen işlemlerin listelendiği bir işlem kayıtları ekranı ve işlem onayları, hata mesajları ile yönlendirmeleri içeren bir bildirim sistemi gibi temel işlevler öne çıkmaktadır.

Bu React arayüzü, sade, kullanıcı dostu ve mobil uyumlu bir tasarımla desteklenmiştir. Ayrıca, uygulama mantığı ile kullanıcı arayüzü arasında REST API üzerinden çift yönlü iletişim kurulmuş, böylece dinamik ve etkileşimli bir kullanıcı deneyimi sağlanmıştır.

4.4. Phantom Dijital Cüzdan Entegrasyonu

Phantom, Solana ekosistemine özel geliştirilmiş, tarayıcı tabanlı bir dijital cüzdan olarak proje kapsamında kullanıcıların blockchain işlemlerini doğrudan gerçekleştirebilmesi amacıyla entegre edilmiştir.

Bu entegrasyon sayesinde kullanıcılar, Phantom hesaplarıyla uygulamaya giriş yapabilmekte, cüzdan bakiyelerini görüntüleyebilmekte, akıllı sözleşmelerle etkileşime geçerek işlem başlatabilmekte ve transfer işlemlerini onaylayarak blockchain'e kayıt edebilmektedir. Phantom ile bağlantı, güvenli bağlantı ve işlem onayı işlevleri de dahil olmak üzere, solana wallet-adapter kütüphanesi aracılığıyla gerçekleştirilmiş ve proje bünyesine başarılı bir şekilde entegre edilmiştir.

4.5. Sistem Bileşenlerinin İletişimi

Geliştirilen sistem, yukarıda açıklanan bileşenlerin senkronize çalışması ile bütüncül bir yapıya sahiptir. Bileşenler arası iletişim, React arayüzü ile backend arasındaki veri akışını sağlayan REST API aracılığıyla gerçekleştirilmiş; kullanıcı işlemleri bu API üzerinden backend'e iletilerek blockchain işlemleri tetiklenmiştir.

Ayrıca, transfer onayı veya sözleşme yanıtı gibi gerçek zamanlı işlem bildirimleri için WebSocket teknolojisi kullanılmıştır. Kullanıcının kimlik doğrulaması, imzalama ve işlem onayı gibi cüzdan bağlantısı gerektiren işlemler ise Wallet Adapter ve Phantom SDK ile sağlanmıştır.

Bu bileşenler, ölçeklenebilir bir yapıda tasarlanarak hem geliştirme sürecinde esneklik sunmuş hem de gelecekte yapılacak entegrasyonlara açık bir mimari oluşturmuştur.



5. UYGULAMA

5.1. Program Tanıtımı ve Amaçları

Bu program, Solana blokchaini üzerinde bir "ödeme" sistemi uygulamak üzere yazılmıştır. Kullanıcılar arasında ödeme transferleri sağlayabilir, ödeme hızını ve miktarını sınırlandırabilir ve belirli yönetim yetkileri sunar. Program ayrıca kara listeleme, program dondurma ve hızlı istekleri sınırlama gibi özelliklere de sahiptir.

5.1.1. Ana program modülü

Program `use anchor_lang::prelude::*;` ile başlar. Bu, Anchor Framework'ün özelliklerini kullanarak Solana üzerinde program yazılmasına imkan tanır. Programdaki önemli fonksiyonlara sahiptir.

5.1.2. initialize_program

```
// Program yönetici yetkilerini ayarla
pub fn initialize_program(ctx: Context<InitializeProgram>) -> Result<> {
    let program_state = &mut ctx.accounts.program_state;
    program_state.admin = ctx.accounts.admin.key();
    program_state.is_frozen = false;
    Ok(())
}
```

Şekil 5.1. Program yönetici yetkilerini ayarlayan kod parçası

Bu fonksiyon, programı ilk kez başlatır, yönetici yetkilerini ayarlar ve bir `program_state` hesabı oluşturarak program çalışma durumu ile yönetici anahtarı gibi bilgileri tutar, ayrıca programı dondurulmamış ("frozen") bir durumda başlatır.

5.1.3. process_payment

Bu, kullanıcılardan ödemeleri işleyen ana fonksiyon olup, belirli miktarlarda SOL transferi gerçekleştirir; fonksiyon, programın çalışma durumu, kara liste kontrolü, kullanıcının SOL bakiyesi, ödeme sıklığı (rate limiting) ve yeniden girişe (reentrancy) karşı önlemler gibi kontrolleri yaparak ödeme işlemi sonrasında ödeme sayısı, son ödeme miktarı ve zaman bilgilerini günceller.

```

// Ödeme işlemi
pub fn process_payment(ctx: Context<ProcessPayment>, amount: u64) -> Result<> {
    // Program dondurulmuş mu kontrolü
    let program_state = &ctx.accounts.program_state;
    require!(!program_state.is_frozen, PaymentError::ProgramFrozen);

    // Yetki kontrolü
    require!(!program_state.is_blacklisted, PaymentError::AccountBlacklisted);

    // Miktar kontrolü
    require!(amount > 0, PaymentError::InvalidAmount);
    require!(amount <= program_state.max_payment_amount, PaymentError::AmountTooLarge);

    // Bakiye kontrolü
    let user_balance = ctx.accounts.user.lamports();
    require!(user_balance >= amount, PaymentError::InsufficientBalance);

    // Reentrancy guard
    require!(!ctx.accounts.program_state.is_locked, PaymentError::Locked);
    ctx.accounts.program_state.is_locked = true;

    // Rate limiting
    let clock = Clock::get()?;
    require!(
        clock.unix_timestamp - ctx.accounts.program_state.last_payment_timestamp
        >= program_state.min_time_between_payments,
        PaymentError::TooManyRequests
    );

    // Transfer işlemi
    let ix = anchor_lang::solana_program::system_instruction::transfer(
        &ctx.accounts.user.key(),
        &ctx.accounts.payment_account.key(),
        amount,
    );

    anchor_lang::solana_program::program::invoke(
        &ix,
        &[
            ctx.accounts.user.to_account_info(),
            ctx.accounts.payment_account.to_account_info(),
        ],
    );

    // State güncelleme
    let payment_state = &mut ctx.accounts.payment_state;
    payment_state.total_payments = payment_state
        .total_payments
        .checked_add(1)
        .ok_or(PaymentError::Overflow)?;
    payment_state.last_payment = amount;
    payment_state.last_payment_timestamp = clock.unix_timestamp;
    payment_state.is_locked = false;

    emit!(PaymentEvent {
        user: ctx.accounts.user.key(),
        amount,
        timestamp: payment_state.last_payment_timestamp,
    });

    Ok(())
}

```

Şekil 5.2. Ödeme sistemi ayarlayan kod parçası

Siber güvenlik açısından, programda yeniden girişe karşı bir kontrol (reentrancy guard) bulunması kritik öneme sahiptir, çünkü bu, bir kullanıcının ödeme işlemi sırasında hileli bir şekilde aynı çağrıyı tekrar yaparak hesap bakiyesini manipüle etmesini engeller; ayrıca, Solana'nın donanım tabanlı doğrulama sistemleri ve Proof of History (PoH) algoritması, işlemlerin zaman damgalarını sıralı bir şekilde doğrulayarak beklenmeyen girişimleri tespit eder, Solana'nın paralel işlem kapasitesi ise işlemlerin izole bir şekilde çalışmasını sağlayarak güvenliği artırır; rate limiting, çok sayıda işlem isteği engellenerek ağı gereksiz yükten korur, kara listeleme ise kötü niyetli kullanıcıların sistemden uzaklaştırılmasını sağlar, ancak alternatif hesaplar

üzerinden tekrar erişim sağlanabilir; Solana'nın Proof of History algoritması ve düşük işlem maliyetleri, ödeme sistemlerinin yüksek işlem hızı ve mikro ödemeler için ideal bir ortam sunar.

5.1.4. update_program_settings

```
// Admin fonksiyonları
pub fn update_program_settings(
    ctx: Context<AdminOnly>,
    new_max_amount: Option<u64>,
    new_min_time: Option<i64>,
) -> Result<()> {
    let program_state = &mut ctx.accounts.program_state;

    if let Some(amount) = new_max_amount {
        program_state.max_payment_amount = amount;
    }
    if let Some(time) = new_min_time {
        program_state.min_time_between_payments = time;
    }

    Ok(())
}
```

Şekil 5.3. Admin fonksiyonlarını barındıran kod parçası

Admin, maksimum ödeme miktarı ve ödemeler arası minimum zamanı değiştirebilir, bu da kötüye kullanım senaryolarını önlemek, güvenlik güncellemeleri ile sistemin performansını ve güvenliğini optimize etmek için kritik öneme sahiptir; Admin, bu ayarları değiştirebilir ve yeni maksimum ödeme miktarı (new_max_amount) ile minimum zaman aralığını (new_min_time) belirleyebilir.

5.1.5. freeze_program

Programı dondurur, yani işlem yapılamaz hale getirir.

5.1.6. blacklist_account

Belirli bir kullanıcıyı kara listeye ekler. Kara listedeki kullanıcılar işlem yapamaz.

```

pub fn blacklist_account(ctx: Context<AdminOnly>, user: Pubkey) -> Result<()> {
    // Hesabı karalisteye ekle
    let state = &mut ctx.accounts.program_state;
    if !state.blacklist.contains(&user) {
        state.blacklist.push(user);
    }
    Ok(())
}

```

Şekil 5.4. Karaliste sistemi kod parçası

5.2. Solana Hesaplarının Temelleri ve Veri Yapıları

Solana'da, tüm veriler zincir üzerinde hesaplar içinde depolanır. Programlar, işlemleri gerçekleştirmek için bu hesaplar üzerinde işlem yapar. Hesaplar iki ana bileşenden oluşur.

5.2.1. Signer

Signer, belirli bir işlemi imzalamaya yetkili bir kullanıcının veya programın kimliğini temsil eder ve her işlemde, işlemin geçerliliğini doğrulamak için bir veya daha fazla hesabın özel anahtarları ile imzalanması gerekir; bu, işlemin yalnızca yetkili kişiler veya programlar tarafından yapılmasını sağlar; örneğin, bir ödeme işlemi sırasında ödeme yapan kişinin Signer olarak geçmesi gerekir.

5.2.2. Account

Account, Solana ağındaki veri depolama birimidir ve programlar tarafından kullanılarak verileri depolamak için optimize edilmiştir; her hesabın benzersiz bir 32 bayt uzunluğundaki bir genel anahtar Public Key (genel anahtar) değeri vardır ve bu değer hesap adresi olarak kullanılır; hesaplar mutable (değiştirilebilir) olabilir ve yalnızca ilgili program tarafından güncellenebilir; örneğin, ödeme durumu (PaymentState) veya programın genel durumu (ProgramState), özel olarak tanımlanmış hesaplarda depolanır ve yalnızca yetkili işlemler tarafından güncellenir.

5.2.3. ProgramState

ProgramState, programın durum bilgilerini saklayan veri yapısıdır ve Solana'nın optimize edilmiş depolama modeliyle uyumludur; bu yapı, program yöneticisinin adresi (admin), programın çalışma durumu (is_frozen), maksimum ödeme miktarı

(max_payment_amount) ve ödemeler arası minimum zaman aralığı (min_time_between_payments) gibi alanları içerir.

Solana'daki hesaplar, maliyeti minimize etmek ve ağdaki kaynak tüketimini azaltmak için sıkı bir şekilde yapılandırıldığından, ProgramState yalnızca gerekli alanları içerir ve her alanın veri boyutu dikkatlice belirlenir. Solana'nın "seeds" ve "bump" gibi mekanizmaları, bu hesapların güvenli ve verimli bir şekilde oluşturulmasını ve yönetilmesini sağlar, bu da performansı artırırken saldırılara karşı ek bir güvenlik katmanını sunar.

5.2.4. PaymentState

Kullanıcı ödeme durumu için ayrı bir hesap, kullanıcının ödeme geçmişi ve güvenliğini izler ve aşağıdaki alanları içerir: total_payments (Kullanıcının toplam ödeme sayısı), last_payment (Son ödeme miktarı), last_payment_timestamp (Son ödeme tarihi), ve is_locked (Yeniden girişe karşı kilit durumu). Bu hesap, ödeme süreçlerini izlemek ve kullanıcı güvenliğini sağlamak için kullanılır.

5.3. Ortamının Yapılandırılması ve Güvenli Oturum Açma Geliştirmesi

5.3.1. Güvenli oturum açmanın implementasyonu

Web uygulamalarının geliştirilmesinde kullanılan bağımlılıkların doğru bir şekilde yapılandırılması, uygulamanın güvenliği ve performansı açısından kritik bir öneme sahiptir. Bu çalışmada kullanılan başlıca bağımlılıklar şunlardır:

Dotenv, ortam değişkenlerini yükleyerek hassas verilerin güvenli bir şekilde saklanmasını sağlar; örneğin, JWT'nin gizli anahtarını (JWT_SECRET) ve token geçerlilik süresini (JWT_EXPIRES_IN) dışarıdan alarak konfigürasyon bilgilerini yönetir. Express, Node.js tabanlı bir web uygulama çatısı olarak, HTTP isteklerini alıp işleyerek web uygulamalarının hızlı ve verimli bir şekilde geliştirilmesine olanak tanır.

```
// JWT Konfigürasyonu
const JWT_CONFIG = {
  secret: process.env.JWT_SECRET as string,
  options: {
    expiresIn: process.env.JWT_EXPIRES_IN || '1h',
    issuer: process.env.JWT_ISSUER,
    audience: process.env.JWT_AUDIENCE,
    algorithm: 'HS512' as const
  }
};
```

Şekil 5.5. JWT konfigürasyonu kod parçası

JWT (JSON Web Token) ise, kullanıcının kimliğini doğrulamak ve yetkilendirme işlemleri yapmak için kullanılan bir kütüphanedir; bu kütüphane sayesinde token'lar oluşturulur ve doğrulanır.

CORS (Cross-Origin Resource Sharing) ise API'nin farklı domainlerden gelen istekleri kabul etmesini sağlar, böylece uygulamanın farklı platformlardan erişilebilirliği sağlanırken güvenlik de artırılmış olur. Bu bağımlılıklar, güvenli bir API oluşturmak için birlikte çalışarak, kullanıcı verilerinin korunmasını ve kimlik doğrulama işlemlerinin doğru bir şekilde yapılmasını sağlar.

5.3.2. Express yapılandırması ve middleware

Express.js, API'nin temel yapı taşı olarak kullanılan bir framework'tür. Express, web uygulamaları geliştirmeyi hızlandıran bir araç olmasının yanı sıra, middleware kullanarak işlem sırasındaki işlemlerin esnek bir şekilde yönetilmesine imkan tanır. Bu projede Express.js ile aşağıdaki middleware yapılandırmaları yapılmıştır: `App.use(cors())` komutu, API'nin farklı domainlerden gelen istekleri kabul etmesini sağlayarak, uygulamanın çeşitli platformlardan veri taleplerini engellemeden kullanıcı deneyimini iyileştirir.

```

export const verifyToken = (req: Request, res: Response, next: NextFunction) => {
  const authHeader = req.headers['authorization'];
  const token = authHeader && (authHeader as string).split(' ')[1];

  if (!token) {
    return res.status(403).json({
      status: 'error',
      message: 'Token gerekli'
    });
  }

  try {
    const decoded = jwt.verify(token, JWT_CONFIG.secret, {
      issuer: JWT_CONFIG.options.issuer,
      audience: JWT_CONFIG.options.audience,
      algorithms: [JWT_CONFIG.options.algorithm]
    }) as any;

    // Token süresi kontrolü
    const now = Math.floor(Date.now() / 1000);
    if (decoded.exp && decoded.exp < now) {
      throw new Error('Token süresi dolmuş');
    }

    // Kullanıcı bilgisini req objesine ekle
    (req as any).user = decoded;
    next();
  } catch (err: any) {
    return res.status(401).json({
      status: 'error',
      message: `Token doğrulama hatası: ${err.message}`
    });
  }
};

```

Şekil 5.6. Token doğrulama kod parçası

5.3.3. JWT konfigürasyonu ve güvenlik önlemleri

JWT (JSON Web Token), kullanıcının kimliğini doğrulamak ve yetkilendirme sağlamak amacıyla kullanılan, JSON formatında imzalanmış bir token'dır. JWT, kullanıcının giriş yaptıktan sonra token almasını ve token'ın, sonraki isteklerde kullanıcının kimliğini doğrulamak için sunucuya gönderilmesini sağlar. Bu yapı, güvenli ve ölçeklenebilir bir kimlik doğrulama çözümü sunar.

JWT_SECRET, token'ın imzalanmasında kullanılan ve yalnızca sunucu tarafında güvenli bir şekilde saklanması gereken gizli anahtar olup, expiresIn parametresi token'ın geçerlilik süresini belirleyerek, kullanıcının token süresi dolmadan önce tekrar kimlik doğrulaması yapmasını sağlar; bu projede varsayılan süre 1 saat olarak belirlenmiştir. Ayrıca, issuer ve audience parametreleri, token'ın geçerliliğini sınırlamak için kullanılarak, issuer token'ı oluşturan kaynağı ve audience ise token'ın

hedef kitlesini tanımlar. Son olarak, algorithm parametresi, token'ın imzalanmasında kullanılan algoritmayı belirler ve bu projede HS512 (HMAC SHA-512) algoritması seçilerek güçlü bir güvenlik sağlanmış ve token'ın doğruluğu bu ölçekte korunmuştur.

5.3.4. Token doğrulama middleware'i

JWT, kullanıcının kimliğini doğrulamak için etkili bir çözüm sunar, ancak her API isteğinde token'ın doğruluğunun kontrol edilmesi gerekir. Bu doğrulama işlemi, özel bir middleware aracılığıyla yapılır. Middleware, gelen her istekte token'ı kontrol eder ve geçersiz token'lar için uygun hata mesajlarını döndürür.

5.3.5. Güvenli token gönderimi (HTTP-only cookie)

Web güvenliği açısından, token'ların istemci tarafında güvenli bir şekilde saklanması önemlidir. Bu amaçla, token'lar HTTP-only çerezler aracılığıyla istemciye gönderilir. HTTP-only çerezler, JavaScript ile erişilemez, bu da XSS (Cross-Site Scripting) saldırılarına karşı önemli bir güvenlik önlemidir.

Bu yapılandırma, token'ın yalnızca HTTPS üzerinden gönderilmesini sağlar (secure: true), çerezin sadece aynı site üzerinden gönderilmesini sağlar (sameSite: 'strict') ve token'ın geçerliliği bir saat ile sınırlıdır (maxAge: 3600000). Bu yöntemler, güvenliği artırarak kötü niyetli saldırılara karşı koruma sağlar.

```
try {
  const token = jwt.sign(payload, JWT_CONFIG.secret, JWT_CONFIG.options);

  // HTTP-only cookie ile token gönderimi
  if (process.env.NODE_ENV === 'production') {
    res.cookie('token', token, {
      httpOnly: true,
      secure: true,
      sameSite: 'strict',
      maxAge: 3600000 // 1 saat
    });
  } else {
```

Şekil 5.7. HTTP ile token gönderimi

5.3.6. Token içeriği ve payload

JWT'nin içeriği, token'ın doğruluğunu sağlamak ve gerektiğinde doğrulama işlemi yapmak için kullanılır. Payload, kullanıcıya ait bilgilerin yanı sıra, token'ın geçerliliğini kontrol etmek için kullanılan zaman damgalarını içerir.

```
const secondUser = {
  id: user.id,
  username: user.username,
  email: user.email,
  isActive: user.isActive,
  role: user.role,
  iat: Math.floor(Date.now() / 1000),
  nonce: Math.random().toString(36).substr(2, 9),
  lastLogin: new Date(),
};
```

Şekil 5.8. JWT payload kod parçası

UserId, her kullanıcıya ait benzersiz bir kimlik numarasını temsil ederken, username kullanıcı adını ve email kullanıcı e-posta adresini belirtir; role, kullanıcının uygulama içindeki rolünü tanımlar (örneğin, admin veya kullanıcı). Ayrıca, iat (Issued At) parametresi token'ın oluşturulma zamanını belirtirken, nonce parametresi ise replay saldırılarına karşı koruma sağlamak amacıyla her token için farklı bir rastgele dize kullanılarak güvenliği artırır.

5.3.7. Bakiye güncelleme işlemi ve yetkilendirme

JWT, kullanıcıların yalnızca geçerli bir token ile işlem yapabilmesini sağlamak için kullanılır. Özellikle, kritik işlemlerden biri olan bakiye güncellemeleri, yalnızca doğrulama işlemi başarıyla geçen kullanıcılara yapılabilir. Bu middleware, yalnızca yetkili kullanıcıların işlem yapabilmesini sağlar. Yalnızca geçerli bir token'a sahip kullanıcılar, bakiye güncellemesi yapabilir.

```
const getUser = ((req, res) => {
  const user = users.find(u => u.username === req.user.username);

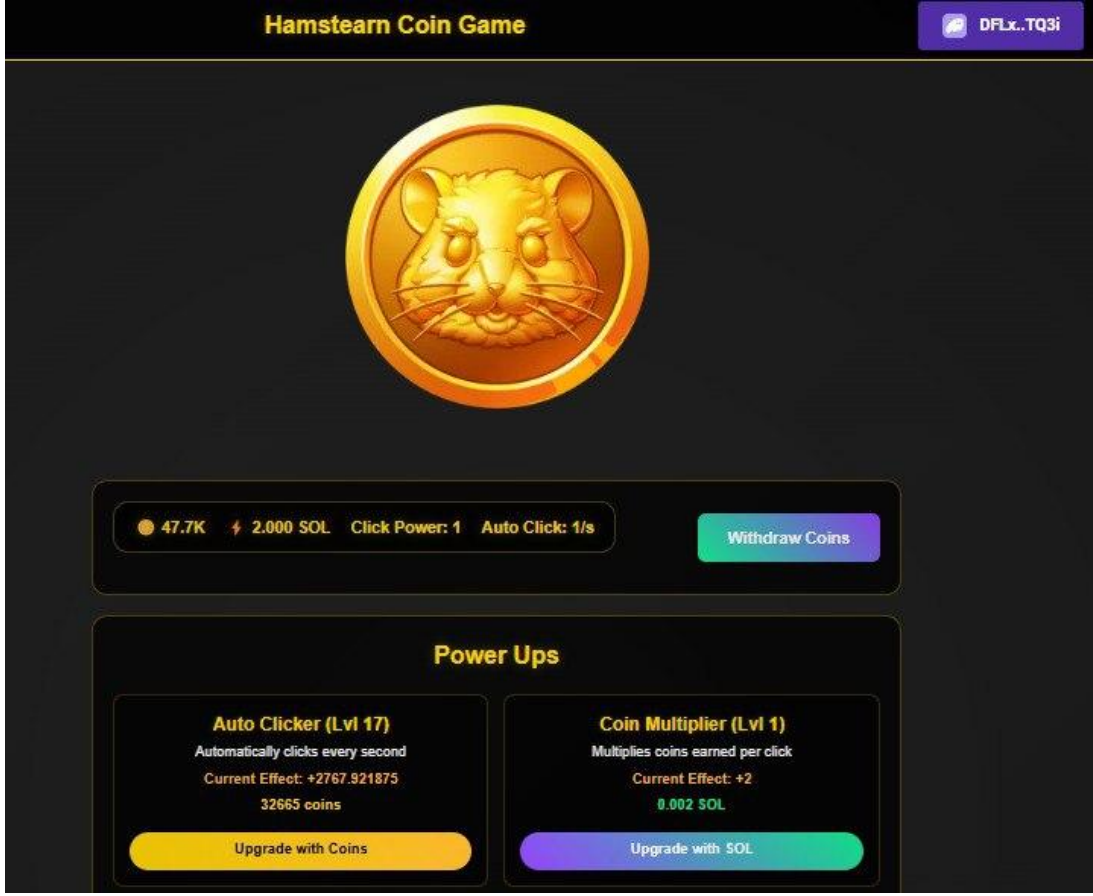
  if(!user) {
    return res.status(404).json({
      status: 'error',
      message: 'Kullanıcı Bulunamadı'
    });
  }
});
```

Şekil 5.9. Kullanıcı bilgileri getiren kod parçası

5.3.8. Geliştirilen uygulamanın son hali

Geliştirdiğimiz web tabanlı oyunumuzun son hali bu şekildedir. Hamstearn Coin Game ile tıklama işlemleri yapılarak ilgili coin kazanılır. Bu işlem Solana altyapısı

kullanarak geliřtirdiđimiz deme sistemiyle gerekleřir. Benzer yapılarda token tabanlı oyunlara rnek olarak geliřtirilmiřtir.



řekil 5.10. Geliřtirilen oyunun son hali

6. BİRİM TESTİ

React kütüphanesi ile geliştirilmiş kullanıcı arayüzü üzerinden Solana ağı üzerinde çalışan, Rust diliyle yazılmış akıllı sözleşmeler kullanılarak blockchain tabanlı bir ödeme sisteminin güvenlik açıklarını tespit etmek ve sistemin güvenilirliğini artırmak amacıyla birim testi uygulanmıştır.

Birim testleri, sistemin temel bileşenlerinin işlevselliğini ve güvenliğini sınamak üzere geliştirilmiş olup, akıllı sözleşmelerin kritik işlevleri üzerinde odaklanmıştır. Test süreci sonucunda bazı zafiyetler tespit edilmiştir. Bu bölümde, tespit edilen zafiyetlerin teknik detayları, potansiyel etkileri ve önerilen çözüm yaklaşımlarını ele almıştır.

6.1. Veri Doğrulama Eksikliği

Testlerimizde orta seviye bir güvenlik açığı olarak tanımlanan veri doğrulama eksikliği tespit edilmiştir. Bu zafiyet özellikle power_up_id parametresi üzerinde yapılan uzunluk ve format kontrollerinin yetersiz olmasından kaynaklanmaktadır. power_up_id parametresi, akıllı sözleşmenin belirli işlem süreçlerinde kimlik doğrulama ve işlem eşleştirme için kritik bir rol oynar.

Uygulanan birim testlerde, bu parametreye geçersiz ya da beklenmeyen formatta veriler gönderilmiş ve sözleşmenin bu durumları yeterince engelleyemediği görülmüştür. Böylelikle, kötü niyetli bir kullanıcı veya saldırgan, hatalı veya manipüle edilmiş power_up_id değerleriyle sistemde beklenmedik davranışların ortaya çıkmasına yol açabilir. Bu durum, örneğin hatalı işlem eşleştirmeleri, yetkisiz erişim ya da işlem manipülasyonları şeklinde zafiyetlere kapı aralayabilir.

Kimlik doğrulama mekanizmalarının atlanması, yanlış işlem kaydı veya hatalı işlem yürütümü, sistemin genel güvenilirliğinin azalması gibi potansiyel etkiler vardır.

power_up_id parametresi için kesin uzunluk ve regex tabanlı format doğrulaması eklenmesi, parametre alındığı her noktada input sanitizasyonu ve validasyon kontrollerinin zorunlu kılınması ve potansiyel hatalı girişler için kullanıcı dostu hata

mesajlarının ve işlem iptali mekanizmalarının devreye alınması gibi çözüm önerileriyle zafiyetler giderilebilir.

6.2. Lamports Manipülasyonu

Birim testler sırasında yüksek öncelikli bir güvenlik açığı olarak tanımlanan ve sistemin temel fonksiyonlarından biri olan `try_borrow_mut_lamports` fonksiyonunun eksik veya yetersiz kontrol edilmesinden kaynaklanan Lamports manipülasyonu zafiyeti tespit edilmiştir. Lamports, Solana ağında kullanılan en küçük işlem birimi olarak, token transferlerinde kritik öneme sahiptir.

Test senaryolarında, bu fonksiyonun yetersiz kontrolü nedeniyle, normalde Solana runtime kuralları çerçevesinde engellenmesi gereken hatalı veya uyumsuz transferler sisteme kabul edilmiştir. Bu durum, blockchain protokolünün öngördüğü kuralların atlanmasına ve uyumsuz işlemlerin blockchain ağına kayıt edilmesine sebep olmuştur.

Yetkisiz token transferi ve varlık kaybı, sistem içi tutarsızlıklar ve hileli işlem gerçekleştirilmesi, ağ üzerinde güven kaybı ve kullanıcıların sisteme olan güveninin sarsılması gibi potansiyel etkiler vardır.

`try_borrow_mut_lamports` fonksiyonunun çağrıldığı her noktada ek güvenlik ve tutarlılık kontrollerinin yapılması, solana runtime kurallarına uygun işlem doğrulama ve hata yakalama mekanizmalarının geliştirilmesi, kritik fonksiyonlar için kapsamlı ek test senaryolarının yazılması ve otomatik güvenlik testlerinin entegre edilmesi gibi çözüm önerileriyle zafiyetler giderilebilir.

6.3. Aritmetik-Kayan Nokta Hatası

Orta seviye bir güvenlik açığı olarak sınıflandırılan aritmetik-kayan nokta hatası, sistemde SOL maliyet ve çekim hesaplarında f64 (floating-point) ile u64 (unsigned integer) dönüşümlerinin uygulanması sonucunda ortaya çıkmıştır. Rust dilinde kayan nokta sayıların tamsayıya dönüştürülmesi hassasiyet kaybına yol açabilir ve küçük fakat kritik bakiyelerde hesaplama sapmalarına neden olabilir.

Testlerde, özellikle düşük bakiye ve küçük işlem tutarlarında yapılan işlemlerde, dönüşüm kaynaklı ufak sapmalar tespit edilmiştir. Bu sapmalar, zamanla sistemde toplam bakiye hesaplamalarında tutarsızlıklara, işlem reddine ya da hatalı bakiye gösterimine sebep olabilir. Kullanıcı bakiyelerinde hata ve yanlış görüntüleme, yanlış

işlem onayları ve işlem iptaller, sistem bütünlüğünün ve finansal doğruluğun bozulması gibi potansiyel etkiler vardır.

Dönüşüm gereksinimi varsa, dönüşüm öncesi ve sonrası aralık kontrolleri ile yuvarlama hatalarının minimize edilmesi, hassasiyet kaybını önlemek için sabit nokta (fixed-point) aritmetik kütüphanelerinin kullanılması gibi çözüm önerileriyle zafiyetler giderilebilir.

6.4. Rust Özel Sorunları

Rust dilinin sahip olduğu güçlü tip sistemi ve bellek güvenliği özelliklerine rağmen, yapılan birim testlerde `try_borrow_mut_lamports` fonksiyonunun çağrılmadan önce bakiye kontrolünün yapılmaması orta seviye bir güvenlik açığı olarak belirlenmiştir. Bu eksiklik, programın kontrol dışı durmasına ya da akıllı sözleşmenin beklenmedik bir şekilde sonlanmasına sebep olabilmektedir.

Bu sorun, özellikle kullanıcı işlemlerinde yetersiz bakiye kontrolü ile tetiklenmekte ve işlem öncesi gerekli güvenlik adımlarının atlanmasına yol açmaktadır. Sonuç olarak, işlem akışında durdurma, kaynakların kilitlenmesi veya hatalı işlem kaydı gibi olumsuz etkiler ortaya çıkmaktadır.

Akıllı sözleşmenin beklenmedik durması ve işlem iptali, kullanıcı deneyiminde aksamalar ve sistem güvenilirliğinde düşüş, olası DoS (Denial of Service) saldırılarına açık hale gelme gibi potansiyel etkiler vardır.

`try_borrow_mut_lamports` fonksiyonundan önce bakiye kontrolü için güvenli ve kesin bir mekanizma eklenmeli, işlem öncesi ve sonrası durum kontrollerinin artırılması, hata yönetimi ve istisna yakalama kodlarının kapsamının genişletilmesi gibi çözüm önerileriyle zafiyetler giderilebilir.

6.5. Test Sonuçları

Uygulanan birim testler sonucunda sistem, yüksek, orta ve düşük öncelikli güvenlik zafiyetleri açısından kapsamlı olarak sınanmıştır. Test süreci, sistemin temel bileşenlerinin fonksiyonel ve güvenlik açılarını ortaya koymuş, dört ana zafiyet haricinde önemli güvenlik açıklarının tespit edilmemesini sağlamıştır. Bulunan zafiyetler, hem kritik hem de orta seviyede riskler içermekte olup, önerilen çözüm yöntemleriyle hızla ortadan kaldırılmıştır.

Özellikle Lamports manipölasyonu gibi yüksek öncelikli zafiyetin erken tespiti ve giderilmesi, sistemin güvenlik seviyesini ciddi oranda artırmıştır. Benzer şekilde, veri doğrulama eksikliklerinin giderilmesi ve aritmetik hassasiyet sorunlarının çözölmesi, sistemin işlevselliğini ve kullanıcı güvenliğini pekiştirmiştir.

Genel olarak, test süreci sayesinde; akıllı sözleşmenin güvenilirliği artırılmış, kullanıcı işlemleri daha sağlam ve doğrulanabilir hale getirilmiş, olası kötü niyetli saldırı ve manipölasyon riskleri azaltılmış, sistem ölçeklenebilirliği ve sürdürülebilirliği güçlendirilmiştir. Bu da daha güvenli bir sistem oluşturmamızı sağlamıştır.

```
// SOL ile power-up satın alma güvenlik testi
it('SOL ile power-up satın alma işlemi yeterli SOL olmadığında hata vermeli', async () => {
  // Yetersiz SOL bakiyesi
  (Connection as any).mockImplementation(() => ({
    getBalance: vi.fn().mockResolvedValue(50000000), // 0.05 SOL
    confirmTransaction: vi.fn().mockResolvedValue({ value: { err: null } }),
  }));

  render(React.createElement(Home));

  // SOL ile alınabilen bir power-up'ı bul
  const solPowerUpId = Object.entries(POWER_UPS).find(([, powerUp]) => powerUp.usesSol)?.[0]

  if (!solPowerUpId) {
    throw new Error('SOL ile alınabilen power-up bulunamadı');
  }

  // Power-up satın alma butonunu bul ve tıkla
  const purchaseButton = screen.getByText('Upgrade with SOL');
  fireEvent.click(purchaseButton);

  // Hata mesajının görüntölendiğini kontrol et
  await waitFor(() => {
    expect(screen.getByText('Yeterli SOL bakiyeniz yok!')).toBeInTheDocument();
  });
});

// Coin ile power-up satın alma güvenlik testi
it('Coin ile power-up satın alma işlemi yeterli coin olmadığında hata vermeli', async () => {
  render(React.createElement(Home));

  // Coin ile alınabilen bir power-up'ı bul
  const coinPowerUpId = Object.entries(POWER_UPS).find(([, powerUp]) => !powerUp.usesSol)?.[0]

  if (!coinPowerUpId) {
    throw new Error('Coin ile alınabilen power-up bulunamadı');
  }

  // Power-up satın alma butonunu bul ve tıkla
  const purchaseButton = screen.getByText('Upgrade with Coins');
  fireEvent.click(purchaseButton);

  // Hata mesajının görüntölendiğini kontrol et
  await waitFor(() => {
    expect(screen.getByText('Yeterli coin bakiyeniz yok!')).toBeInTheDocument();
  });
});
```

Şekil 6.1. Birim testinden bir kesit

7. SONUÇLAR

Bu çalışmada oyun platformlarında blockchain tabanlı ödeme sistemleri güvenlik yönleriyle ele alınarak, bu alana ışık tutulmak istenmiştir.

Geliştirilen uygulama React kütüphanesi ile geliştirilmiş bir kullanıcı arayüzü üzerinden Solana ağı üzerinde çalışan, Rust diliyle yazılmış akıllı sözleşmeler kullanılarak bir blockchain tabanlı ödeme sistemi geliştirilmiş ve bu sistemin güvenlik açısından değerlendirilmesi yapılmıştır.

Sistem tasarımında, işlem güvenliği, kullanıcı gizliliği ve varlık sahipliğinin korunmasına yönelik tedbirler alınmıştır. Solana blockchain altyapısı, yüksek hızlı ve düşük maliyetli işlem yapabilme özellikleriyle bu tasarımın temelini oluşturmuş ve kullanıcıların güvenli bir ortamda işlem yapmasını sağlamıştır. Rust dilinin bellek güvenliği ve performans avantajları, akıllı sözleşme geliştirme sürecinde kritik bir rol oynamış; işlem mantığı, veri doğrulama ve kullanıcı yetkilendirme süreçleri titizlikle tasarlanmıştır.

Bu sistemde, dijital cüzdan entegrasyonu önemli bir bileşen olarak öne çıkmış ve kullanıcıların Solana uyumlu cüzdanlar aracılığıyla güvenli bir şekilde işlem yapabilmeleri sağlanmıştır.

Oyun platformlarındaki ödeme sistemleri, dijital varlıkların güvenli bir şekilde transferi ve saklanmasını gerektirir. Bu sistemde, blockchain teknolojisinin sunduğu değişmezlik, şeffaflık ve merkeziyetsizlik özelliklerinden yararlanılmış; işlem izni yalnızca kullanıcı onayı ile gerçekleşen bir yapı kurulmuştur. Aynı zamanda, akıllı sözleşmelerin doğru ve güvenilir çalışması için sıkı güvenlik önlemleri alınmış, veri bütünlüğü ve yetkisiz erişim gibi riskler minimize edilmiştir. Bu yöntemler, kullanıcıların dijital varlıklarını güvenle yönetebileceği ve blockchain tabanlı ödeme sistemlerini sorunsuz bir şekilde kullanabileceği bir çözüm sunmuştur.

Oyun içi varlıkların gerçek dünyadaki karşılıkları ve bu varlıkların güvenli transferi, blockchain teknolojisinin sunduğu çözümler sayesinde daha erişilebilir hale gelmiştir. Dijital varlıkların artan önemi, güvenlik standartlarının gelişmesini ve kullanıcı alışkanlıklarının bu teknolojilere olan güvenini artırmasını sağlamaktadır.

Bu çalışmalar, blockchain tabanlı ödeme sistemlerinin oyun sektöründe nasıl daha güvenilir ve verimli hale getirilebileceğine dair değerli bir bakış açısı sağlamış ve bu teknolojinin daha geniş alanlarda benimsenmesine katkı sağlamıştır.

Geliştirdiğimiz projede, Solana blockchain ağı üzerinde çalışan bir ödeme sistemi geliştirilmiş ve bu sistem, React ile oluşturulmuş tıklama tabanlı bir web oyununa entegre edilmiştir. Geliştirilen sistem, kullanıcılar arasında güvenli ve denetimli bir şekilde ödeme transferi yapılmasını sağlamaktadır. Sistem yalnızca ödeme transferleriyle sınırlı kalmayıp aynı zamanda ödeme hızını ve miktarını sınırlandırabilmekte, kullanıcı kara listeleme, işlem kısıtlama, programı dondurma gibi yönetici bazlı kontrol özellikleri de sunmaktadır. Rust diliyle yazılmış olan bu akıllı sözleşmeler, Anchor framework'ü sayesinde Solana üzerinde güvenli ve modüler şekilde çalışmaktadır. Programın temel amacı, güvenli ödeme işlemleri sağlamak, kötüye kullanımları önlemek ve kullanıcılar için istikrarlı bir mikro ödeme altyapısı oluşturmaktır.

Programın ilk adımı, `initialize_program` fonksiyonu ile gerçekleştirilir. Bu fonksiyon, programı başlatır, bir yönetici belirler ve programın çalışma durumunu tanımlayan bir durum (state) hesabı oluşturur. Program başlatıldığında, dondurulmamış bir modda çalışmaya başlar. Ödeme işlemlerinden sorumlu olan `process_payment` fonksiyonu, belirli miktarlarda SOL transferi yapılmasını sağlar. Bu fonksiyon işlem öncesinde çeşitli kontroller gerçekleştirir. Kullanıcının kara listede olup olmadığı, yeterli bakiyesinin bulunup bulunmadığı, son işlem zamanına göre bir sınırlama gerekip gerekmediği ve yeniden giriş saldırılarına karşı sistemin açık olup olmadığı gibi unsurlar dikkate alınır. Reentrancy guard yapısı sayesinde, aynı anda birden fazla işlem gerçekleştirilmesinin önüne geçilir. Solana'nın Proof of History algoritması ve paralel işlem işleyişi, bu ödeme sisteminin güvenliğini daha da güçlendirir. Rate limiting ile kötü niyetli çoklu talepler engellenir, kara liste özelliği ile istenmeyen kullanıcıların sistem dışında tutulması sağlanır.

Yönetici, `update_program_settings` fonksiyonu aracılığıyla ödeme miktarı limitini ve ödemeler arası minimum süreyi değiştirebilir. Bu yetki, sistemin yoğun kullanım anlarında performansını korumak ve güvenliği artırmak için kritik bir öneme sahiptir. Aynı zamanda `freeze_program` fonksiyonu, herhangi bir güvenlik açığı veya olağan dışı bir durum oluşması halinde sistemin geçici olarak dondurulmasını sağlar. `blacklist_account` fonksiyonu ile belirli kullanıcılar sistemden izole edilir. Bu

önlemler, blockchain tabanlı bir sistemde merkezi olmayan ancak denetlenebilir bir güvenlik mekanizması kurulmasına yardımcı olur.

Solana üzerinde geliştirilen bu programın veri yapıları da güvenlik ve performans açısından optimize edilmiştir. Signer, işlemi gerçekleştirme yetkisine sahip kimlikleri temsil ederken; Account, verilerin depolandığı temel yapılardır. Her hesap, benzersiz bir genel anahtarla tanımlanır ve yalnızca ilişkili program tarafından güncellenebilir. ProgramState, programın yönetici adresi, programın dondurulmuş olup olmadığı, maksimum ödeme miktarı ve ödemeler arası minimum süre gibi temel bilgileri tutar. Bu yapı yalnızca gerekli verileri barındırır, böylece ağ yükü azaltılır. PaymentState ise her kullanıcıya ait ödeme geçmişini, son ödeme miktarını ve yeniden girişe karşı kilit durumunu içerir. Bu yapı sayesinde her kullanıcının işlemleri kayıt altında tutulur ve güvenlik ihlallerine karşı gerekli önlemler alınır.

Projede web uygulaması güvenliğini sağlamak için çeşitli teknolojiler ve yapılandırmalar kullanılmıştır. Dotenv kütüphanesi, JWT gibi hassas yapıların gizli anahtarlarını ortam değişkenleri olarak güvenli şekilde yönetir. Express.js ise API altyapısını kurarak, HTTP isteklerinin hızlı ve güvenilir bir şekilde işlenmesini sağlar. API güvenliği, JSON Web Token (JWT) ile kimlik doğrulama yapılarak sağlanmaktadır. Her kullanıcı başarılı bir şekilde giriş yaptığında kendisine özel bir token verilir ve bu token sonraki isteklerde kullanıcıyı doğrulamak için kullanılır. Token'lar, yalnızca sunucu tarafından erişilebilen HTTP-only çerezler aracılığıyla iletilir. Bu çerezler JavaScript ile okunamadığı için XSS saldırılarına karşı yüksek güvenlik sağlar.

Express uygulaması içerisinde kullanılan middleware'ler sayesinde, gelen istekler kontrol edilerek yalnızca geçerli token'a sahip kullanıcıların işlem yapmasına izin verilir. Bu yapı, hem sistem güvenliğini artırır hem de kullanıcı kimliğini korur. Ayrıca token doğrulaması yapılmadan yapılan istekler engellenerek, sistem üzerinde yetkisiz erişimlerin önüne geçilir. Token içeriğinde kullanıcıya ait kimlik bilgileri, kullanıcı rolü, e-posta adresi ve zaman damgaları yer alır. Bu yapı sayesinde, her bir kullanıcının kim olduğu, hangi yetkilere sahip olduğu ve ne zaman giriş yaptığı kayıt altında tutulur. Replay saldırılarına karşı ise token içerisine eklenen rastgele "nonce" değerleri sayesinde güvenlik sağlanır.

Geliştirilen sistem, sadece güvenli bir ödeme altyapısı sunmakla kalmaz, aynı zamanda gerçek zamanlı olarak çalışan, mikro ödemelerle kullanıcıyı ödüllendiren bir oyun deneyimi sağlar. Kullanıcılar, "Hamstearn Coin Game" adlı web tabanlı oyunda, tıklama yoluyla coin kazandıkça sistem arka planda Solana ağı üzerinden işlemleri gerçekleştirir. Bu yapı, blockchain tabanlı oyun uygulamalarına yönelik önemli bir örnek sunmakta ve benzer projeler için temel bir model olarak kullanılabilir.

Sonuç olarak blockchain tabanlı sistemler, güvenliği ve erişilebilirliği açısından oyun platformları için bir alternatif olarak önümüze çıkıyor. Kullanıcı alışkanlıklarının değişmesiyle, bu teknoloji daha fazla kullanılacak ve güvenlik standartları oturtularak hayatımızda kalıcı yer edecektir.



KAYNAKLAR

- [1] Anmol Gajrani, Decentralized dreams - Crafting a secure and fair blockchain gaming environment.
- [2] M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: a state of the art survey," 2018.
- [3] T. Min, H. Wang, Y. Guo, and W. Cai, "Blockchain games: a survey," 2019.
- [4] M. Iqbal and R. Matulevicius, "Blockchain-based application security risks: a systematic literature review," 2019.
- [5] B. Saha, M. Mehedi Hasan, N. Anjum, S. Tahora et al., "Protecting the decentralized future: an exploration of common blockchain attacks and their countermeasures," 2023.
- [6] S. Dong, K. Abbas, M. Li, and J. Kamruzzaman, "Blockchain technology and application: an overview," 2023. ncbi.nlm.nih.gov
- [7] M. Lewis and C. Crawford, "Architectural design for secure smart contract development," 2024.
- [8] Sally M. Gainsbury & Alex Blaszczyński, "How blockchain and cryptocurrency technology could revolutionize online gambling", 2017
- [9] KN Erman, Blok zincir teknolojisini kullanarak nesnelerin interneti ağında veri güvenliğini sağlama: akıllı ev erneği, 2023
- [10] W Yang, S Garg, A Raza, DP Herbert & BH Kang, "Blockchain: trends and future", 2018
- [11] PJ Taylor, T Dargahi, A Dehghantanha, RM Parizi ve KKR Choo, "A systematic literature review of blockchain cyber security", 2020
- [12] Bilash Saha, "Protecting the decentralized future: an exploration of common blockchain attacks and their countermeasures", 2023
- [13] Fatih Süküt, "Blockchain technology in archiving and record management activities: an evaluation in terms of information security", 2023
- [14] İbrahim Halil Efendioğlu, "The mediating effect of blockchain technology on the cryptocurrency purchase intention", 2023
- [15] Myles Lewis & Chris Crawford, "Architectural design for secure smart contract development", 2024
- [16] G Topal - Kronotop İletişim Dergisi, 2024 - dergipark.org.tr. "Modern toplumda mitlerin dönüşümü ve sinemanın rolü: kültür dünyası insanının gündüz düşleri üzerine bir inceleme".
- [17] S Eyüpgiller – "Social review of technology and change, 2023 - dergipark.org.tr. Türk vergi sisteminde dijital dönüşümde önemli bir dönem: 2017-2021"

- [18] İ YILMAZ – “International journal of social humanities”, 2022 - jshsr.org. “Metaverse ve nft dünyasına tasarım açısından bir bakış”. jshsr.org
- [19] F Süküt – “Library archive and museum research journal”, 2024 - dergipark.org.tr. “Arşivcilik ve belge yönetimi faaliyetlerinde blokzincir teknolojisi: bilgi güvenliği bağlamında bir değerlendirme.” dergipark.org.tr
- [20] J Zarrin, H Wen Phang, L Babu Saheer, B Zarrin –“Cluster computing”, 2021 - Springer. “Blockchain for decentralization of internet: prospects, trends, and challenges.” springer.com
- [21] M Kvet, K Matiasko - Sensors, 2020 - mdpi.com. “Data block and tuple identification using master index”. mdpi.com
- [22] [22] J Kalajdjieski, M Raikwar, N Arsov, G Velinov... - Blockchain: research, 2023 - Elsevier. “Databases fit for blockchain technology: a complete overview.” sciencedirect.com
- [23] I Aviv – “International conference on intelligent vision and ...”, 2021 - Springer. “The distributed ledger technology as development platform for distributed information systems.” researchgate.net
- [24] U Rahardja, AN Hidayanto, N Lutfiani... - Sci. J ..., 2021 - researchgate.net. “Immutability of distributed hash model on blockchain node storage.” researchgate.net
- [25] O Ceylan, AH Isık - Uluborlu mesleki bilimler dergisi, 2023 - dergipark.org.tr. “Blokzincir teknolojisi ve uygulama alanları.” dergipark.org.tr
- [26] A Vosughi, A Tamimi, AB King, S Majumder... - ... and sustainable energy ..., 2022 - Elsevier. “Cyber–physical vulnerability and resiliency analysis for der integration: a review, challenges and research needs”
- [27] JP Vergne - Organization theory, 2020 - journals.sagepub.com. “Decentralized vs. distributed organization: blockchain, machine learning and the future of the digital platform.” sagepub.com
- [28] Z Önder - 2023 - acikerisim.bartın.edu.tr. “Yazılım tanımlı çoklu ağlarda makine öğrenmesi ve blokchaini ile geliştirilmiş servis kalitesi destekli yönlendirme mimarisi.”
- [29] S Gökpınar – “Dicle üniversitesi sosyal bilimler enstitüsü dergisi, 2021 – dergipark.org.tr. blokchaini teknolojisinin geleceği: kripto para birimleri ve ötesi.” dergipark.org.tr
- [30] Hİ Yıldız - 2023 - acikerisim.uludag.edu.tr. “Merkez bankası dijital parası: dünyadaki gelişmeler ve Türkiye için model önerisi.” uludag.edu.tr
- [31] K. Phimmuang and K. Sripanidkulchai, "Measurement and analysis of blockchain peers," IEEE Access, vol. 12, pp. 135075–135088, 2024. <https://doi.org/10.1109/ACCESS.2024.3462969>.
- [32] ÖZ Sabri, FS ONURSAL, NC UCA - 2020 - books.google.com. “Dijital gelecekte mesleklerin ve sektörlerin dönüşümü”. researchgate.net
- [33] P Freni, E Ferro, R Moncada - Blockchain: Research and Applications, 2022 - Elsevier. “Tokenomics and blockchain tokens: a design-oriented morphological framework.” sciencedirect.com

- [34] Y Tian, Z Lu, P Adriaens, RE Minchin... - Frontiers of engineering ..., 2020 - Springer. "Finance infrastructure through blockchain-based tokenization." researchgate.net
- [35] P Freni, E Ferro, R Moncada – "Blockchain: research and applications, 2022 - Elsevier. "Tokenomics and blockchain tokens: a design-oriented morphological framework." sciencedirect.com
- [36] A Lisi, A De Salve, P Mori, L Ricci, S Fabrizi – Future generation computer, 2021 - Elsevier. "Rewarding reviews with tokens: An ethereum-based approach." sciencedirect.com
- [37] AK Layr - Milan Law Review, 2021 - riviste.unimi.it. "Tokenization of assets: security tokens in Liechtenstein and Switzerland." unimi.it,
- [38] G Wang, M Nixon - Proceedings of the 14th IEEE/ACM International ..., 2021 - dl.acm.org. SoK: "Tokenization on blockchain." iacr.org
- [39] K Malinova, A Park - Management science, 2023 - pubsonline.informs.org. "Tokenomics: when tokens beat equity." ssrn.com
- [40] A Gupta, J Rathod, D Patel, J Bothra... - ... and network security ..., 2020 - Springer. "Tokenization of real estate using blockchain technology." researchgate.net
- [41] S Agrawal - International Journal of Intelligent Automation ..., 2021 - research.tensorgate.org. "Integrating digital wallets: advancements in contactless payment technologies." tensorgate.org
- [42] KP Jørgensen, R Beck - Business & information systems engineering, 2022 - Springer. "Universal wallets." itu.dk
- [43] A El Masry - 2023 - search.proquest.com. "The wallet of digital citizens: online payment adoption in the developing countries' public administration–case of Egypt." aucegypt.edu
- [44] Y Bulut, İ Sertkaya - Bilişim Teknolojileri Dergisi, 2020 - dergipark.org.tr. "Security problem definition and security objectives of cryptocurrency wallets in common criteria." dergipark.org.tr
- [45] RG Utomo, R Yasirandi - Scientific Journal of Informatics, 2024 - journal.unnes.ac.id. "Securing digital wallet loyalty: unveiling the impact of privacy and security." unnes.ac.id



ÖZGEÇMİŞ

Ad-Soyad : Seyyit Murat SEÇİLMİŞ

ÖĞRENİM DURUMU:

- **Lisans** : 2020, Sakarya Üniversitesi, Bilgisayar ve Bilişim Bilimleri Fakültesi, Bilgisayar Mühendisliği
- **Yükseklisans** : 2025, Sakarya Üniversitesi, Bilgisayar Mühendisliği Anabilim Dalı, Siber Güvenlik Yüksek Lisans

MESLEKİ DENEYİM:

- 15 yılın üzerinde fantastik / bilim kurgu yazarlığı yapmaktadır
- 2016-2019 yılları arasında 3B Animasyon alanın bir projenin yürütücüsü olarak çalıştı.
- 2021 yılında Boxu adında bir oyun geliştirme ekibi kurdu. Bu ekip halen aktif olarak geliştirme yapmaktadır.
- 2024 yılında bir oyun geliştiricisi organizasyonu olan in-die Valley'i kurdu.

TEZDEN TÜRETİLEN ESERLER:

- Seçilmiş, Çavuşoğlu, (2024, 26-27, Aralık). On Game Development Platforms Blockchain Based Security Of Payment Systems, *14th International Istanbul Scientific Research Congress*, Istanbul, Türkiye 1793-1796
- Seçilmiş, Çavuşoğlu, 2024. On Game Development Platforms Blockchain Based Security Of Payment Systems, *14TH INTERNATIONAL İSTANBUL SCIENTIFIC RESEARCH CONGRESS PROCEEDINGS BOOK*, 1793-1796