



Teknoloji Fakültesi

MARMARA ÜNİVERSİTESİ

TEKNOLOJİ FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

BİTİRME PROJESİ

Marmara Coin

PROJE YAZARLARI

FATİH MEHMED BİLGİN- EMİR MUHAMMET AYDEMİR

170419043- 171419008

DANIŞMAN

Dr. Öğr. Üyesi ALİ SARIKAŞ

İL, TEZ YILI

İstanbul, 2023

MARMARA ÜNİVERSİTESİ
TEKNOLOJİ FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

Marmara Üniversitesi Teknoloji Fakültesi Bilgisayar Mühendisliği Öğrencileri Fatih Mehmed Bilgin ve Emir Muhammet Aydemir'in "Marmara Coin" başlıklı bitirme projesi çalışması,/....../..... tarihinde sunulmuş ve jüri üyeleri tarafından başarılı bulunmuştur.

Jüri Üyeleri

Prof. Dr. Adı SOYADI (Danışman)

Marmara Üniversitesi (İMZA)

Doç. Dr. Adı SOYADI (Üye)

Marmara Üniversitesi (İMZA)

Dr. Öğr. Üyesi Adı SOYADI (Üye)

Marmara Üniversitesi (İMZA)

İÇİNDEKİLER

	Sayfa
KISALTMALAR LİSTESİ.....	5
ŞEKİL LİSTESİ.....	6
ÖZET.....	7
BÖLÜM 1. GİRİŞ.....	8
1.1. Bitirme Projesinin Amacı.....	9
1.2. Literatür Taraması.....	10
BÖLÜM 2. MATERYAL VE YÖNTEM	13
2.1. C# Programlama Dili.....	13
2.2. SQL Server Veri Tabanı.....	13
2.2.1. Veri Tabanı İşlemleri İçin Kullanılacak Yöntem.....	14
2.3. Blok Zincir.....	14
2.3.1. Blok Zincir Yapısı.....	15
2.3.2. Blok Zincir Çalışma Mantığı.....	16
2.3.3. Blok Zincir Avantajları.....	18
2.3.3.1. Merkeziyetsizlik.....	18
2.3.3.2. Değiştirilemezlik.....	19
2.3.3.3. Şeffaflık.....	19
2.3.3.4. İzlenebilirlik.....	20
2.3.3.5. Dağıtıklık.....	21
2.3.4. Blok Zincir Dezavantajları.....	22
2.3.4.1. %51 Saldırıları.....	22
2.3.4.2. Verileri Değiştirememe.....	22
2.3.4.3. Geniş Depolama Alanı İhtiyacı.....	22
2.3.5. Genesis Blok.....	23
2.3.6. İşlem.....	23
2.3.7. Blok.....	25
2.3.8. Cüzdan.....	27
2.3.9. Consensus Algoritması.....	28
2.3.9.1. Proof of Work.....	29

2.3.9.2. Proof of Stake.....	30
2.3.10. Blok Zincirde Kullanılacak Karma Algoritması.....	31
2.4. Oluşturulacak Ağ Yapısı.....	32
2.5. Uygulama Testleri.....	33
2.6. Uygulama Geliştirme Ortamı.....	34
BÖLÜM 3. BULGULAR VE TARTIŞMA.....	36
3.1. Blok Zincir Uygulaması.....	36
3.1.1. API Tasarımı.....	37
3.1.2. Kontrol Mekanizması.....	39
3.1.3. Ödül Dağıtımı.....	40
3.1.4. Kullanıcı Uygulaması.....	41
3.1.5. P2P Ağ Oluşturulması.....	44
3.2. Performans Değerlendirmesi.....	46
3.3. Güvenlik Analizi.....	46
3.4. Uygulama Alanları.....	50
3.5. Ölçeklenebilirlik.....	50
3.6. Sürdürülebilirlik ve Çevresel Etkiler.....	51
KAYNAKLAR.....	53

KISALTMALAR/ABBREVIATIONS

IoT: Internet of Things

SQL: Structured Query Language

API: Application Programming Interface

ANSI: American National Standards Institute

SHA-1: Secure Hash Algorithm 1

GUI: Graphical User Interface

EF: Entity Framework

OOP: Object Oriented Programming

PoS: Proof of Stake

PoW: Proof of Work

P2P: Peer to Peer

ŞEKİL LİSTESİ

	Sayfa
Şekil 1. Blok zincir yapısı.....	15
Şekil 2. Blok zincir çalışma mantığı.....	17
Şekil 3. Blok zincir tabanlı ödül sistemi işlem yapısı.....	24
Şekil 4. Blok yapısı.....	26
Şekil 5. Blok zincir çalışma mantığı.....	27
Şekil 6. Consensus algoritmalarının karşılaştırılması.....	30
Şekil 7. Blok zincir tabanlı sistemde kullanılan ağ yapısı.....	32
Şekil 8. Uygulamanın temellerini gösteren şekil.....	35
Şekil 9. API Tasarımı temsili görseli.....	36
Şekil 10. Kontrol mekanizması çalışma şekli.....	38
Şekil 11. Temsili blok görseli.....	39
Şekil 12. Uygulamaya giriş arayüzü ekran görüntüsü.....	40
Şekil 13. Uygulamaya ait kullanıcı ana sayfası ekran görüntüsü.....	40
Şekil 14. Uygulamaya ait görevler sayfası ekran görüntüsü.....	41
Şekil 15. P2P bağlantısı için sunucu örnek kod parçacığı ekran görüntüsü.....	42
Şekil 16. P2P bağlantısı için istemci örnek kod parçacığı ekran görüntüsü.....	43
Şekil 17. Güvenliğe yönelik salt ve hash fonksiyonu.....	45
Şekil 18. Sistem giriş ve doğrulama kısımlarının kod ekran görüntüsü.....	46
Şekil 19. Zincir doğrulama fonksiyonu, kod örneği.....	47

ÖZET

Çalışma blok zincir sistemini temel alarak bir ödül sistemi oluşturmayı hedeflemektedir. Çalışmanın amacı merkeziyetsiz ve güvenli olarak bir sistem oluşturmak ve işlemlerin takibini bu sistem üzerinden yapmaktır. Oluşturulan sistem sayesinde tüm işlemler şeffaf bir şekilde görülebilecek, aynı zamanda merkeziyetsiz ve denetlenebilir bir yapı oluşturulmuş olacaktır. Çalışma içerisinde uygulama kullanıcılarının görev tamamlama durumlarına göre onlara ödül verecek bir sistem tasarlanmıştır, verilen ödüllerin kayıt ve takibi için ise blok zincir sisteminin kullanılmasına karar verilmiştir. Kullanılacak blok zincir sistemi ile birlikte kullanıcıların işlemleri takip edilebilecek ve şeffaf olacaktır. Şeffaflık ve takip edilebilirlik ise beraberinde denetlenebilir bir yapı getirecek ve güvenli bir sistemin temellerini oluşturacaktır. Sistem kullanıcıların her tamamladığı görev için onlara bir ödül verecek ve verilen ödülün kaydı blok zincir üzerinde bir blok oluşturarak zincire eklenecektir. Bu şekilde sürdürülebilir, şeffaf ve merkeziyetsiz bir sistem elde edilmesi hedeflenmektedir.

ABSTRACT

The study aims to create a reward system based on the blockchain system. The aim of the study is to create a decentralized and secure system and to follow up the transactions through this system. With the system created, all transactions will be seen in a transparent way and a decentralized and auditable structure will be created at the same time. In the study, a system was designed to reward the application users according to their task completion status, and it was decided to use the blockchain system for the recording and tracking of the awards given. With the blockchain system to be used, users' transactions will be tracked and transparent. Transparency and traceability, on the other hand, will bring auditable structure and form the basis of a secure system. The system will give users a reward for each completed task, and the record of the reward will be added to the chain by creating a block on the blockchain. In this way, it is aimed to achieve a sustainable, transparent and decentralized system.

1.GİRİŞ

Günümüzde teknolojinin hızla ilerlemesiyle birlikte, birçok sektörde inovasyonlar ve yenilikler yaşanmaktadır. Bu sektörlerden biri de finansal işlemlerdir. Geleneksel finansal işlemlerde kullanılan yöntemlerin yanı sıra, son yıllarda blok zincir teknolojisi kullanılarak ödeme sistemleri de geliştirilmektedir.

Blok zincir teknolojisi, merkezi olmayan ve şeffaf bir yapı sunarak güvenli işlemler yapılmasına olanak sağlar. Bu nedenle, özellikle finansal işlemlerde kullanımı yaygınlaşmaktadır[1]. Blok zincir tabanlı ödeme sistemleri, geleneksel finansal kurumların aracılık rolünü ortadan kaldırarak, doğrudan bireyler arasında güvenli ve hızlı para transferi sağlar. Ayrıca, uluslararası ödemelerde düşük maliyetler ve hızlı işlem süreleri sunarak, sınırları aşan finansal işlemlerin gerçekleştirilmesini kolaylaştırır.

Ödül sistemleri de bu alanda geliştirilen uygulamalardan biridir. Blok zincir tabanlı ödül sistemleri, çeşitli sektörlerde kullanıcıların başarılarını ödüllendirmek için kullanılır. Örneğin, üniversitelerin öğrenci veya öğretim görevlilerine ödüller vermesini ve bunları blok zincir teknolojisi ile kaydetmesini sağlar. Bu sayede, ödülün sahibinin kim olduğu, ne zaman ve nasıl kazandığı gibi bilgiler doğrulanabilir ve güvenli bir şekilde kaydedilebilir[2]. Böylelikle, ödül sistemi kullanıcıları arasında güven ve şeffaflık sağlanır.

Blok zincir tabanlı ödül sistemlerinin bir avantajı, katılımcıların doğrulama sürecine dahil olabilmesidir. Blok zincir teknolojisi, kullanıcıların katkılarına dayalı olarak ödül kazanmalarını sağlar. Bu, sistemdeki kullanıcıları teşvik eder ve iş birliğini teşvik eder. Ayrıca, blok zinciri üzerindeki kayıtların değiştirilemez olması, sahtecilik veya hile girişimlerini önler ve güvenilir bir ortam sağlar.

Ancak, blok zincir tabanlı ödül sistemleri bazı dezavantajlara da sahiptir. Örneğin, blok zincirlerin ölçeklenebilirlik sorunları olabilir. Blok zincirdeki her işlem, tüm ağ katılımcıları tarafından doğrulandığı için, büyük ölçekte işlem hacmiyle başa çıkmak zor olabilir.

Bir diğer dezavantaj, blok zincir tabanlı ödül sistemlerinin enerji tüketimi konusudur. Özellikle PoW konsensüs algoritmasına dayalı blok zincirler, madencilik sürecinde yüksek miktarda enerji harcar. Bu durum çevresel etkiyi artırabilir ve sürdürülebilirlik açısından

sorunlara yol açabilir. Bu nedenle, alternatif konsensüs algoritmaları, örneğin PoS, daha enerji verimli bir yaklaşım sunarak bu soruna çözüm oluşturmaya çalışmaktadır.

Blok zincir tabanlı ödül sistemlerinin kullanım alanları sadece finansal işlemlerle sınırlı değildir. Örneğin, e-ticaret platformları, sadakat programları veya sosyal ağlar gibi çeşitli sektörlerde blok zincir tabanlı ödül sistemleri uygulanabilir. Bu sistemler, kullanıcılara belirli etkinlikler veya katkılar için ödüller vererek müşteri sadakatini artırabilir, kullanıcı katılımını teşvik edebilir ve veri güvenliği sağlayabilir.

Sonuç olarak, blok zincir tabanlı ödül sistemleri, güvenli, şeffaf ve değiştirilemez bir şekilde ödüllerin kaydedilmesini ve dağıtılmasını sağlayan yenilikçi bir yaklaşımdır. Bununla birlikte, ölçeklenebilirlik, enerji tüketimi ve teknolojik sınırlamalar gibi bazı zorluklar da göz önünde bulundurulmalıdır. Gelişen teknolojiler ve iyileştirmelerle birlikte, blok zincir tabanlı ödül sistemlerinin daha geniş bir kullanım alanına sahip olması ve finansal işlemlerin daha güvenli ve verimli hale gelmesi beklenmektedir.

1.1. Bitirme Projesinin Amacı

Bu proje, blok zincir teknolojisi kullanarak bir ödül sistemi geliştirmeyi amaçlamaktadır. Özellikle, bu ödül sistemi üniversitelerin öğrenci veya öğretim görevlilerine ödüller vermesini sağlamayı ve bunları güvenli ve şeffaf bir şekilde kaydetmeyi hedeflemektedir. Bu sayede, ödül kazananların bilgileri doğrulanabilir ve blok zincir teknolojisi sayesinde şeffaf bir şekilde izlenebilir hale getirilecektir.

Projenin amacı aynı zamanda, üniversitelerin öğrenci veya öğretim görevlilerine daha adil bir ödül sistemi sunmalarını sağlamaktır. Bu sayede, ödüllerin kazanılması ve dağıtılması daha şeffaf ve adil bir şekilde gerçekleştirilecek ve bu da üniversitelerin öğrenci veya öğretim görevlilerinin sadakatini artırabilecektir.

Projenin bir diğer amacı da, blok zincir teknolojisi kullanarak bir ödül sistemi geliştirerek, bu alanda yeni bir uygulama örneği sunmaktır. Bu sayede, blok zincir teknolojisi kullanımı konusunda farkındalık yaratmak ve bu teknolojinin farklı alanlarda kullanımına olanak sağlamak hedeflenmektedir.

Sonuç olarak, bu projenin amacı blok zincir teknolojisi kullanarak güvenli, şeffaf ve adil bir ödül sistemi geliştirmek, üniversitelerin öğrenci veya öğretim görevlilerine olan sadakatini artırmak ve blok zincir teknolojisi kullanımı konusunda farkındalık yaratmaktır.

1.2. Literatür Taraması

Günümüz iş dünyasında, blok zincir teknolojisi birçok alanda kullanılmaktadır ve giderek daha fazla popülerlik kazanmaktadır. Bu teknoloji, merkezi olmayan ve şeffaf bir yapı sunarak güvenli veri paylaşımı ve işlem süreçlerini sağlamaktadır. Blok zincirin kullanım alanları arasında finansal işlemler, sağlık hizmetleri, tedarik zinciri yönetimi, oy verme sistemleri ve daha pek çok sektör yer almaktadır. Bu çalışmada, blok zincir teknolojisinin ödül sistemlerine uygulanması ve potansiyel faydaları üzerinde durulmaktadır.

Blok zincir tabanlı ödül sistemleri, üniversitelerin öğrencilere ve öğretim görevlilerine daha adil ve şeffaf bir şekilde ödüller sunmasını hedeflemektedir. Geleneksel ödül sistemlerinde, ödül kazananların hakları ve başarıları zaman zaman sorgulanabilirken, blok zincir teknolojisi sayesinde bu sorunların önüne geçebilmektedir. Blok zinciri, ödül kazananların bilgilerini doğrulanabilir, değiştirilemez ve şeffaf bir şekilde kaydederek, ödüllerin adil bir şekilde dağıtılmasını sağlamaktadır. Böylece, öğrencilerin ve öğretim görevlilerinin başarıları güvence altına alınırken, üniversitelerin ödül süreçlerini daha etkin bir şekilde yönetmesi ve raporlaması mümkün olmaktadır.

Birçok akademik çalışma, blok zincir tabanlı ödül sistemlerinin potansiyel faydalarını araştırmıştır. Örneğin, blok zincir teknolojisi kullanarak oluşturulan ödül sistemleri [3], tedarik zinciri yönetimi gibi alanlarda verimlilik artışı sağlayabilir. Tedarik zinciri yönetiminde, ürünlerin kaynaklarından tüketiciye kadar olan yolculuğu karmaşık ve çok sayıda aracıyı içerir. Blok zincir teknolojisi, bu süreçteki tüm paydaşları bir araya getirerek, ürünlerin kaynağından tüketiciye kadar olan yolculuğunu şeffaf bir şekilde takip etmeyi ve verilerin doğruluğunu sağlamayı mümkün kılar. Bu sayede, lojistik, envanter yönetimi, kalite kontrol ve sertifikasyon gibi alanlarda verimlilik artışı elde edilebilir.

Bir başka araştırma[4], blok zincir tabanlı ödül sistemlerinin öğrenci sadakatini artırabileceğini ve öğrencilerin daha güçlü bir bağlılık hissetmelerini sağlayabileceğini ortaya koymaktadır. Blok zincir teknolojisi, öğrencilerin başarıları ve katkıları için adil bir şekilde ödüllendirilmelerini ve bunun sonucunda öğrencilerin motivasyonlarının artmasını sağlamaktadır. Geleneksel ödül sistemlerinde, öğrencilerin başarıları ve katkıları kaybolma

riski taşımakta ve bazen haksızlıklar yaşanabilmektedir. Blok zincir teknolojisi, bu sorunları ortadan kaldırarak, öğrencilerin ödülleri güvenli bir şekilde almasını ve bunlara erişimini kolaylaştırmaktadır. Katılımcılar arasında rekabeti teşvik ederek performansı arttırılabilir ve motivasyonu yükseltebilir. Doğrulanabilirliği sayesinde, ödülleri adil bir şekilde dağıtıldığına dair şüphe olmaz ve katılımcılar başarılarının takdir edildiğini bilmekten dolayı daha güçlü bir bağlılık hissederler.

Blok zincir tabanlı ödül sistemleri aynı zamanda öğrenci verilerinin güvenli bir şekilde saklanmasını sağlar. Geleneksel ödül sistemlerinde, öğrenci verileri genellikle merkezi bir sunucuda depolanır ve bu durum veri güvenliği risklerini beraberinde getirebilir[5]. Blok zinciri teknolojisi, verilerin dağıtık bir yapıda şifrelenerek depolanmasını sağlar, böylece verilerin yetkisiz erişimlere karşı korunması ve manipülasyona karşı dayanıklı hale getirilmesi mümkün olur. Bu da öğrencilerin kişisel verilerinin güvenliğini sağlar ve gizliliklerini korur. Merkezi olmayan doğası, verilerin dağıtık bir ağ üzerinde şifrelenmiş olarak depolanmasını sağlar ve bu da veri manipülasyonu veya yetkisiz erişim riskini azaltır.

Blok zincir tabanlı ödül sistemlerinin bir diğer avantajı da katılımcıların doğrulanabilirliğini sağlamasıdır. Blok zinciri, ödül kazananların kimliklerini ve başarılarını doğrulanabilir bir şekilde kaydeder. Bu sayede, işverenler veya diğer kurumlar, öğrencilerin kazandığı ödülleri sorgulayabilir ve doğrulayabilir. Aynı zamanda, blok zinciri, ödül kazananların başarılarını birbirleriyle karşılaştırma imkânı sağlayarak rekabeti teşvik eder ve daha iyi performansı ödüllendirir. Bu da öğrencilerin daha motive olmasını ve sürekli gelişim için çaba göstermelerini sağlar.

Blok zincir tabanlı ödül sistemlerinin uygulama alanları sadece eğitimle sınırlı değildir. Örneğin, blok zinciri teknolojisi kullanarak oluşturulan ödül sistemleri, sağlık hizmetleri sektöründe de kullanılmaktadır. Sağlık kurumları, hastaların ve sağlık çalışanlarının başarılarını takip etmek ve ödüllendirmek için blok zincir tabanlı ödül sistemlerini benimseyebilirler.

Blok zinciri, sağlık hizmetlerinde kalite kontrol ve performans yönetimi açısından önemli bir araç olabilir. Sağlık kurumları, blok zinciri teknolojisini kullanarak hastaların sağlık kayıtlarını güvenli bir şekilde depolayabilir ve bu kayıtlara erişimi sınırlayabilir. Aynı zamanda, sağlık çalışanlarının performansını değerlendirmek için blok zincir tabanlı ödül

sistemleri kullanılabilir. Sağlık çalışanları, başarılarına ve katkılarına göre ödüllendirilebilir ve bu ödüller blok zincirinde doğrulanabilir bir şekilde kaydedilebilir.

Örneğin, bir sağlık kurumu, blok zinciri tabanlı bir ödül sistemini kullanarak hastaların sağlık verilerini takip edebilir ve sağlıklı davranışlara teşvik edebilir. Hastalar, sağlık hedeflerine ulaştıklarında veya belirli tedavi planlarına bağlı kaldıklarında ödüller alabilirler. Bu ödüller, blok zinciri üzerinde doğrulanabilir ve geriye dönük olarak takip edilebilir. Bu şekilde, sağlık kurumları hastaların daha aktif bir rol üstlenmelerini teşvik edebilir ve sağlıklarını daha iyi yönetmelerine yardımcı olabilir.

Bunun yanı sıra, blok zinciri tabanlı ödül sistemleri[6], iş süreçlerini daha verimli hale getirebilir ve maliyetleri azaltabilir. Blok zinciri teknolojisi, aracıları ortadan kaldırarak doğrudan işlem yapılmasını sağlar ve bu da işlem süreçlerini hızlandırır ve maliyetleri düşürür.

Sonuç olarak, blok zincir tabanlı ödül sistemleri, eğitim ve sağlık hizmetleri sektöründe kullanıldığı gibi diğer birçok sektörde de uygulanabilir. Blok zinciri teknolojisi, verilerin güvenliği, şeffaflığı ve doğrulanabilirliği konusunda önemli avantajlar sunmaktadır. Bu sistemler, ödüllerin adil bir şekilde dağıtılmasını ve kaydedilmesini sağlayarak katılımcıların güvenini artırır. Ayrıca, blok zinciri teknolojisi, veri manipülasyonu ve hile girişimlerine karşı dirençli olduğu için ödül sistemlerinin güvenilirliğini ve bütünlüğünü sağlar.

2.MATERYAL VE YÖNTEM

2.1 C# Programlama Dili

Bu çalışmada, blok zinciri uygulaması C# programlama dili kullanılarak geliştirilmiştir. C#, Microsoft tarafından geliştirilen, modern bir nesne yönelimli programlama dilidir. C# programlama dili, genel amaçlı bir dil olup, masaüstü uygulamaları, web uygulamaları, oyun geliştirme, mobil uygulamalar ve IoT (nesnelerin interneti) gibi birçok farklı platform ve amaç için kullanılabilir.

C#, C++ ve Java gibi programlama dillerine benzer şekilde, C# da geniş bir kütüphane sistemi sunar ve aynı zamanda platform bağımsızdır. Bu da C# ile yazılan bir uygulamanın farklı işletim sistemlerinde (Windows, macOS, Linux vb.) çalışabilmesini sağlar.

C#, açık kaynak kodlu .NET Framework platformu ile birlikte kullanıldığında, uygulama geliştiricilere güçlü bir araç seti sunar. C# dilinde yazılan uygulamalar, .NET Framework'ün avantajlarından faydalanarak hızlı, güvenilir ve kolay bir şekilde geliştirilebilir.

Sonuç olarak, C#, modern bir programlama dili olup, birçok farklı platformda kullanılabilir. C# programlama dilinin kullanımı, geniş bir kütüphane desteği ve güçlü bir araç seti ile kolaylaştırılmaktadır.

2.2 SQL Server Veri Tabanı

Veri depolama için, SQL Server veritabanı kullanılmıştır. Microsoft SQL Server, Microsoft tarafından geliştirilen ve yönetilen, ilişkisel veritabanı yönetim sistemi (RDBMS) yazılımıdır. SQL Server, verilerin saklanması, yönetimi ve erişimi için kullanılan bir yazılımdır ve özellikle büyük ölçekli işletmeler için ideal bir seçenektir.

SQL Server, veri yönetimi için birçok farklı seçenek sunar. Örneğin, veritabanı tasarımı, veri saklama, veri güvenliği, yedekleme ve kurtarma, veri analizi ve raporlama gibi birçok farklı işlevsellik sunar.

SQL Server, birçok endüstri standardı ile uyumludur ve farklı işletim sistemleri üzerinde (örneğin Windows, Linux vb.) kullanılabilir. Ayrıca, SQL Server, birçok farklı programlama dili ile kullanılabilen açık bir API (Application Programming Interface) sunar.

SQL Server'ın bir diğer önemli özelliği, büyük ölçekli işletmelerin ihtiyaçlarını karşılamak için ölçeklenebilir bir platform sunmasıdır. Veritabanı büyüdükçe, SQL Server, yüksek performans, güvenilirlik ve iş sürekliliği sağlamak için tasarlanmıştır. Bu çalışmada blok zinciri uygulamasını kullanacak kullanıcıların kimlik bilgilerinin güvenli bir biçimde saklanması için SQL Server veritabanı kullanılmıştır.

2.2.1 Veri Tabanı İşlemleri İçin Kullanılacak Yöntem

Bu çalışmada veritabanı işlemleri için Entity Framework kullanılması hedeflenmektedir. Entity Framework (EF), Microsoft tarafından geliştirilen bir açık kaynaklı nesne ilişkisel eşleme (ORM) çerçevesidir. EF, veritabanı işlemlerini kolaylaştırır ve .NET uygulamaları ile etkileşimde bulunur. EF, .NET Framework ile birlikte gelir ve .NET programlama dilleri, özellikle C# ile birlikte kullanılır. Bu çerçeve, veritabanı işlemlerinin gerçekleştirilmesi için kullanılan SQL kodunu otomatik olarak oluşturur ve yürütür. Bu sayede, veritabanı işlemleri için yazılan kod miktarı azalır ve uygulama geliştirme süreci hızlanır. EF, nesne ilişkisel eşleme prensibine dayanır. Bu prensibe göre, veritabanındaki her bir tablo bir nesne olarak modellenir ve bu nesneler arasındaki ilişkiler otomatik olarak tanımlanır. Bu sayede, veritabanı işlemleri nesne yönelimli programlama (OOP) ile entegre edilir ve veritabanı işlemleri daha doğal bir şekilde gerçekleştirilebilir. EF, veritabanındaki değişiklikleri takip eder ve bu değişiklikleri veritabanına yansıtmak için SQL kodunu otomatik olarak oluşturur. Bu sayede, veritabanı işlemleri daha güvenli hale gelir ve veritabanı tutarlılığı sağlanır. EF, farklı veritabanı yönetim sistemleri ile uyumludur ve birden fazla veritabanı türü için destek sunar. EF ayrıca, veritabanı işlemlerinin yanı sıra, diğer .NET Framework özellikleri ile de entegre edilebilir.

2.3 Blok Zincir

Geliştirilecek ödül sisteminin blok zincir temelli olarak geliştirilmesi hedeflenmektedir. Blok zinciri, birçok bilgisayarın dağınık olarak çalıştığı bir veritabanı sistemidir. Blok zinciri teknolojisi, her bir bloğun bir önceki bloğa bağlanması ve böylece bir zincir oluşturması ile karakterize edilir. Bu zincir, blokların birbirine bağlı olması sayesinde verilerin güvenli ve şeffaf bir şekilde saklanması ve paylaşılmasını sağlar.

Blok zinciri teknolojisi, asıl olarak Bitcoin gibi kripto para birimleri ile ilişkilendirilir. Ancak, blok zinciri teknolojisi, finans sektöründeki uygulamaların yanı sıra, sağlık, lojistik, enerji ve birçok farklı endüstrideki uygulamalar için de kullanılabilir.

Blok zinciri teknolojisi, merkezi olmayan bir yapıya sahiptir, yani bir merkezi otoriteye ihtiyaç duymaz. Veriler, bloklar halinde şifrelenerek saklanır ve bir blok oluşturulduktan sonra, içerdiği veriler değiştirilemez hale gelir. Böylece, blok zinciri teknolojisi, verilerin manipülasyonu ve hile yapılmasını engeller. Bu teknoloji, işlemleri doğrulamak ve doğruluğunu sağlamak için karma fonksiyonlarını kullanır[7].

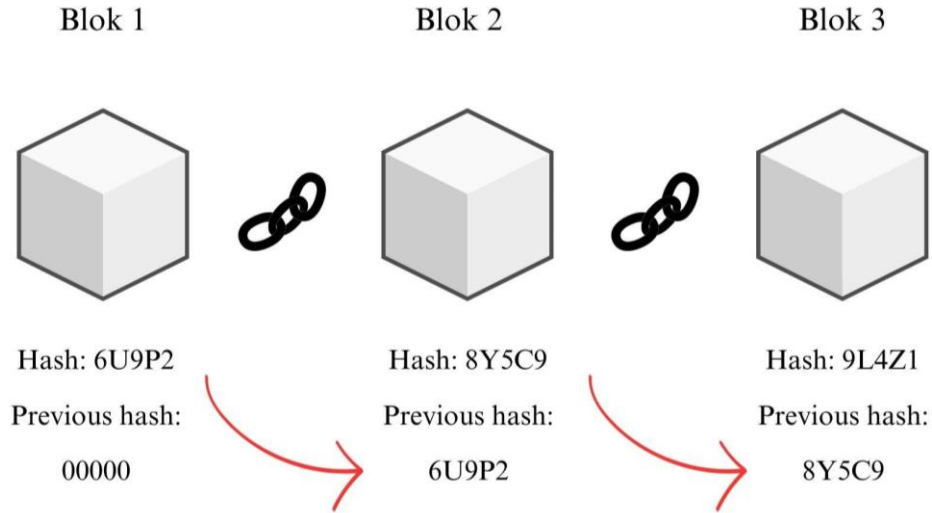
2.3.1 Blok Zincir Yapısı

Blok zincir, dağıtılmış bir defter veya veritabanıdır. Bu defter, blok adı verilen veri yapılarından oluşur. Her blok, geçerli işlemi ve blok zincirine bağlanacak önceki bloğa bir referans içerir. Bu sayede, her bir blok bir önceki bloğun verilerini korur ve zincirleme şeklinde bağlantı oluşturur.

Blok zincir'in önemli bir özelliği, merkezi olmayan bir yapıya sahip olmasıdır. Ağdaki tüm katılımcılar, bir kopyasına sahip oldukları bu defteri paylaşırlar ve güncellemeleri toplu olarak onaylar. Bu dağıtılmış yapı, verilerin tek bir yerde toplanmasını önler ve güvenilirliği artırır.

Bir işlem gerçekleştiğinde, bu işlem bir blok içerisine eklenir. Blok daha sonra ağdaki tüm katılımcılara yayılır ve onay için beklemeye alınır[8]. Doğrulama işlemi, blokların geçerliliğini doğrulamak ve ağdaki diğer katılımcılarla senkronize etmek için kriptografik algoritmalar kullanır. Bu doğrulama mekanizmasına konsensüs protokolü denir.

Bloklar onaylandıktan sonra, blok zinciri büyür ve değiştirilmez hale gelir. Her blok, içerdiği verilerin kriptografik bir karmasını içerir ve bir sonraki bloğa referans verir. Bu şekilde, bir blokta yapılan herhangi bir değişiklik tüm zinciri etkiler ve hemen görünür hale gelir.



Şekil 1. Blok zincir yapısı.

Blok zincir teknolojisinin en popüler uygulamalarından biri kripto para birimleri olmuştur. Bununla birlikte, blok zincir kullanımı kripto para birimleri ile sınırlı değildir. Örneğin, blok zincir teknolojisi tedarik zinciri yönetimine, oylama sistemlerine, sağlık kayıtlarına ve diğer birçok alana uygulanabilir. Bizim sistemimizde ise, blok zincir teknolojisi üniversite kampüs ağına uygulanacaktır.

Kısacası, bir blok zinciri dağıtılmış bir defter veya veritabanıdır. Merkezi olmayan yapısı, veri güvenilirliğini ve bütünlüğünü artırır. İşlemler bloklar halinde kaydedilir ve kriptografik algoritmalar kullanılarak doğrulanır. Bu şekilde, blok zinciri güvenli ve değişmez bir veritabanı görevi görür[9].

2.3.2 Blok zincir Çalışma Mantığı

Blok zincirin çalışma mantığı, merkezi olmayan bir yapıya sahip olan ve verilerin güvenli ve değiştirilemez bir şekilde paylaşıldığı bir sistemdir. Blok zincirin çalışma mantığı şu adımlarla açıklanabilir:

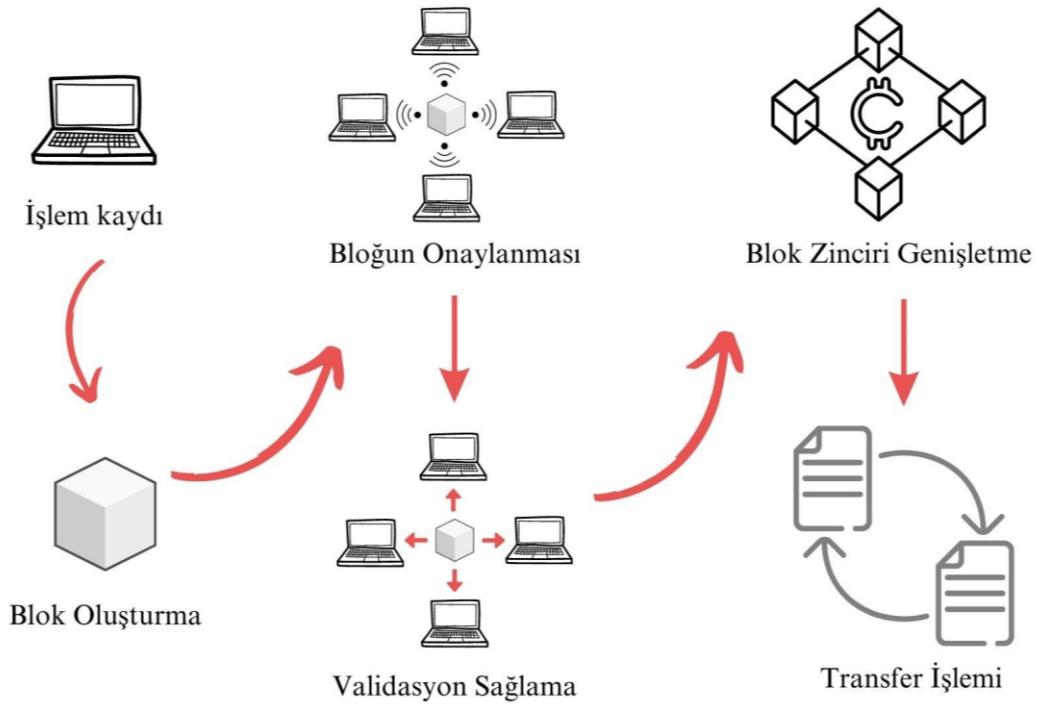
İşlem Kaydı; bir kullanıcı, bir başka kullanıcıya para göndermek istediğinde, bu işlem bir işlem olarak kaydedilir. İşlem, gönderici ve alıcı bilgilerini, miktarı ve diğer gerekli verileri içerir.

Blok Oluşturma; işlemler biriktikçe, yeni bir blok oluşturulur. Bu blok, işlemlerin listesini ve bir önceki bloğun hash değerini içerir. Hash değeri, bir bloğun benzersiz bir kimliğini temsil eder ve bloğun içeriğinin değiştirilip değiştirilmediğini tespit etmek için kullanılır.

Bloğun Onaylanması; yeni oluşturulan blok, ağdaki katılımcılara yayılır ve onay için bekler. Bloğun geçerliliğini doğrulamak için katılımcılar, kriptografik algoritmalar kullanarak bloğun içeriğini kontrol ederler. Örneğin, işlemlerin doğru ve geçerli olduğunu, imzaların doğru olduğunu ve bakiyelerin uyumlu olduğunu doğrulamak için kontroller yapılır.

Konsensüs Sağlama; bloğun geçerliliği doğrulandıktan sonra, konsensüs protokolü kullanarak blok zincire eklenir. Konsensüs protokolü, ağdaki tüm katılımcıların bloğun geçerliliği konusunda anlaşmaya varmasını sağlar. Örneğin, PoW veya PoS gibi konsensüs algoritmaları kullanılabilir.

Blok Zinciri Genişletme; onaylanan blok, blok zincirine eklenir ve değiştirilemez hale gelir. Yeni bir blok oluşturulduğunda, bu blok önceki bloğun hash değeriyle bağlantı kurar ve zincirleme bir yapı oluşturur. Bu sayede, bloklar birbirine bağlıdır ve bir blok üzerinde yapılan herhangi bir değişiklik, tüm blokları etkiler ve hemen fark edilir hale gelir.



Şekil 2. Blok zinciri çalışma mantığı.

2.3.3 Blok Zincir Avantajları

Blok zincir teknolojisi, birçok sektörde devrim niteliğinde değişikliklere yol açabilecek önemli avantajlara sahiptir. Bu avantajlar, merkeziyetsizlik, değiştirilemezlik, şeffaflık, izlenebilirlik ve dağıtıklık olarak sıralanabilir.

2.3.3.1 Merkeziyetsizlik

Merkeziyetsizlik, blok zincir teknolojisinin temel bir özelliğidir ve geleneksel sistemlerden farklı olarak merkezi bir otoriteye bağlı olmadan çalışır. Geleneksel finansal sistemlerde, para transferleri, veri saklama ve işlemlerin doğrulanması gibi faaliyetler, genellikle bir merkezi kuruluş veya otorite tarafından yönetilir. Bu durum, güvenilirlik ve kontrolün belirli bir otoriteye bağlı olmasını sağlar, ancak bu otoritenin güvenilmez veya tek bir noktada bir hata olması durumunda sistem bütünlüğü tehlikeye girebilir.

Blok zincir teknolojisi ise merkezi bir otoriteye veya aracıya ihtiyaç duymadan çalışır. Veriler, işlemler ve bloklar, dağıtılmış bir ağ üzerinde paylaşılır ve doğrulanır. Katılımcılar arasında doğrudan etkileşim gerçekleşir ve her bir katılımcı, kendi düğümünde (node) bir kopya tutar. Bu dağıtılmış doğa, güvenli bir ortam sağlar ve verilerin tek bir noktada veya otoritede toplanmasını önler.

Blok zincirin merkeziyetsizliği, güvenlik ve şeffaflık sağlama açısından önemlidir. Veriler, işlemler ve bloklar, şifreli bir şekilde blok zincire eklenir ve her bir düğüm tarafından doğrulanır. Bu doğrulama süreci, kriptografik algoritmalar ve konsensüs mekanizmaları kullanılarak gerçekleştirilir. Bu sayede, blok zincirdeki bilgilerin manipüle edilmesi veya değiştirilmesi zorlaşır.

Merkeziyetsizlik ayrıca, güvenlik ve güvenilirlik konusunda da önemli bir faktördür. Blok zincirdeki veriler, dağıtılmış bir ağ üzerinde çoğaltıldığı için, tek bir noktadaki bir arızanın veya saldırının tüm sistemi etkileme riski azalır. Verilerin şeffaf bir şekilde paylaşılması, blok zincir üzerindeki işlemlerin doğrulanabilirliğini artırır ve yanlış veya hileli işlemlerin tespitini kolaylaştırır[10]. Sonuç olarak, merkeziyetsizlik, blok zincir teknolojisinin temel bir özelliğidir ve güvenli, şeffaf ve güvenilir bir ortam sağlar.

2.3.3.2 Deęiřtirilemezlik

Deęiřtirilemezlik, blok zincir teknolojisinin önemli bir avantajıdır ve güvenilirlięi saęlamak için kullanılır. Bir kez bir bloęa eklenen veriler, geriye dönük olarak deęiřtirilmesi veya silinmesi mümkün deęildir. Bu durum, verilerin güvenlięini artırır ve manipölasyon girişimlerini önler.

Blok zincirdeki deęiřtirilemezlik, dağıtılmış doęası ve kriptografik algoritmalar kullanılarak saęlanır. Her blok, bir önceki bloęun bir parçası olarak baęlantılıdır ve verilerin doęruluęunu ve bütünlüęünü saęlamak için kriptografik karmalar kullanılır. Bu karmalar, blok içindeki verilerin matematiksel bir temsidir ve herhangi bir deęişiklik yapıldığında karmalar da deęişir.

Bir bloęa veri eklenmesi ve onaylanması için genellikle konsensüs algoritmaları kullanılır. Bu algoritmalar, aędaki katılımcılar arasında bir fikir birlięi saęlamak için kullanılır ve blokların onaylanmasını belirler. Bir blok, çoęunluęun onayını aldıęında blok zincire eklenir ve bu noktada deęiřtirilemezlik başlar.

Deęiřtirilemezlik, finansal işlemlerde büyük önem taşır. Örneęin, bir kez bir ödeme işlemi geręekleřtięinde, bu işlem blok zincire eklenir ve geriye dönük olarak deęiřtirilmesi veya silinmesi imkânsız hale gelir. Bu durum, ödeme süreklilięi ve güvenlięi saęlar. Benzer şekilde, dięer kayıt tutma alanlarında da deęiřtirilemezlik önemlidir. Örneęin, tıbbi kayıtlar, mülkiyet belgeleri veya oy verme işlemleri blok zincirde güvenli ve deęiřtirilemez bir şekilde saklanabilir.

Deęiřtirilemezlik aynı zamanda güvenilirlik ve şeffaflık saęlar. Blok zincirdeki veriler, her düęümde tutulan bir kopya üzerinde depolanır. Bu dağıtılmış doęa, verilerin tek bir noktada veya otoritede toplanmasını ve manipöl edilmesini önler. Verilerin geręeklięi ve bütünlüęü, blok zincirdeki dięer katılımcılar tarafından doęrulanabilir ve şeffaf bir şekilde görülebilir.

2.3.3.3 Şeffaflık

Şeffaflık, blok zincir teknolojisinin temel bir özellięidir ve işlemlerin ve blokların tüm katılımcılar tarafından görülebilir ve doęrulanabilir bir şekilde kaydedildięi bir halka açık defter oluřturulmasını saęlar. Bu özellik, blok zincirin güvenilirlik, doęruluk ve hesap verebilirlik saęlamasına yardımcı olur.

Blok zincirdeki her işlem, tüm ağ katılımcıları tarafından gözlemlenebilir. Bu işlemler, bloklar halinde birleştirilir ve ardışık olarak zincirleme bir yapı oluştururlar. Bu yapıda, her blok önceki bloğa bağlıdır ve geçerli olabilmesi için önceki bloğun doğrulanması gerekmektedir. Bu durum, işlemlerin gerçekliğini ve doğruluğunu kontrol etmek için katılımcıların kendi kopyalarında blok zincirini gözlemlemesini sağlar.

Şeffaflık, güven oluşturma'nın önemli bir unsuru olarak öne çıkar. Katılımcılar, herhangi bir işlemi gerçekleştiren tarafın, işlemin ne zaman, nerede ve hangi şartlar altında yapıldığını görebilirler. Aynı şekilde, işlemlerin sonucu ve etkisi de şeffaf bir şekilde görülebilir. Bu durum, işlemlerde hileli veya yanlış davranışların tespit edilmesini kolaylaştırır ve güvenli bir işlem ortamı oluşturur.

Blok zincirdeki şeffaflık, finansal işlemlerden kaynaklanan avantajların yanı sıra, diğer alanlarda da önemli etkilere sahiptir. Örneğin, kaynak dağıtımı veya yardım programlarında blok zincir tabanlı şeffaf sistemler, harcamaların izlenmesini ve kaynakların doğru bir şekilde dağıtılmasını sağlar. Ayrıca, tedarik zinciri yönetimi gibi alanlarda da şeffaflık, ürünlerin geçmişini izlemeyi ve taklitlerin önlenmesini sağlar.

Şeffaflık, blok zincir teknolojisinin gücünü artıran bir faktördür. Katılımcılar arasındaki güveni artırır ve manipülasyon girişimlerine karşı bir önlem olarak hizmet eder. Herkesin işlemleri görebilmesi ve doğrulayabilmesi, daha adil ve şeffaf bir işlem ortamı yaratır.

2.3.3.4 İzlenebilirlik

İzlenebilirlik, blok zincir teknolojisinin bir diğer önemli avantajıdır. Her bir işlem blok zincirinde ayrıntılı bir şekilde kaydedilir ve izlenebilir hale gelir. Bu sayede, işlemlerin kaynağı, geçmişi ve hedefi hakkında detaylı bilgilere erişilebilir.

Blok zincirindeki her bir işlem, bir blok içinde yer alır ve bir önceki bloğa bağlıdır. Her blok, işlemlerin bir listesini içerir ve ardışık olarak zincirleme bir yapı oluşturur. Bu yapı, işlemlerin izlenebilirliğini sağlar. Her işlem, blok zincirinde benzersiz bir kimlikle tanımlanır ve bu kimlik, işlemin ayrıntılarına, tarihe ve işlem gerçekleştiren taraflara erişmek için kullanılır.

İzlenebilirlik aynı zamanda finansal işlemlerde de büyük önem taşır. Her bir finansal işlem, blok zincirinde kaydedildiği için, işlemin kaynağı ve hedefi açık bir şekilde belirlenebilir. Bu durum, yasadışı faaliyetlerin tespitini kolaylaştırır ve finansal suçların önlenmesine yardımcı olur. Ayrıca, izlenebilirlik, vergi uyumluluğu ve raporlama gerekliliklerini yerine getirmeyi kolaylaştırır.

İzlenebilirlik, güvenilir bir izleme sistemi sağlar ve işlemlerin güvenliği ve doğruluğunu artırır. Blok zinciri, işlemlerin tüm katılımcılar tarafından görülebilir olduğu için, hileli veya yanlış işlemler kolayca tespit edilebilir. Bu durum, işlemlerin doğrulanabilirliğini artırır ve güven oluşturur.

2.3.3.5 Dağıtıklık

Dağıtıklık, blok zincirin önemli bir özelliğidir ve verilerin ve işlemlerin blok zincir ağına bağlı tüm katılımcılar arasında dağıtılması anlamına gelir. Geleneksel sistemlerin aksine, blok zincirde merkezi bir otorite veya aracıya ihtiyaç duyulmaz. Bunun yerine, katılımcılar arasında doğrudan etkileşim ve veri paylaşımı gerçekleşir.

Bir blok zincir ağı, katılımcıların kendi bilgisayarlarındaki düğümler aracılığıyla ağa katıldığı bir yapıdır. Her bir düğüm, blok zincirinin bir kopyasını tutar ve yeni blokların onaylanmasına ve eklenmesine katkıda bulunur. Bu dağıtılmış yapı, verilere yönelik tehditleri azaltır ve blok zincirin dayanıklılığını artırır.

Dağıtıklık, verilere ve işlemlere erişimi artırır. Veriler blok zincirinde tutulduğu için, her bir katılımcı verilere erişebilir ve doğrulama yapabilir. Bu, güvenilirliği artırır ve merkezi bir noktada veri saklanmasıyla ilgili riskleri azaltır. Aynı zamanda, veri kaybını da önler çünkü blok zinciri tüm katılımcılar arasında dağıtıldığı için tek bir noktada veri kaybı riski ortadan kalkar.

Dağıtıklık aynı zamanda sistem dayanıklılığını artırır. Merkezi sistemlerde, bir merkezi otoritenin veya sunucunun arızalanması veya hedef alınması durumunda sistemin çökme riski vardır. Ancak blok zincirde, veriler ve işlemler birçok düğüme dağıtıldığından, bir

düğümün arızalanması veya saldırıya uğraması durumunda bile diğer düğümler ağı devamlılığını sağlar[11].

Dağıtıklık aynı zamanda güvenilirliği ve güveni artırır. Blok zinciri, her bir işlemi ve veriyi katılımcılar arasında doğrulayarak güvenilirliği sağlar. Tek bir merkezi otoriteye veya aracıya bağımlı olmadığı için, her katılımcının ağa katkıda bulunma ve işlemleri doğrulama yeteneği vardır. Bu da güven oluşturur ve güvenlik açıklarını en aza indirir.

2.3.4 Blok Zincir Dezavantajları

Blok zincir teknolojisi, pek çok avantajı ile birlikte bazı dezavantajları da beraberinde getirir. Bu dezavantajlar, teknolojinin uygulanacağı alanlarda dikkate alınması gereken önemli faktörlerdir.

2.3.4.1 %51 Saldırıları

%51 saldırısı blok zinciri ağının güvenliğini tehdit eden bir dezavantajdır. Blok zincir ağına bağlı olan madenci kontrolünün tek bir kişi veya grup tarafından ele geçirilmesi durumunda, %51 saldırısı gerçekleştirilebilir. Bu durumda, saldırgan ağdaki blokları manipüle edebilir, işlemleri geri alabilir veya çift harcamalar yapabilir. Bu tür bir saldırı, blok zincirin güvenliğini tehlikeye atabilir ve sistemde ciddi sorunlara yol açabilir.

2.3.4.2 Verileri değiştirememe

Blok zincirdeki veriler, bir kez bloğa eklenip onaylandıktan sonra geriye dönük olarak değiştirilemez. Bu özellik, verilere güvenilirlik sağlar ve manipülasyon girişimlerini önler. Ancak, yanlışlıkla veya hatalı bir şekilde kaydedilen verilerin düzeltilmesi veya güncellenmesi zor olabilir. Bu durumda, hataların veya yanlış bilgilerin kalıcı olması riski ortaya çıkabilir.

2.3.4.3 Geniş depolama alanı ihtiyacı

Blok zincir teknolojisi, tüm işlem geçmişini ve blokları her katılımcıya dağıtarak çalışır. Bu da büyük miktarda depolama alanı gerektirir. Özellikle ölçeklendirme sorunuyla karşılaşıldığında, blok zincirin büyümesi ve depolama gereksinimlerinin artması sorunlara neden olabilir. Bu durum, bazı uygulamalar için pratik olmayabilir ve depolama maliyetlerini artırabilir.

2.3.5 Genesis Blok

Genesis blok, kampüs ağındaki kullanılacak blok zincir tabanlı ödül sisteminin başlangıç noktasıdır. Bu blok, blok zincirinin temel bloğunu oluşturur ve diğer tüm blokların referans noktası olarak görev yapar.

Kampüs ağı başlatıldığında, öncelikle genesis blok oluşturulur ve blok zinciri inşa edilmeye başlanır. Genesis blok, diğer bloklardan farklı olarak önceki bir bloğa referans içermez çünkü bu blokla birlikte blok zinciri henüz başlamıştır.

Genesis blok, kampüs ağındaki kullanılacak ödül sisteminin temel parametrelerini belirlemek için özel olarak tasarlanmış bir blok içeriğine sahiptir. Örneğin, blok içeriğinde kampüsün adı, sembolü veya logo gibi kampüse özgü bilgiler yer alabilir. Ayrıca, kampüs ağının başlangıç tarihi, ödül puanlarının değeri, öğrencilerin veya fakülte üyelerinin gerçekleştirmeleri gereken görevlerin detayları gibi bilgiler de içerebilir.

Kampüs ağındaki kullanılacak ödül sistemi, katılımcıların çeşitli görevleri tamamlamasına dayalı olabilir. Örneğin, döküman okuma, pet şişe atma gibi görevler ödül kazanmalarını sağlayabilir. Katılımcılar bu görevleri tamamladıkça ödül puanları kazanır ve bu puanlar daha sonra belirli bir kripto para birimiyle ödül olabilir.

Genesis bloğu, diğer bloklar gibi benzersiz bir hash değeri ile tanımlanır. Bu hash değeri, bloğun içeriğinin bütünlüğünü ve bloğun değiştirilip değiştirilmediğini tespit etmek için kullanılır[12].

Kampüs ağındaki kullanılacak bu blok zincir tabanlı ödül sistemi, genesis blok ile başlar ve katılımcıları teşvik etmek, motive etmek ve ödüllendirmek amacıyla kullanılır. Genesis blok, blok zincirinin başlangıç noktasını temsil eder ve sistemin güvenli ve güvenilir bir şekilde çalışmasını sağlar.

2.3.6 İşlem

Kampüs ağındaki blok zincir tabanlı ödül sisteminde, işlemler (transactions), katılımcıların ödül puanlarını kazanmak veya kullanmak için gerçekleştirdikleri eylemleri temsil eder. Her bir işlem, blok zincirine eklenmeden önce doğrulanır ve onaylanır.

Blok zincir tabanlı ödül sistemi projemizde bir işlem gönderici, alıcı, miktar ve zaman bileşenlerinden oluşur:

Gönderici, işlemi başlatan kişinin veya hesabın adresi veya kimliğidir. Ödül sistemindeki işlemde, gönderici ödül puanlarını kullanmak veya transfer etmek isteyen kişiyi temsil eder. Gönderici, kendi hesabından belirli bir miktar ödül puanını düşerek işlemi gerçekleştirir.

Alıcı, işlem sonucunda ödül puanlarının gönderildiği kişinin veya hesabın adresi veya kimliğidir. Ödül sistemindeki işlemde, alıcı ödül puanlarını kazanmak veya transfer edilmek isteyen kişiyi temsil eder. Alıcı, ödül puanlarını kendi hesabına aktarılmasını sağlar.

Miktar, gönderilen veya alınan ödül puanlarının miktarını veya değerini belirtir. İşlemde belirtilen miktar, göndericinin hesabından düşülerek alıcının hesabına eklenir. Miktar, ödül puanlarının transfer edilen veya kazanılan miktarını ifade eder.

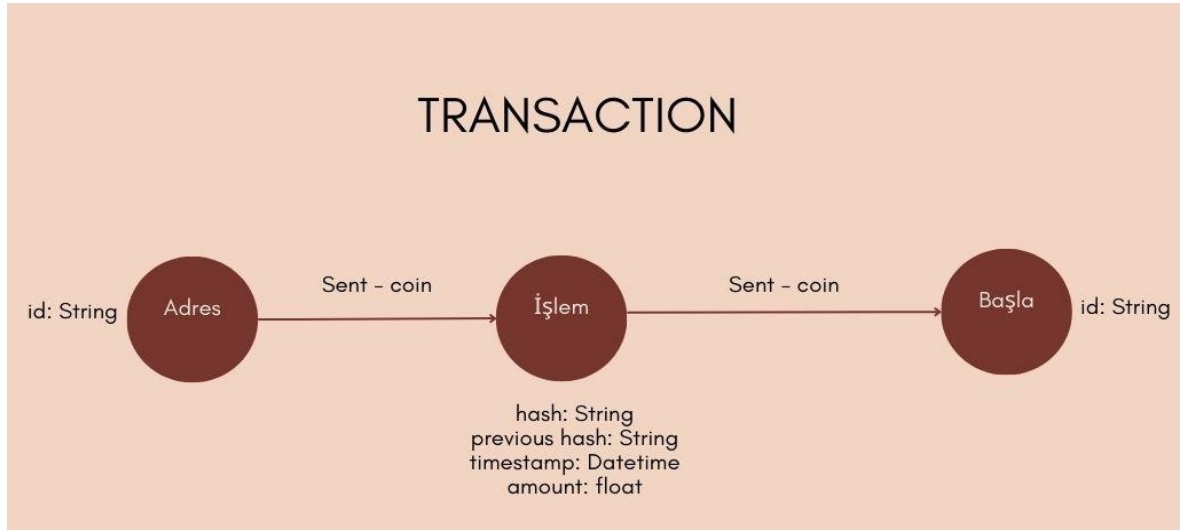
Zaman, işlemin gerçekleştiği tarih ve saat bilgisini temsil eder. İşlem, belirli bir zaman damgası ile kaydedilir ve blok zincirine eklenir. Zaman bilgisi, işlem sürecinin izlenmesi, işlemlerin sıralamasının sağlanması ve işlem geçmişinin doğrulanması için önemlidir.

Örneğin, bir öğrenci kütüphaneden kitap ödünç aldığı anda, bir işlem gerçekleşir. Bu işlemde, öğrencinin hesabından belirli bir miktar ödül puanı düşülerek kütüphanenin hesabına aktarılır. İşlem, öğrencinin gönderici adresini, kütüphanenin alıcı adresini, ödül puanı miktarını ve geçerli bir zaman damgasını içerir. Bu işlem blok zincirine eklenir ve diğer katılımcılar tarafından doğrulanır.

Blok zincir tabanlı ödül sistemindeki işlemler, merkezi bir otoriteye veya aracıya ihtiyaç duymadan doğrulanır ve gerçekleştirilir. Her işlem, blok zincirinde kalıcı olarak kaydedildiğinden, tüm katılımcılar tarafından takip edilebilir ve denetlenebilir. Bu sayede, işlemlerin şeffaflığı ve güvenilirliği sağlanır.

İşlemler, kampüs ağında yapılan her türlü ödül kazanma veya harcama faaliyetini temsil eder. Bu, döküman okuma, pet şişe atma gibi görevlerin tamamlanması, etkinliklere katılım, projelerin sunumu gibi aktiviteleri içerebilir. Her işlem, blok zincir tabanlı ödül sisteminin

hedeflerine ulaşılmasına katkıda bulunur ve katılımcılara güçlü bir motivasyon kaynağı sağlar.



Şekil 3. Blok zincir tabanlı ödül sistemi işlem yapısı.

2.3.7 Blok

Blok zincir tabanlı ödül sisteminde, işlemler bloklar halinde gruplandırılır ve bloklar ardışık olarak birbirine bağlanarak oluşturulan bir blok zinciri oluşturur. Her blok, bir dizi işlemi içerir ve bir önceki bloğun hash değerini referans alır.

Blok zincir tabanlı ödül sisteminde bir blok hash değeri, blok numarası, önceki bloğun hash değeri, işlemler ve zaman damgası bileşenlerini içerir.

Blok numarası, bloğun blok zinciri içindeki benzersiz sırasını belirleyen bir sayıdır. Bu numara, blokların hangi sırayla eklenildiğini gösterir ve blokların doğru bir şekilde yerleştirilmesini sağlar.

Önceki Blok Hash değeri, bir bloğun önceki bloğa referans veren hash değeridir. Bu hash değeri, bir önceki bloğun tüm verilerinin işlenmesiyle elde edilir. Önceki bloğun hash değeri, mevcut bloğun içerisinde yer alır ve blokları birbirine bağlayarak bir blok zinciri oluşturur.

İşlemler, bir blokta yer alan işlemler, blok zinciri üzerinde gerçekleştirilen ödül puanı transferleri veya kullanımlarını temsil eder. İşlemler, bloğun veri içeriğini oluşturan önemli bileşenlerdir.

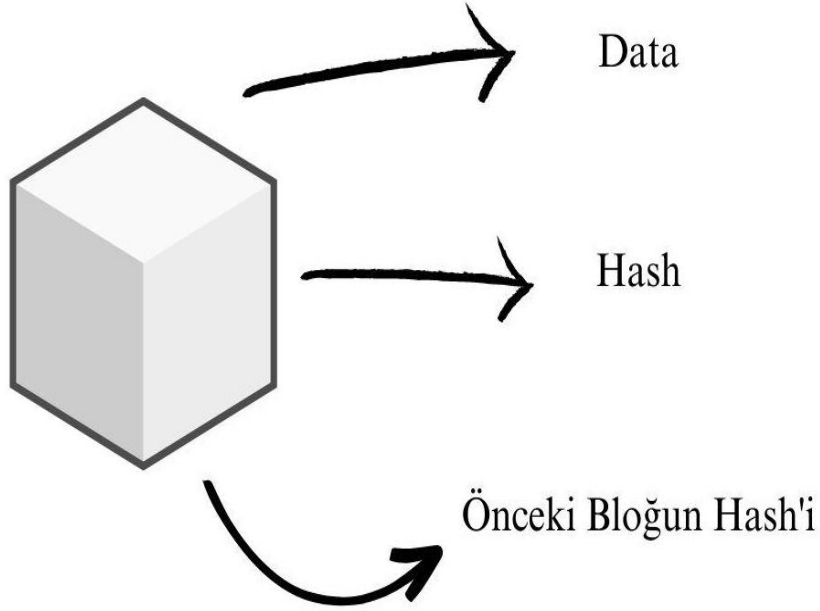
Zaman Damgası, bir bloğun oluşturulduğu zamanı belirten bir damgadır. Bu zaman damgası, bloğun hangi tarih ve saatte oluşturulduğunu gösterir. Zaman damgası, bloğun oluşturulma sürecine ilişkin bir referans noktası sağlar ve blokların zaman içindeki sıralamasını belirler.

Hash Değeri, bir bloğun benzersiz kimliğini temsil eden ve bloğun içeriğiyle bağlantılı olan bir kriptografik değerdir. Bloğun içeriği (blok numarası, önceki blok hash'i, işlemler, zaman damgası) belirli bir hash algoritması kullanılarak işlenir ve sabit bir uzunlukta benzersiz bir hash değeri elde edilir. Bu hash değeri, bloğun bütünlüğünü ve değiştirilmezliğini sağlar.

Her blok, işlemleri toplar ve bu işlemleri doğrular. Daha sonra, bloğun hash değeri hesaplanır ve blok zincirine eklenir. Bir bloğun hash değeri, bloktaki tüm verilerin kriptografik bir algoritma kullanılarak işlenmesiyle elde edilir.

Blok zinciri, blokların ardışık olarak birbirine bağlanmasıyla oluşur. Bir blok, önceki bloğun hash değerini referans alır ve bu sayede tüm bloklar birbirine bağlanır. Her yeni blok, bir önceki bloğun hash değerini içerir, böylece blokların sırası ve bütünlüğü korunur.

Blokların zincirleme yapısı ve kriptografik hash fonksiyonları sayesinde blok zinciri değiştirilemez hale gelir. Bir bloğun verileri değiştirilirse, o bloğun hash değeri de değişir ve bu durum blok zincirindeki diğer bloklarla uyumsuzluk oluşturur. Bu nedenle, bir bloğun içeriği değiştirilmek istenirse, tüm sonraki blokların da güncellenmesi gerekmektedir. Bu özelliği sayesinde blok zinciri, güvenli ve değiştirilemez bir kayıt defteri olarak kullanılabilir.



Şekil 4. Blok yapısı.

2.3.8 Cüzdan

Cüzdan, blok zincir tabanlı ödül sistemlerinde kullanılan ve kullanıcının dijital varlıklarını depoladığı bir dijital cüzdandır. Bir cüzdan, kullanıcının kripto para birimlerini saklamasına, göndermesine ve almasına olanak tanır.

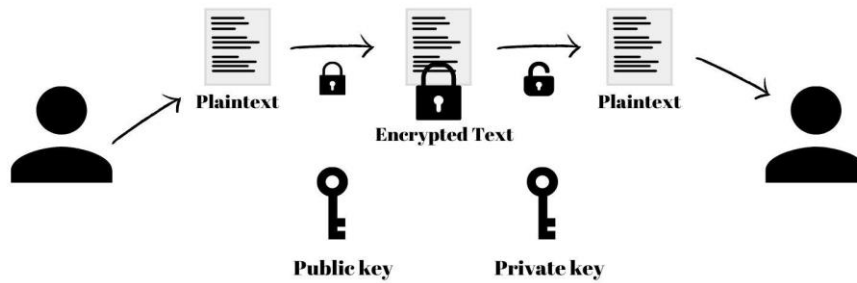
Bir cüzdan, genellikle kullanıcının açık anahtarı ve özel anahtarını içerir. Açık anahtarı, diğer kullanıcıların size kripto para göndermesine izin veren bir adrestir. Özel anahtar ise, cüzdanınızla yapılan işlemleri imzalamak ve varlıklarınızı korumak için kullanılan gizli bir anahtardır.

Cüzdanlar, çeşitli şekillerde ve platformlarda mevcut olabilir. Örneğin, masaüstü cüzdanları bilgisayarda çalışan yazılımlar olarak bulunabilir. Mobil cüzdanlar, akıllı telefonlar için özel olarak tasarlanmış uygulamalar aracılığıyla erişilebilir. Ayrıca, web tabanlı cüzdanlar da çevrimiçi bir platformda erişilebilirlik sağlar.

Cüzdanlar, kullanıcıların kripto para birimlerini güvenli bir şekilde saklamalarını sağlamak için güvenlik önlemleriyle korunurlar. Özel anahtarların güvenli bir şekilde saklanması önemlidir, çünkü bir kullanıcının özel anahtarları ele geçirildiğinde, varlıklarını kaybetme riskiyle karşı karşıya kalabilir.

Cüzdanlar aynı zamanda kullanıcılara işlem geçmişini görüntüleme, farklı kripto para birimlerini takip etme ve transfer işlemleri gerçekleştirme gibi işlevlere de sahiptir. Kullanıcılar genellikle bir cüzdan aracılığıyla diğer cüzdanlara kripto para transferi yapabilir, işlem yapabilir ve varlıklarını yönetebilir.

Cüzdanlar, blok zincir teknolojisinin merkezi olmayan ve güvenli doğasını kullanarak kullanıcılara kripto para birimlerini kontrol etme ve yönetme imkânı sunar. Kullanıcılar, kendi cüzdanları üzerinde tam kontrole sahiptir ve üçüncü taraflara güvenmek zorunda kalmadan işlemlerini gerçekleştirebilirler[13].



Şekil 5. Blok zincir çalışma mantığı.

2.3.9 Consensus Algoritmaları

Consensus algoritmaları, blok zincir tabanlı sistemlerde kullanılan ve tüm katılımcıların anlaşmaya varmasını sağlayan protokollerdir. Bu algoritmalar, dağıtılmış ağdaki farklı düğümler arasında fikir birliği sağlanmasını hedefler ve blok zincirinin güvenilir ve tutarlı bir şekilde güncellenmesini sağlar.

Consensus algoritmaları, blok zinciri üzerinde yapılan değişikliklerin kabul edilmesi ve onaylanması için kullanılır. İşlem doğrulama, yeni blokların eklenmesi ve çifte harcama gibi saldırılarla mücadele gibi görevleri yerine getirirler. Bu algoritmalar, ağdaki farklı katılımcıların oybirliği sağlamasını ve güvenli bir şekilde iş birliği yapmalarını sağlar. PoW ve PoS, en yaygın kullanılan consensus algoritmalarıdır.

2.3.9.1 Proof of Work

Proof of Work, blok zincir tabanlı bir sistemde konsensüs sağlamak için kullanılan bir algoritmadır. Temel amacı, ağdaki katılımcıların belirli bir işlemi gerçekleştirmeleri için hesaplama gücü harcamalarını gerektirmektedir. PoW, Bitcoin'in orijinal beyaz kağıdında tanıtılan bir mekanizmadır. PoW madencilik süreci, zorluk seviyesi, iş kanıtı, blok onayı gibi temel bileşenlerden oluşmaktadır.

Madencilik sürecinde PoW kullanılarak işlem yapmak isteyen bir kullanıcı, belirli bir görevi gerçekleştirmek için hesaplama gücünü kullanır. Bu görev, belirli bir sayıyı (nonce) bulmak için hesaplamalar yapmaktır. Sayının bulunması için çeşitli hesaplamalar yapılır ve bu hesaplamaları gerçekleştiren kullanıcıya madenci denir.

Zorluk seviyesi, PoW algoritmasında bulunması gereken nonce değerinin zorluğunu belirler. Zorluk seviyesi, ağdaki madencilik gücüne bağlı olarak düzenli aralıklarla ayarlanır. Zorluk seviyesi yüksek olduğunda, daha fazla hesaplama gücü gerektirir ve bulunması daha zor hale gelir.

İş kanıtı aşamasında, bir madenci, doğru nonce değerini bulduğunda, buluşunu diğer ağ katılımcılarına kanıtlar. Bulduğu değeri diğer madencilere göndererek ve işlemi doğrulayan bir "iş kanıtı" sağlayarak bunu yapabilir. İş kanıtı, diğer kullanıcıların doğrulama yapmasına olanak tanır.

Blok onayı aşamasında, madenciler buldukları geçerli nonce değerlerini yeni bir bloğun başına ekler ve bloğu ağdaki diğer katılımcılara yayımlar. Diğer katılımcılar, bu bloğu kendi yerel kopyalarına ekler ve zincirin uzunluğunu doğrular. En uzun zincir, doğrulanmış ve onaylanmış kabul edilir.

2.3.9.2 Proof of Stake

Proof of Stake, Ethereum 2.0 gibi bazı blok zincir ağlarında kullanılan bir consensus algoritmasıdır. Bu algoritma, katılımcıların blokları oluşturma hakkını ellerinde bulundurdıkları varlıklarının miktarına dayandırır. Yani, bir kişinin ağdaki oy hakkı, elindeki kripto para birimi miktarına bağlıdır. PoS algoritmasında, blokların doğrulanması ve yeni blokların eklenmesi için rastgele bir seçim süreci vardır. Seçilen düğüm, bloğu ekler ve ödül alır. PoS, enerji verimliliği açısından PoW'a göre avantaj sağlar ve daha az hesaplama gücü gerektirir. Aynı zamanda, PoS algoritması, kullanıcılara ödül olarak yeni kripto para birimi üretme yerine, var olan kripto paraları tutmaları ve kullanmaları için teşvik sağlar. Bu, ağın daha sürdürülebilir bir şekilde çalışmasına yardımcı olur. PoS jeton sahipliği, blok üretme, validator seçimi, kötü niyetli davranışlarla mücadele ve ödüllendirme gibi temel bileşenlerden oluşur.

PoS'de, jeton sahipliği kavramı, blok üretme hakkının belirlenmesinde kullanılır ve bu hak, kullanıcının sahip olduğu jeton miktarına dayanır. Kullanıcının ağda daha fazla jetona sahip olması, blok üretme olasılığını artırır.

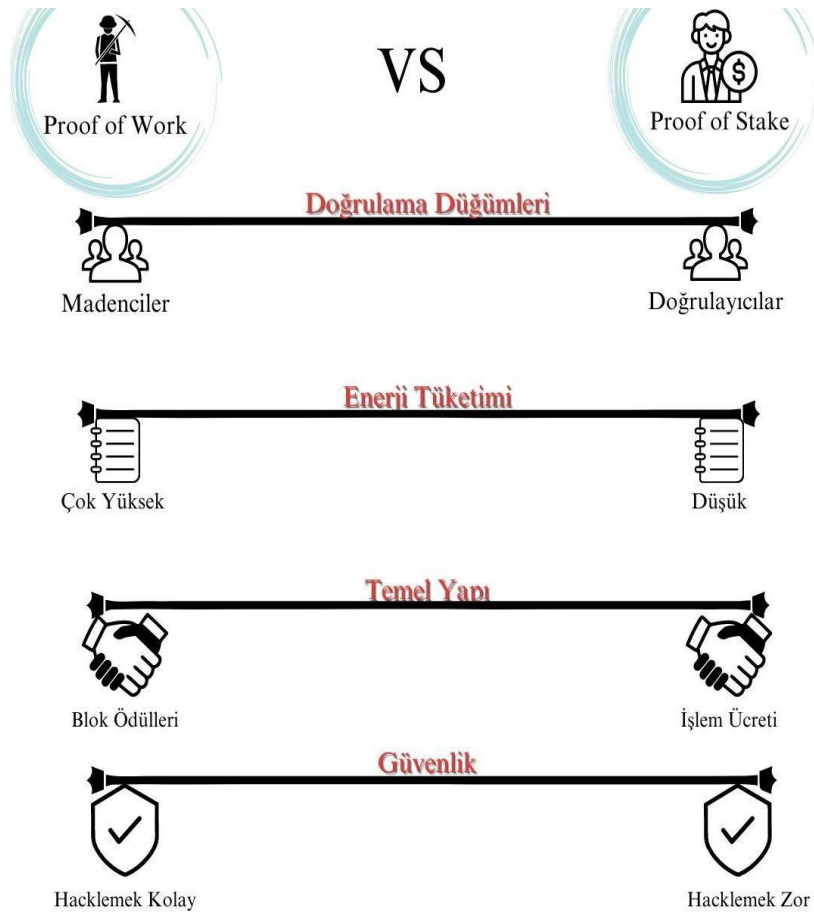
PoS'de, blok üretme işlemi için bir "hakem" veya "validator" seçimi yapılır. Bu seçim, bir bloğu doğrulamak ve blok zincirine eklemek için sorumlu olan kişiyi belirler. Bu seçim, jeton sahipliğiyle belirlenir. Daha fazla jetona sahip olan kullanıcılar, blok üretme hakkını daha yüksek bir olasılıkla kazanır. Bu sayede, enerji tüketimi ve işlemci gücüne dayalı PoW algoritmasının aksine daha enerji verimli bir yöntem elde edilir.

PoS'de, validator seçimi genellikle rastgele bir seçim yerine kullanıcının blok üretme hakkını, jetonlarını kilitli durumda tutmasına bağlı olarak belirler. Bu, kullanıcıların belirli bir süre boyunca jetonlarını kilitli durumda bırakmalarını gerektirir. Kilitli jetonlar, ağın güvenilirliğini artıran bir teminat görevi görür.

PoS, kötü niyetli davranışlarla mücadele etmek için çeşitli mekanizmalara sahiptir ve bu sayede ağdaki kullanıcıların kötü niyetli davranışlara karşı önlem almasını sağlar. Bunlardan biri, kullanıcının kötü davranışı tespit edilirse jetonlarının bir kısmının veya tamamının kaybedilmesini içerebilir. Bu tür bir mekanizma, ağın güvenliğini sağlamak için kullanıcıları teşvik eder.

Ödüllendirme, PoS'de blok üretme hakkı kazanan kullanıcıları ödüllendirmek için bir mekanizma sağlar. Blok üreten kullanıcılar, yeni oluşturulan bloklardan elde edilen işlem ücretleri ve blok ödüllerini alır. Bu, kullanıcıları ağı katılım ve işlem yapma konusunda teşvik eder.

PoW ve PoS, blok zincir tabanlı sistemlerde konsensüs sağlamak için kullanılan iki önemli mekanizmadır. Her birinin kendi avantajları ve dezavantajları vardır ve projenin ihtiyaçlarına bağlı olarak tercih edilirler. Bu mekanizmalar, blok zincir teknolojisinin güvenli ve dağıtık doğasını sürdürmek için önemli rol oynar.



Şekil 6. Consensus algoritmalarının karşılaştırılması.

2.3.10 Blok Zincirde Kullanılacak Karma Algoritması

Kullanılacak karma (hash) algoritması, blok zincir tabanlı ödül sisteminizde güvenliğini sağlamak amacıyla SHA-1 şifrelemesidir. SHA-1, Amerikan Ulusal Standartlar Enstitüsü (ANSI) tarafından tasarlanan bir kriptografik karma fonksiyonudur. Karma fonksiyonları, girdileri sabit boyutlu çıktıya dönüştüren matematiksel fonksiyonlardır. SHA-1, özellikle dijital imza ve mesaj doğrulama işlemleri gibi kriptografik uygulamalarda yaygın olarak

kullanılmıştır. Bu algoritma, bir girdi verisini 160-bit uzunluğunda bir çıktıya dönüştürerek verinin bütünlüğünü sağlar. Karma fonksiyonları, güvenliği ön planda tutan bir yaklaşımı temsil eder ve blok zinciri tabanlı ödül sisteminizde her bir bloğun benzersiz bir kimlik numarasına sahip olmasını sağlayarak verilerin güvenliğini artırır. SHA-1 algoritması, verinin değiştirilmesi, manipüle edilmesi veya tahmin edilmesi zor olan bir çıktı üretir, bu da sisteminizdeki blokların güvenli bir şekilde birbirine bağlanmasını ve manipülasyonlara karşı dirençli olmasını sağlar.

2.4 Oluşturulacak Ağ Yapısı

Bir blok zincir tabanlı proje geliştirirken, oluşturulacak ağ yapısı, sisteminizin nasıl çalışacağını ve katılımcıların nasıl etkileşimde bulunacağını belirleyen kritik bir unsurdur. Ağ yapısı, blok zincirine katılan düğümler arasındaki iletişimi ve veri paylaşımını düzenler.

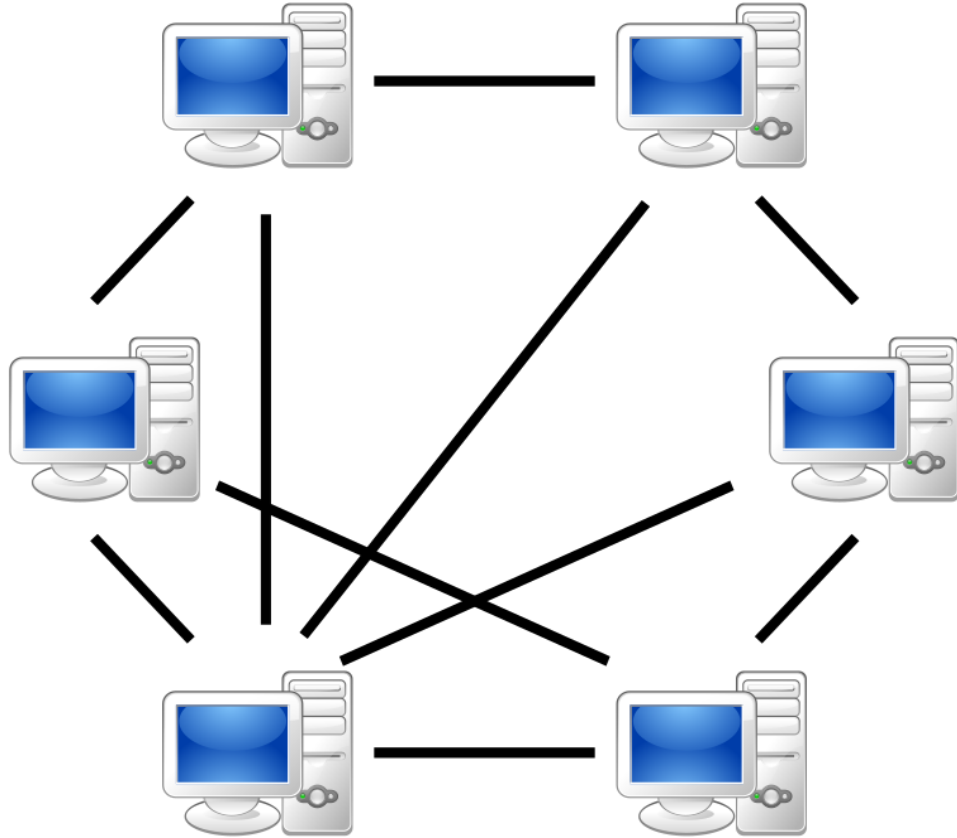
Blok Zincir Tabanlı Ödül Sisteminde genel olarak, bir blok zinciri ağı, düğüm, p2p ve websockets bileşenlerinden oluşmaktadır.

Bir blok zinciri ağındaki düğümler, ağa katılan ve işlem gerçekleştiren cihazları temsil eder. Her düğüm, blokları doğrulama, işlem yapma ve yeni blokları oluşturma yeteneğine sahiptir. Düğümler, ağıdaki verilerin güvenliğini ve bütünlüğünü sağlamak için kriptografik algoritmalar kullanır. Blok zinciri ağına katılan her düğüm, ağın güvenliğine ve konsensüs sağlamaya katkıda bulunur.

Bir blok zinciri ağı, genellikle P2P ağ yapısı kullanır. Bu, merkezi bir sunucuya veya otoriteye bağımlı olmadan düğümlerin doğrudan birbirleriyle iletişim kurabildiği bir yapıdır. P2P ağı, verilerin düğümler arasında paylaşılmasını, blok zincirinin güncellenmesini ve konsensüsün sağlanmasını kolaylaştırır. Bu yapı, ağın dağıtılmış ve güvenli bir şekilde çalışmasını sağlar.

WebSockets, istemci ve sunucu arasında sürekli açık bir bağlantı sağlar. Bu bağlantı, katılımcıların anlık olarak veri alışverişinde bulunmasına izin verir. İstemci tarafından gönderilen veriler, sunucu tarafından hızlı bir şekilde işlenir ve diğer katılımcılara anında yayılır. Bu sayede, görevlerin tamamlanması, ödül puanlarının güncellenmesi ve diğer etkileşimler anlık olarak gerçekleştirilebilir.

Ağ yapısı oluşturulurken, düğümler arasındaki veri senkronizasyonu, konsensüs algoritmalarının uygulanması, güvenlik mekanizmalarının belirlenmesi ve kullanıcıların ağa erişimini sağlamak gibi faktörler dikkate alınmıştır[14].



Şekil 7. Blok zincir tabanlı sistemde kullanılan ağ yapısı.

2.5 Uygulama Testleri

Uygulama testleri, blok zinciri tabanlı ödül sisteminizin doğru ve güvenilir bir şekilde çalışmasını sağlamak amacıyla kapsamlı bir test sürecini içerir. Bu testler, önceden belirlenmiş görevlerin (ör. döküman okuma, pet şişe atma) sisteminizin beklentilere uygun şekilde işlediğini doğrulamayı hedefler.

Veri Doğruluğu Testleri, Sisteme girilen verilerin doğru bir şekilde kaydedildiğini ve işlendiğini doğrulamak için veri doğruluğu testleri yapılır. Örneğin, bir kullanıcının döküman okuma görevini tamamlaması durumunda ilgili verilerin sisteme doğru bir şekilde kaydedildiğini ve kullanıcının ödül aldığını test eder.

İşlevsellik Testleri, Sisteminizin işlevselliğini doğrulamak için çeşitli senaryolar üzerinde testler yapılır. Örneğin, kullanıcıların belirli bir görevi tamamlaması ve bu tamamlanmış görevin sistem tarafından doğru bir şekilde kaydedilmesi test edilir. Ayrıca, kullanıcıların ödül puanlarını görüntülemesi, kullanıcılara ödül puanı transferi yapılması gibi işlevler de test edilir.

Performans Testleri, Sisteminizin yük altında nasıl performans gösterdiğini test etmek için performans testleri gerçekleştirilir. Örneğin, sistemde aynı anda çok sayıda kullanıcının görevleri tamamlaması ve ödül puanı transferleri gerçekleştirmesi simüle edilir. Bu testler, sistemde herhangi bir performans sorunu olup olmadığını ve sistem kaynaklarının etkin bir şekilde kullanıldığını değerlendirir[15].

Güvenlik Testleri, Sisteminizin güvenliğini test etmek için güvenlik testleri yapılır. Bu testler, sistemde herhangi bir zayıf nokta veya güvenlik açığı olup olmadığını belirlemeyi amaçlar. Örneğin, kullanıcı kimlik doğrulama süreci, veri şifreleme yöntemleri ve diğer güvenlik önlemleri test edilir.

Uyumluluk Testleri, Sisteminizin diğer bileşenler ve harici hizmetlerle uyumlu bir şekilde çalıştığını doğrulamak için uyumluluk testleri yapılır. Örneğin, sistemde kullanılan diğer yazılım bileşenlerinin, veritabanı sistemlerinin ve harici API'ların uyumluluğu test edilir[16].

2.6 Uygulama Geliştirme Ortamı

Kullanıcı arayüzü tasarımı için Visual Studio ile Windows Forms Tasarımcısı kullanılmıştır. Visual Studio, Microsoft tarafından geliştirilmiş bir entegre geliştirme ortamıdır. Windows Forms, Microsoft tarafından geliştirilen bir grafiksel kullanıcı arayüzü (GUI) çerçevesidir. Windows Forms, .NET Framework ile birlikte gelir ve .NET programlama dilleri, özellikle

C# ile birlikte kullanılır. Windows Forms, kullanıcı arayüzü geliştirme için kullanılan bir araçtır ve Microsoft Visual Studio gibi geliştirme ortamlarında kullanılabilir. Bu araç, butonlar, metin kutuları, listeler, menüler ve diğer grafik öğeleri gibi birçok önceden oluşturulmuş kontrolü içerir. Ayrıca, özel kullanıcı arayüzü öğeleri de oluşturulabilir. Windows Forms, masaüstü uygulamaları geliştirmek için kullanılabilir. Bu uygulamalar, bilgisayarın işletim sistemi üzerinde çalışır ve internet bağlantısına ihtiyaç duymaz. Windows Forms, veritabanı işlemleri gibi diğer .NET Framework özellikleri ile de entegre edilebilir.

Bu materyal ve yöntemler, çalışmamızda kullanılan araçları ve teknolojileri ayrıntılı olarak açıklamaktadır ve benzer bir blok zinciri uygulaması geliştirmek isteyen araştırmacılara yardımcı olabilir.

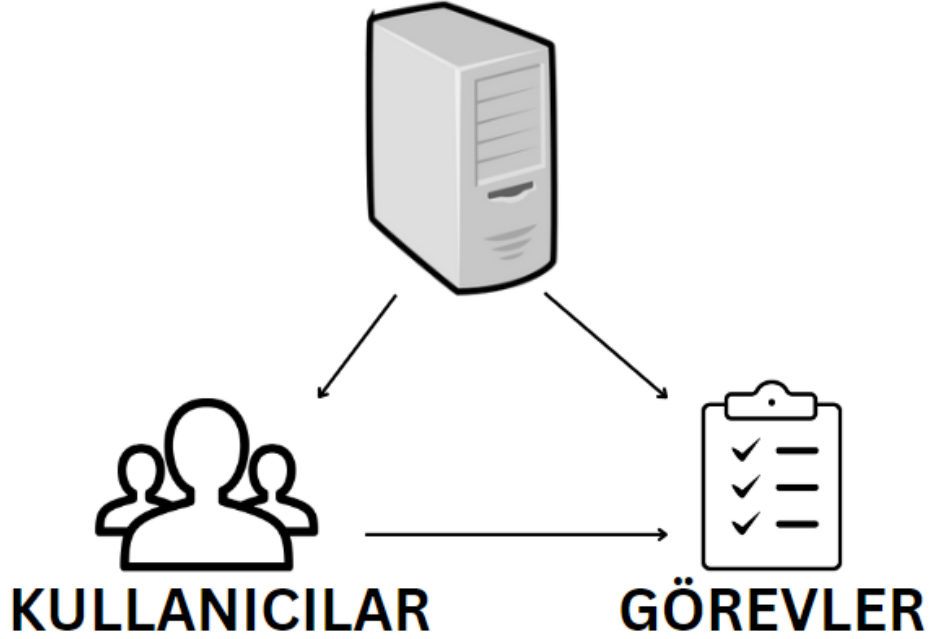
3.BULGULAR VE TARTIŞMA

Bu kısımda çalışma sırasında geliştirilen projenin hedeflenen ve elde edilen sonuçlarına yer verilmiş, ardından elde edilen sonuçlar ile hedeflenenler kıyaslanarak sistemin faydaları, eksiklikleri ve başarısı tartışılmıştır.

3.1 Blok Zincir Uygulaması

Çalışma kapsamında blok zincir tabanlı olarak bir ödül sistemi tasarlanması hedeflenmiş ve belirlenen hedef doğrultusunda çeşitli uygulamalar geliştirilerek, bir sistem oluşturulmuştur. Çalışmada geliştirilen blok zincir uygulaması, ödül sistemi için şeffaf ve güvenli bir ortam sağlamak amacı ile tasarlanmıştır. Aynı zamanda ödüllerin blok zincir sisteminde saklanarak izlenebilirliği ve denetlenebilirliğinin artırılması amaçlanmıştır. Öncelikle bir blok zincir ağı oluşturulmuş ve kullanıcılar arasında veri paylaşımı, zincir senkronizasyonu ve işlem gerçekleştirme imkânı sağlayacak bir dağıtık yapı oluşturulmuştur. Kullanıcılara atanan görevler kapsamında, görev tamamlanma durumuna göre ödül almaya hak kazanan kullanıcılara ödül verilmesi ve bunun kaydının da blok zincir üzerinde tutulması hedeflenmektedir. Blok zincir uygulaması ayrıca veri güvenliği ve bütünlüğü sağlama konusunda da önemli bir rol oynamaktadır. Her bir veri işlemi, blok zincir ağına dahil edilen bir blok olarak kaydedilmekte ve bu blokların ardışık olarak sıralanması ile veri bütünlüğü sağlanmaktadır. Ayrıca her bir blok üzerinde yapılan değişiklikler geriye dönük olarak izlenebilir ve manipülasyon girişimleri tespit edilebilir.

KONTROL MEKANİZMASI



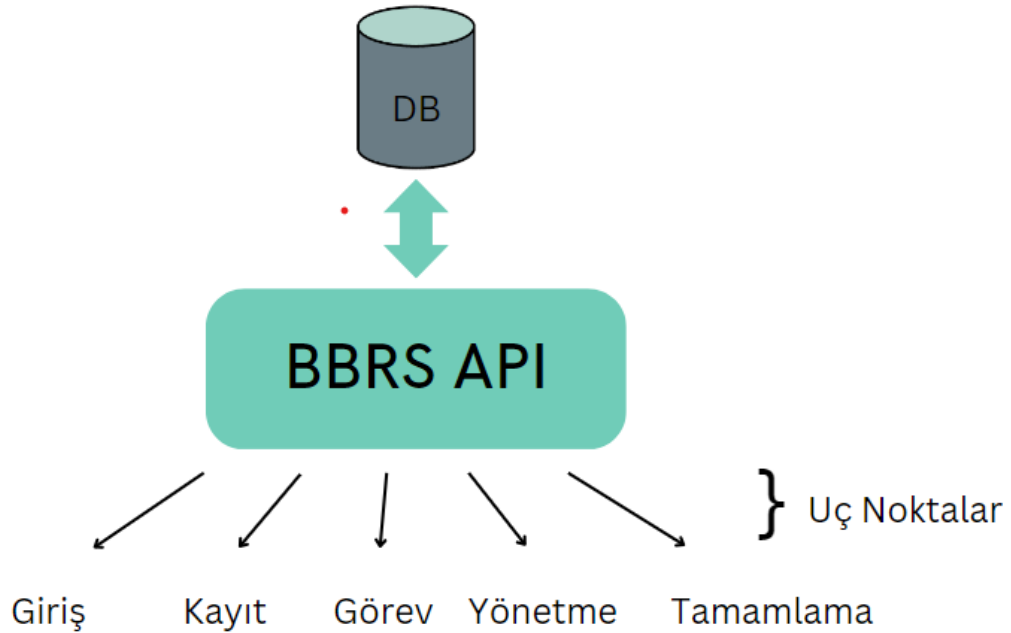
Şekil 8. Uygulamanın temellerini gösteren şekil.

Çalışmada geliştirilen blok zincir uygulaması 3 temel bileşen üzerinde durmaktadır. Bunlar bir kontrol mekanizması, kullanıcılar ve kullanıcılara ait görevlerdir. Sisteme üye olarak giriş yapan kullanıcılar, sistemde tanımlı görevleri tamamlayarak ödül almaya hak kazanır, sistemin kontrol mekanizması kullanıcıların görev tamamlama durumunu sürekli olarak kontrol eder ve ödül almaya hak kazanan kullanıcılara, hak ettikleri ödülü vererek bunu bloğa yazar ve zincire ekler, sonrasında zinciri talep eden kullanıcılar arasında dağıtır. Kullanıcılar sisteme her giriş yaptıklarında zincirlerinin güncelliğini kontrol ederler ve zincirlerinin güncel olma durumuna göre istek yaparak, oluşturulan P2P ağında diğer kullanıcılardan zincirlerini alarak kontrol sonunda güncel zincire kavuşup bunu kendi zincirlerinin yerine yazarlar, böylece kendi zincirlerini de güncellemiş olurlar.

3.1.1 API Tasarımı

Bu çalışmada, blok zincir tabanlı ödül sistemi için API tasarımı büyük önem taşımaktadır. API, sistem kullanıcılarının blok zincir ödül sistemi ile etkileşimde bulunmalarını sağlayan bir arayüzdür. API tasarımı, kullanıcıların verileri almasını, işlem yapmasını ve ödül sistemi ile etkileşime geçmesini kolaylaştırmak amacıyla özenle düşünülmelidir. API tasarımı

yapılırken, öncelikli olarak kullanıcı ihtiyaçları ve ödül sistemi gereksinimleri dikkate alınmalıdır. API tasarımında, uygun veri formatları ve protokolleri kullanmak da önemlidir. JSON, yaygın olarak kullanılan bir veri formatıdır ve genellikle API istek ve yanıtlarında tercih edilen formattır. RESTful API tasarım prensipleri, veri işlemlerini basitleştirmek ve birlikte çalışabilirlik sağlamak için yaygın olarak kullanılan bir yaklaşımdır. Bu çalışmadaki API tasarımında RESTful prensipleri, veri işlemleri için ise JSON veri formatı kullanılmıştır. API tasarımı ayrıca güvenlik önlemlerini de içermelidir. Bu çalışma kapsamında geliştirilen API ve tasarımı ile birlikte kullanıcıların sistem ile rahat bir şekilde etkileşime girerek sisteme erişmesine ve erişim sırasında gerekli doğrulamaların yapılarak kullanıcı erişimi sırasında güvenliğinin sağlanması hedeflenmiştir.



Şekil 9. API Tasarımı temsili görseli.

Çalışmada tasarlanan API yalnızca kullanıcılar için değil aynı zamanda kontrol mekanizması için de uç noktalar sunmaktadır. Böylece API hem kullanıcıların hem de kontrol mekanizmasının ödül sistemi ile rahatça iletişim kurup işlemlerini yapabilmesine olanak sağlamaktadır.

API üzerindeki kayıt uç noktası aracılığı ile kullanıcılar, JSON formatında kayıt için istenen, kullanıcı adı, posta ve şifre bilgilerini göndererek kayıt işlemlerini yapabilmektedir. Kullanıcıdan veriler alındıktan sonra veriler üzerinde kontroller yapılarak veritabanı ile bağlantı kurulur ve kullanıcı kaydedilmeye uygunsa veritabanına ve sisteme kullanıcı kayıt edilir.

Giriş uç noktası aracılığı ile kullanıcılar, posta ve şifrelerini girerek API isteği yaparlar, yapılan istek API üzerinde değerlendirilir, veritabanı ile gerekli bağlantılar kurularak posta ve kullanıcı adının doğru olması durumunda kullanıcıya doğrulama için yetki verilir, ardından bu uç nokta altındaki farklı bir fonksiyona istek yaptırılarak kullanıcıdan posta kutusuna gönderilen doğrulama kodunun girilmesi istenir. Kullanıcının doğrulanmasının ardından sisteme giriş için kullanıcıya izin verilir ve onay cevap olarak gönderilir.

Görev uç noktası aracılığı ile kullanıcıların sisteme giriş yaptıktan sonra ilgili arayüze eriştiklerinde görevlerinin listelenmesi adına uygulama tarafından istek yapılarak görevlerin listelenmesi işleminin tamamlanması sağlanır.

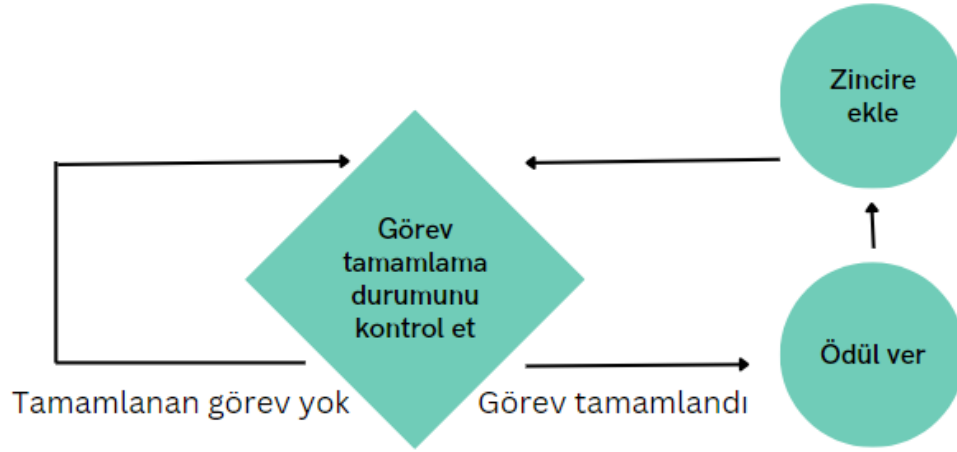
Yönetme uç noktası aracılığı ile kullanıcılar görev tamamladığında, görev tamamlama durumunun sisteme bildirilmesi sağlanır ayrıca bu uç nokta altındaki farklı bir fonksiyon ile birlikte kontrol mekanizmasının görev tamamlayanları kontrol edilmesi ve ödül dağıtımı aşamalarının gerçekleştirilmesine yardımcı olunur.

Tamamlama uç noktası, kullanıcılara görev tamamladıktan sonra ödül verilmesi işlemlerinin tamamlanması için farklı fonksiyonlar sunar. Görev tamamlayan kullanıcıların cüzdan adreslerine erişim sırasında ve cüzdanlara ödülleri gönderilmesi aşamaları da bu uç nokta aracılığı ile olmaktadır.

Ayrıca API üzerindeki uç noktalar ek olarak, uç noktalardaki işlemlerin gerçekleştirilmesi adına kullanılabilecek yardımcı fonksiyonların olduğu farklı sınıflar ve metodlar bulunmaktadır.

3.1.2 Kontrol Mekanizması

Bu çalışmada blok zincir tabanlı ödül sistemi oluşturulması hedeflenmiştir. Oluşturulan bu sistemin en önemli bileşenlerinden birisi de kontrol mekanizmasıdır. Bu mekanizma sürekli olarak kullanıcıların görev tamamlama durumlarını kontrol ederek, görev tamamlayan kullanıcılara ödülleri dağıtma sorumluluğunu üstlenen yapıyı oluşturmaktadır.



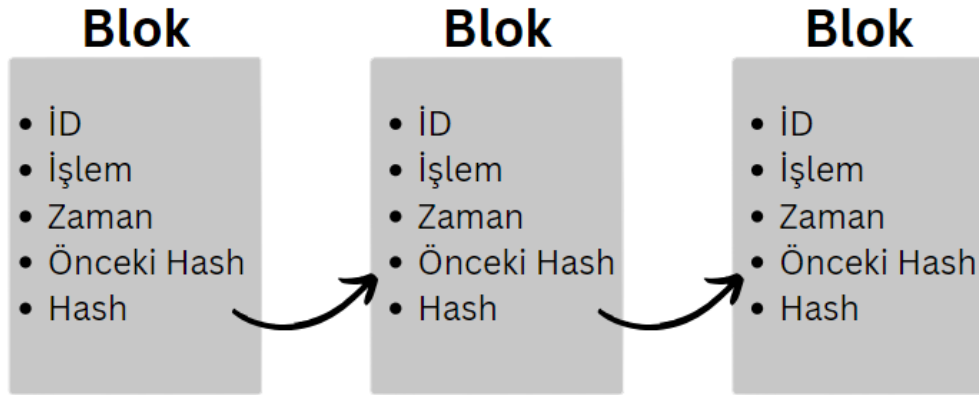
Şekil 10. Kontrol mekanizması çalışma şekli.

Kullanıcılar tarafından görevler tamamlandığında API aracılığı ile tamamlanan görevler veritabanına kaydedilmektedir. Kontrol mekanizması yapısı ise sonsuz bir döngü üzerine inşa edilmiştir, bu yapıda sonsuz döngü içerisinde sürekli olarak bir kontrol işlemi sağlanır. Yapılan kontrol işleminde tamamlanan görevler onaylanır, görevi tamamlayan kullanıcılar kontrol edilerek, görevi tamamlayan kullanıcılara hak ettikleri ödülleri vermek üzere gerekli süreç işletilmeye başlanır. Süreç sonunda kullanıcılara ödülleri verilerek zincire ve kullanıcıların cüzdanlarına işlenmiş olmaktadır.

3.1.3 Ödül Dağıtımı

Çalışma kapsamında geliştirilen sistem, ödül verme üzerine kurulmuştur. Bu sebeple sistemin en önemli parçalarından biri de ödül dağıtımıdır. Tamamen birbirleri ile iletişimde ve senkron halde çalışan parçaların bir araya gelerek oluşturduğu sistemde ödül dağıtımı kısmı da kontrol mekanizması tarafından diğer parçalarla uyumlu olarak gerçekleştirilen bir süreçtir. Kontrol mekanizması tarafından sürekli kontrol edilen görev tamamlama durumu sonucunda, görevin bir kullanıcı tarafından tamamlanmış olması koşuluna bağlı olarak ödül dağıtımı süreci yürütülmektedir. Bu süreç içerisinde ilk olarak görev tamamlayan kullanıcının, görevi tamamlama durumu onaylanır ardından API aracılığı ile kullanıcıya ait cüzdan adresi alınır, alınan cüzdan adresi oluşturulacak işlemin hedef adres kısmına yazılır, ardından işlem oluşturulur. İşlem oluşturulmasının ardından kullanıcının cüzdanına ödül gönderilerek cüzdanda olan miktar güncellenir, sonrasında veritabanında tamamlanan

görevler kısmındaki kullanıcının tamamladığı görevin ödül verilme durumu değiştirilerek, ödül verildi olarak işaretlenir.



Şekil 11. Temsili blok görseli.

Ardından kullanıcıya verilen ödül için oluşturulmuş işlem ile birlikte yeni bir blok oluşturulur. Oluşturulan bloğa id değeri ve zaman bilgisi eklenir. Sonrasında kendinden önceki bloğun hash bilgisi zincirden okunarak, yeni oluşturulan bloğa önceki bloğun hash'i kısmına eklenir. Oluşturulan bu bilgiler ile birlikte blok hash algoritmasına sokularak bloğa ait hash değeri elde edilir ve blok oluşturma işlemi tamamlanmış olur. Ardından yeni oluşturulan blok zincire eklenir, zincirin güncel hali dosyaya yazılarak süreç tamamlanır.

3.1.4 Kullanıcı Uygulaması

Bu çalışmada, kullanıcıların blok zincir tabanlı ödül sistemin erişebilmesi açısından kullanıcı uygulaması olarak WinForms kullanılmıştır. WinForms, Microsoft tarafından geliştirilen ve Windows tabanlı masaüstü uygulamalarının hızlı ve kolay bir şekilde oluşturulmasını sağlayan bir geliştirme platformudur. Geliştirilen uygulama, kullanıcıların ödül sistemi ile etkileşimde bulunmasını sağlayan bir arayüz sunmaktadır.



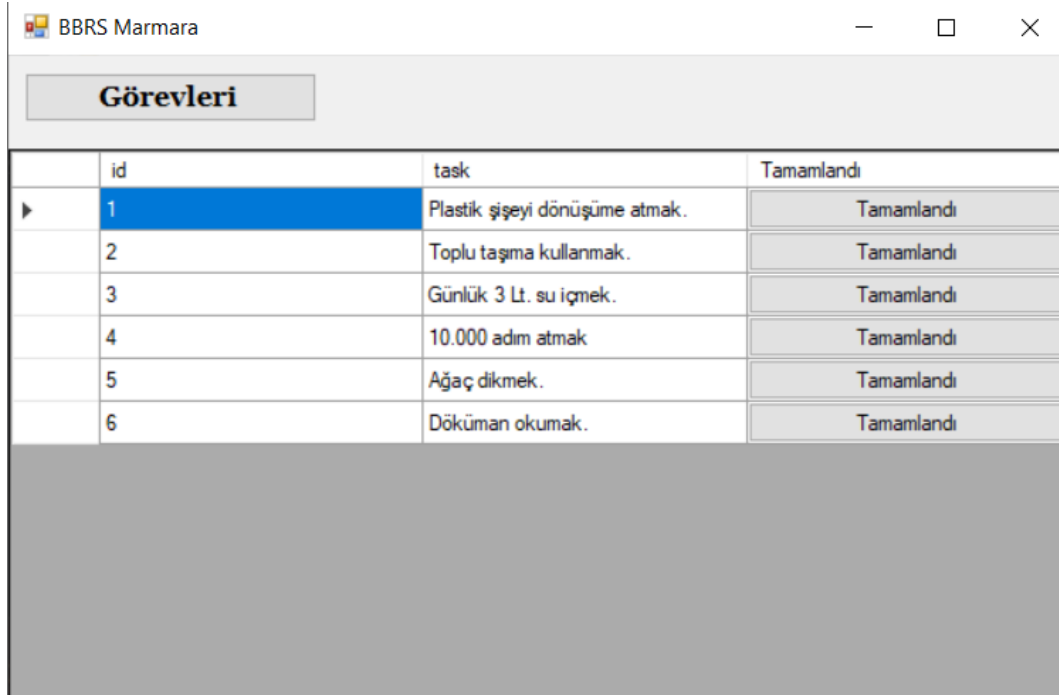
Şekil 12. Uygulama giriş arayüzü ekran görüntüsü

Uygulamayı geliştirirken ilk tasarlanıp sunulan arayüz, kullanıcı giriş ve kayıt ekranıdır. Bu ekran sayesinde kullanıcılar sisteme kayıt olabilmekte veya giriş yapabilmektedir. Kullanıcı giriş ekranı ile birlikte kullanıcılar giriş yaparak sisteme erişebilmektedir.



Şekil 13. Uygulamaya ait kullanıcı ana sayfası ekran görüntüsü.

Kullanıcılar giriş ekranından, bilgilerini doğru bir şekilde girdikten sonra sisteme giriş yapmaktadırlar. Sisteme giriş yapıldıktan sonra ana sayfa onları karşılamaktadır, bu sayfa ile kullanıcılar cüzdan adreslerini görebilmekte, cüzdan adreslerini kopyalayabilmekte ve cüzdanlarında bulunan ödül miktarını da görebilmektedir. Ayrıca sayfanın alt kısmında bulunan butonlar ile birlikte kullanıcılara kendi sistemlerinde olan zinciri güncelleme ve görev arayüzüne geçebilme imkânı sunulmaktadır.



	id	task	Tamamlandı
▶	1	Plastik şişeyi dönüşüme atmak.	Tamamlandı
	2	Toplu taşıma kullanmak.	Tamamlandı
	3	Günlük 3 Lt. su içmek.	Tamamlandı
	4	10.000 adım atmak	Tamamlandı
	5	Ağaç dikmek.	Tamamlandı
	6	Döküman okumak.	Tamamlandı

Şekil 14. Uygulamaya ait görevler sayfası ekran görüntüsü.

Kullanıcılar anasayfa üzerinde görevler butonuna tıkladıktan sonra şekil 14’de görülen görevler sayfasına yönlendirilmektedir. Bu sayfa ile birlikte kullanıcıya mevcut görevlerin bir listesi sunulmaktadır. Ayrıca bu sayfa kullanıcılara, belirli görevleri tamamlama işlevselliğini sunmaktadır. Bu işlevsellik sayesinde kullanıcılar seçtikleri bir görevi tamamlayabilmektedir. Görevin bu ekran ile tamamlanmasının ardından görevin tamamlandığında gerçekleşecek işlemler de bu sayfada işletilmeye başlatılacak süreç ile başlamaktadır.

Bu çalışmada geliştirilen uygulama ile kullanıcıların blok zincir tabanlı ödül sistemi ile etkileşime geçmesi kolaylaştırılmakta, kullanıcılara basit ve işlevsel bir arayüz sunulmaktadır. Bu uygulama sayesinde kullanıcılar görevleri görüntüleyebilmekte, tamamlayabilmekte ve cüzdan adreslerini, içerisindeki miktarı görebilmektedir.

3.1.5 P2P Ağ Oluşturulması

Bu çalışmada geliştirilen blok zincir tabanlı ödül sistemi içerisinde kullanıcılar arası iletişimi sağlamak amacıyla P2P ağ oluşturulması hedeflenmiştir. P2P ağları, blok zincir mimarisine uygun bir şekilde, dağıtık bir yapıda çalışan ve merkezi bir otoriteye ihtiyaç duymadan doğrudan kullanıcılar arasında veri ve kaynak paylaşımını sağlayan ağlardır. P2P ağı kurmak için ilk olarak ağ protokolü belirlenmelidir. Çalışmada oluşturulacak ağ için WebSocket protokolü belirlenmiştir. Geliştirilen ödül sistemi için iletişim, kullanıcılar arasında veri alışverişini, zincir doğrulanmasını ve diğer ağ aktivitelerini içermektedir. Geliştirilen sistemde kullanılan P2P ağları ile birlikte, sistemdeki her bir kullanıcının dağıtık bir yapıda birbirleri ile iletişim kurması sağlanmaktadır.

```
public class P2PServer: WebSocketBehavior
{
    private bool _chainSynched;
    private WebSocketServer _wss;

    1 reference
    public void Start()
    {
        _wss = new WebSocketServer("ws://127.0.0.1:23456");
        _wss.AddWebSocketService<P2PServer>("/Blockchain");
        _wss.Start();
        Console.WriteLine("started server");
    }

    0 references
    protected override void OnMessage(MessageEventArgs e)
    {
        if(e.Data == "Hi Server")
        {
            Console.WriteLine(e.Data);
            Send(JsonConvert.SerializeObject(Program.MarmaraCoin));
        }
        else
        {
            Blockchain newChain = JsonConvert.DeserializeObject<Blockchain>(e.Data);
            if(newChain.IsValid() && newChain.Chain.Count > Program.MarmaraCoin.Chain.Count)
            {
                Program.MarmaraCoin = newChain;
            }
            if(!_chainSynched)
            {
                Send(JsonConvert.SerializeObject(Program.MarmaraCoin));
                _chainSynched = true;
            }
        }
    }
}
```

Şekil 15. P2P bağlantısı için sunucu örnek kod parçası ekran görüntüsü.

Geliştirilen sistemde her uygulama ve kontrol mekanizması hem bir sunucu, hem de bir istemci gibi davranmaktadır. Şekil 15’de uygulamanın sunucu gibi davranması için işletilen kod parçasığına bir örnek verilmiştir. Bu örnekte de görüleceği üzere, uygulama ağ üzerinde

bir sunucu başlatmaktadır, ardından belirtilen port üzerinden gelecek istekleri dinlemektedir. Gelen isteklere göre koşul ifadesi ile farklı kod bloklarını çalıştırmaktadır, gelen istekte eğer bir zincir gönderildiyse bu zinciri almakta ve çeşitli sorgulardan geçirmektedir. Bu sorgular ile birlikte zincirin geçerliliğini ve güncelliğini ölçen uygulama, eğer kendi üzerinde tuttuğu zincirden daha güncel ve geçerli bir zincir ile karşılaşır, zincirini güncellemektedir. Gelen zincirin geçerli olmaması veya eski bir versiyon olması durumunda ise istemciye kendi zincirini göndermektedir. Uygulamalar üzerinde çalışan bir başka senaryoda ise uygulamalar istemci gibi davranmaktadır.

```
public class P2PClient
{
    IDictionary<string, WebSocket> wsDict = new Dictionary<string, WebSocket>();

    0 references
    public void connect(string url)
    {
        if(!wsDict.ContainsKey(url))
        {
            WebSocket ws = new WebSocket(url);
            ws.OnMessage += (sender, e) =>
            {
                if (e.Data == "Hi Client")
                {
                    Console.WriteLine(e.Data);
                }
                else
                {
                    var newChain = JsonConvert.DeserializeObject<Blockchain>(e.Data);
                    if (!newChain.IsValid() || newChain.Chain.Count <= Program.MarmaraCoin.Chain.Count)
                    {
                        return;
                    }
                    else
                    {
                        Program.MarmaraCoin = newChain;
                    }
                }
            };
            ws.Connect();
            ws.Send("Hi Server");
            ws.Send(JsonConvert.SerializeObject(Program.MarmaraCoin));
            wsDict.Add(url, ws);
        }
    }
}
```

Şekil 16. P2P bağlantısı için istemci örnek kod parçacığı ekran görüntüsü.

Uygulama istemci gibi davrandığında ise, sunucu gibi davranan diğer uygulamalara istek göndermektedir. Gönderdiği istek karşısında dönen yanıtı inceleyen uygulama, eğer gelen zincir geçerli ve kendi zincirinden güncel ise kendi zincirini gelen zincir ile güncellemektedir. Uygulamanın kendi zincirinin daha güncel olması durumunda ise, uygulama sunucuya kendi zincirini göndermektedir.

3.2 Performans Değerlendirmesi

Bu çalışmada geliştirilen blok zincir tabanlı ödül sisteminin performansı incelendiğinde, sistemin 3 farklı bileşen üzerinde durduğu gözlemlenmiştir. Bu bileşenlerin performansları ayrı ayrı incelenerek bir bütün şeklinde değerlendirilebilmektedir. Bileşenler kontrol mekanizması, API ve kullanıcı uygulaması olarak incelenebilmektedir.

Kontrol mekanizması bileşeni, kullanıcının gerçekleştirdiği görevleri takip etmek ve doğrulamak için kullanılır. Bu bileşen, görev tamamlama işlemlerini hızlı ve güvenilir bir şekilde gerçekleştirmelidir. Performans değerlendirmesi sırasında kontrol mekanizması bileşeninin doğrulama süresi, hatalı doğrulama oranı ve sistemin yanıt verme hızı gibi ölçütler dikkate alınmaktadır. Örneğin, kontrol mekanizması görev tamamlama doğrulama süresini en aza indirmeli ve kullanıcıların görevlerini hızlı bir şekilde onaylamalıdır.

API bileşeni, kullanıcı uygulaması ile blok zincir tabanlı ödül sistemi arasındaki iletişimi sağlar. Bu bileşenin performansı, hızlı ve güvenli veri alışverişi yeteneklerine bağlıdır. Performans değerlendirmesi sırasında API'nin yanıt süresi, isteklerin işleme alınma hızı ve veri bütünlüğü gibi faktörler göz önünde bulundurulur. Örneğin, API'nin düşük gecikme süresi ve yüksek işlem kapasitesi, sistem performansının iyileştirilmesine katkı sağlar.

Kullanıcı uygulaması bileşeni, kullanıcıların görevleri tamamlamasını sağlar ve ödülleri takip etmelerine olanak tanır. Bu bileşenin performansı, kullanıcı deneyimi, kullanıcı arayüzü ve kullanıcı dostu olma gibi faktörlere bağlıdır. Performans değerlendirmesi sırasında kullanıcı uygulamasının hızı, kullanıcı arayüzünün kullanım kolaylığı ve görev tamamlama sürecinin kullanıcı dostu olup olmadığı gibi ölçütler göz önünde bulundurulur. Örneğin, kullanıcı uygulamasının yüksek hızı ve kullanıcı dostu arayüzü, kullanıcıların sistemi etkili bir şekilde kullanmasını sağlar.

Tüm bu bileşenlerin performansı bir bütün olarak değerlendirildiğinde, blok zincir tabanlı ödül sisteminin başarısı belirlenebilir. Performans değerlendirmesi sonuçlarına dayanarak, sistemin hedeflenen görevleri doğru ve etkili bir şekilde yerine getirip getirmediği ve kullanıcı deneyimini nasıl etkilediği değerlendirilebilir. Bu değerlendirme, sistemdeki olası zayıf noktaları belirlemek ve geliştirmeler yapmak için önemli bir adımdır.

3.3 Güvenlik Analizi

Çalışma kapsamında geliştirilen blok zincir tabanlı ödül sistemi'nin önemli parçalarından biri de güvenlidir. Kullanıcı ve sistem adına güvenliği sağlayacak önlemler almak, kullanıcı ve sistem verilerini korumak adına önem teşkil etmektedir. Sistemde bulunacak herhangi bir

açıklık bilgi güvenliğinin 3 temel unsuru olan gizlilik, bütünlük ve erişilebilirlik ilkelerini tehlikeye sokacağından, bu çalışmada güvenlik konusunda özellikle dikkat edilmiştir. Sistemin parçalarından kullanıcı uygulamasını kullanan bir kullanıcı sisteme kullanıcı adı, posta ve şifre alanlarını doldurarak kayıt olmaktadır. Kayıt süreci için ilk olarak kullanıcı girdileri alınarak API isteği yapılmaktadır. API tarafında karşılanan isteğin parametreleri alınarak veritabanında gerekli kontroller yapılmaktadır, eğer kullanıcı postasına ait başka bir hesap yok ise kullanıcı kaydı oluşturulmaktadır.

```
public string createSalt()// salt oluşturur.
{
    Random rnd = new Random();
    string salt = rnd.Next(1000000,9999999).ToString();
    return salt;
}
1 reference
public string getHash(string passwd,string salt)//user'a ait password'ü salt ile birlikte hashler
{
    SHA1 sHA1 = new SHA1CryptoServiceProvider();
    string sifrelenecek_veri = passwd + salt;
    string hash = Convert.ToBase64String(sHA1.ComputeHash(Encoding.UTF8.GetBytes(sifrelenecek_veri)));
    return hash;
}
```

Şekil 17. Güvenliğe yönelik salt ve hash fonksiyonu.

Şekil 17’de ekran görüntüsü paylaşılan kod parçacığı ile birlikte öncelikle kullanıcıya ait salt bilgisi oluşturulmaktadır. Salt veri tabanlarında veri saklarken, şifreleme kısmında kompleksliği artırmak için kullanılan rastgele sayılardan oluşan değeri ifade etmektedir. Kullanıcı kaydı sırasında rastgele olarak oluşturulan salt değeri veritabanında kullanıcıya ait sütuna kaydedilir. Ardından kullanıcıdan gelen şifre bilgisi, oluşturulan salt ile birlikte hash fonksiyonuna girdi olarak verilir ve hashlenmiş veri elde edilir, elde edilen veri veritabanında şifreli biçimde saklanmaktadır. Yapılan bu işlemler sayesinde veritabanı’nın herhangi bir saldırıya maruz kalması durumunda, saldırganın kullanıcıya ait şifre bilgilerine düz metin olarak erişip bu bilgileri kullanarak kullanıcı hesabına ve sisteme zarar vermesi engellenmiş olmaktadır.

Ayrıca kullanıcı giriş yapmak istediğinde, uygulamaya mail ve posta verilerini girecektir, ardından kontroller yapılacaktır, kontroller sırasında direk olarak şifre’nin düz metin olduğu hiçbir işlem yapılmayacağı için sistem bu aşamada kendini güvene almıştır. Kullanıcıya ait salt bilgisi ile kullanıcının girdiği şifre hashlenerek elde edilen sonuç veritabanındaki şifrelenmiş veri ile karşılaştırılır, eşleşme sağlandığı durumda kullanıcıya giriş için izin verilmekte ve doğrulama kısmına geçilmektedir, aksi durumda ise kullanıcıya giriş için izin verilmemektedir.

Çalışmada geliştirilen sistemde güvenliğinin önemli bir kısmını doğrulama süreçleri oluşturmaktadır. Geliştirilen uygulamada 2 aşamalı doğrulamaya özen göstermektedir. Kullanıcılar posta ve şifreleri ile blok zincir tabanlı ödül sistemine giriş yapmak istediklerinde, girdikleri verilerin doğruluğu kontrol edilir, doğru olması halinde kullanıcı doğrulama sürecine yönlendirilmektedir.

```
[HttpPost]
[Route("api/Login/Post")]
0 references
public IActionResult Post([FromBody] login_user_model user)
{
    string mail = user.mail;
    string password = user.password;

    if(ud.login_user(mail, password))
    {
        cache.Remove("key");
        // Doğrulama kodunu oluşturun
        verificationCode = GenerateVerificationCode();
        cache.Add("key", verificationCode, DateTimeOffset.Now.AddMinutes(30));

        // Doğrulama kodunu kullanıcıya gönderin (örneğin e-posta ile)
        SendVerificationCode(mail, verificationCode);

        // Doğrulama kodunu ve kullanıcı bilgilerini geçici bir veritabanına kaydedin
        SaveVerificationCode(mail, verificationCode);

        return Ok();
    }
    else
    {
        return BadRequest();
    }
}
```

Şekil 18. Sistem giriş ve doğrulama kısımları kod ekran görüntüsü.

Doğrulama sürecinde şekil 18’de verilen ekran görüntüsü örneğinde olduğu gibi süreç ilerlemektedir. İlk olarak kullanıcıya ait bir doğrulama kodu oluşturulur, ardından kullanıcıya ait doğrulama kodu, kullanıcıya ait posta adresine gönderilir ardından kullanıcıdan kendisine gönderilen doğrulama kodunun girilmesi istenir. Kullanıcı kendisine gelen doğrulama kodunu girerek bir API isteği yapar, API tarafından gelen isteğin içerisinde doğrulama kodu alınarak sistem içerisinde kullanıcı için oluşturulmuş doğrulama kodu ile karşılaştırılır. Doğrulama kodlarının eşleşmesi durumunda kullanıcıya sisteme girebilmesi için izin verilmektedir. Kendisini doğrulayan kullanıcı, iznin olduğu API yanıtı uygulamaya geldiğinde sisteme giriş yapabilmektedir.

Çalışmada güvenlik konusunda odaklanılan bir başka konu da kullanıcı, şifre ve veri güvenliğinin yanında zincir güvenliğidir. Blok zincir tabanlı ödül sisteminde, zincirin güvenliği ve bütünlüğü, sistemin güvenliği ve itibarı açısından en önemli unsurların başında gelmektedir. Geliştirilen sistemde zincir güvenliği için hash fonksiyonlarının kullanılmasının yanında, zincir doğrulanması için de farklı metodlar kullanılmaktadır.

```
public bool IsValid()
{
    for (int i =1; i < Chain.Count; i++)
    {
        Block currentBlock = Chain[i];
        Block prevBlock = Chain[i-1];

        if (currentBlock.Hash_!= currentBlock.CreateHash())
        {
            return false;
        }

        if (currentBlock.PreviousHash != prevBlock.Hash_)
        {
            return false;
        }
    }
    return true;
}
```

Şekil 19. Zincir doğrulama fonksiyonu kod örneği.

Sistemde zincir güvenliği ve doğruluğu için kontrol kontrol gerçekleştiren fonksiyonlardan biri de şekil 19'de örneği verilen fonksiyondur. Bu fonksiyon ile birlikte zincir incelenerek doğrulanmaktadır. İlk olarak zincir uzunluğu kadar dönecek bir döngü oluşturan fonksiyon sonrasında her aşama için zincire ait 2 bloğu kendisine alır ve ilk olarak blok üzerinde yazana bloğa ait hash'in doğruluğunu kontrol eder, bu kontrol sırasında bir sorun ile karşılaşmaması halinde bir önceki blok hash'i ile o anki bloğa ait önceki blok hash'i değerini karşılaştırarak kontrol eder. Yapılan kontroller sonrasında fonksiyon bir sorun oluşmaması durumunda zinciri doğrulayarak kullanıcıya bildirmektedir. Bu mekanizma sayesinde, her aşamada kullanıcının kendi yerel depolama alanında bulunan zincir ve dışarıdan kendini güncellemek için aldığı zincirler kontrol edilmektedir.

Veri bütünlüğü, kimlik doğrulama, gizlilik ve zincir doğrulama gibi işlevlerin olması geliştirilen sistemin güvenlik açısından sağlam temellere sahip olduğunu ortaya koymaktadır.

3.4 Uygulama Alanları

Bu çalışmada blok zincir tabanlı ödül sistemi, üniversite öğrencileri ve potansiyel kullanıcıların farkındalıklarını arttırmak, onları motive etmek ve teşvik etmek için geliştirilmiştir. Çalışma sayesinde insanlar görevlerini daha iyi bir motivasyon ile yerine getirebilir, farkındalık ve bu alanlarda kendilerini teşvik edebilmektedir. Geliştirilen sistemin bu bağlam haricinde de kullanılabileceği alanlar bulunmaktadır. Tedarik zincirleri, perakende sektörü ve e-ticaret platformlarındaki sadakat programlarında kullanılabilecek bir sistemdir. Aynı zamanda bankalar veya çeşitli yatırım kuruluşları açısından finansal, egzersiz yapmaya teşvik etme ve benzeri durumlarda sağlık alanında, sosyal sorumluluk projeleri, doğa dostu projeler gibi alanlarda ise sosyal ve çevresel alanlarda faydalı davranışları artırıcı bir etken olarak kullanılabilmektedir. Geliştirilen blok zincir tabanlı ödül sistemi esnekliği ve adaptasyon yeteneği ile birlikte, birçok farklı sektörde çeşitli uygulama alanları ve senaryoları için kendisine potansiyel oluşturmaktadır. Bu tarz sistemlerin kullanılması ile birlikte kullanıcıların motivasyonunu artırma, teşvik etme, sosyal ve çevresel aktivitelere katkıda bulunma gibi alanlarda fayda sağlanmaktadır. Ayrıca sistem izlenebilirlik, merkeziyetsizlik ve değiştirilemezlik açısından da faydalı ve birçok alana uygulanabilir bir sistemdir.

3.5 Ölçeklenebilirlik

Ölçeklenebilirlik kavramı, bir sistem veya ağın artan talep ve kullanıcı sayısı ile başa çıkabilme yeteneğini ifade etmektedir. Çalışmada geliştirilen blok zincir tabanlı ödül sistemi için de önemli bir faktör oluşturmaktadır. Sistem merkezi olmayan, dağıtık bir yapıya sahip olması nedeniyle ölçeklenebilir ve geniş çapta kullanılabilir olmaktadır. Sistemin ölçeklenebilirliğini etkileyen farklı faktörler bulunmaktadır, kullanıcı ödül talepleri, görev tamamlama durumları, ödül verilmesi ve zincir senkronizasyonu durumları için işlem hızının yeterli düzeyde olması gerekmektedir, zamanla genişleyebilecek bir sistemde, sistemin geniş kullanıcı kitlesinin de taleplerini karşılayabilmesi gerekmektedir. Blok zincir ödül sistemi bir başka faktör olan işlem kapasitesi faktöründe ise dağıtık bir yapı sunarak, genişletilme durumlarında optimize edilmiş bir deneyim sunmaktadır. Ağ yükü faktörü ise sistemin genişletilmeye ve sahip olduğu imkanlarına bağlı olarak, sistemin önüne yük dengeleyici ve benzeri yük dengeleme hizmeti yapan araçlar konumlandırılması durumunda trafik yükünü genişletilme durumunda kaldırabilecek bir kapasiteye sahiptir. Ayrıca geliştirilen sistemde çeşitli zincir doğrulama işlemlerinin istemci üzerinde yapılacak şekilde dizayn edilmesi ile daha fazla işlem hızı ve daha düşük işlem maliyeti sağlanması hedeflenmektedir. Blok zincir

tabanlı bir ödül sisteminin ölçeklenebilir bir yapıda olması bu sistemin daha fazla kullanıcıya hitap edebilme potansiyelini göstermektedir. Ölçeklenebilir bir sistem, daha verimli, güvenli ve kullanıcı dostu bir sistem haline gelmektedir.

3.6 Sürdürülebilirlik ve Çevresel Etkiler

Bu çalışmada sürdürülebilirlik ve çevresel etkiler birkaç başlık altında incelenebilir. Geliştirilen blok zincir tabanlı ödül sistemi enerji verimliliği açısından değerlendirilecek olursa, bitcoin gibi blok zincir kullanan algoritmalarla kıyasla yoğun olarak enerji harcama açısından daha avantajlı olmaktadır. Diğer blok zincir uygulamalarında çok enerji tüketen uygulamaların başında işlem madenciliği ve konsensüs algoritmaları gelmektedir, ancak geliştirilen sistem bu algoritmalar daha az maliyetli tutularak enerjiden tasarruf edilerek çevreci bir yaklaşım izlenmiştir. Geliştirilen blok zincir tabanlı ödül sistemine katılım için ekstra bir cihaz veya donanım ihtiyacı doğmayacağından sistem kullanıcılarına ekstra bir maliyet ve doğaya ekstra bir atık doğurmayacaktır.

Geliştirilen blok zincir tabanlı ödül sisteminin topluma olan etkileri incelendiğinde, toplumun önemli bileşenlerinden olan üniversite kurumundakileri kullanıcı kitlesi olarak hedefleyen uygulama, izlediği çevreci politika ile birlikte hem bireysel hem de toplumsal olarak fayda sağlamaktadır. Çalışmanın ölçeklenebilir bir yapıda olması sebebi ile sistem toplumun farklı kesimlerine de uygulanabilme yeteneğine sahiptir, bu sayede toplumun her kesiminden insanlara erişerek onları çevresel ve bireysel olarak motive ve teşvik edici bir politika izlenebilmektedir. Bu kısımda çalışmanın çevresel etkileri başlığı altında incelenebilmektedir.

Sonuç olarak, bu çalışmada bir blok zinciri uygulamasının nasıl kullanıldığı ve ödül sistemi için nasıl bir çözüm sağladığı ayrıntılı bir şekilde incelenmiştir. Blok zinciri teknolojisi, ödül sistemlerinin güvenlik, şeffaflık ve veri bütünlüğü gibi temel unsurlarında önemli avantajlar sunmaktadır. Bu avantajlar, ödül sistemlerini daha güvenilir, şeffaf ve manipülasyona karşı dayanıklı hale getirir.

Araştırmada, blok zinciri teknolojisinin ödül sistemlerine nasıl entegre edilebileceği ve nasıl kullanıldığı ayrıntılı bir şekilde ele alınmıştır. Ödül sistemi, katılımcılara çevre dostu davranışlar, toplum hizmetine katkılar veya belirli başarılar gibi görevleri yerine getirmeleri karşılığında dijital ödüller sunmaktadır. Bu görevler, blok zinciri ağı tarafından güvenli bir şekilde kaydedilmekte ve doğrulanmaktadır.

Ayrıca, çalışmada blok zinciri uygulamalarının ölçeklenebilirlik ve performans zorlukları da ele alınmıştır. Blok zinciri teknolojisinin mevcut haliyle büyük ölçekli kullanımlara uygun olmadığı ve performans sorunlarına yol açabileceği vurgulanmıştır, ancak gerekli sistem bileşenlerinin entegre edilmesi ile birlikte blok zincir tabanlı ödül sistemi genişletilebilmektedir. Bu nedenle, gelecekte yapılacak araştırma ve geliştirme çalışmalarıyla blok zinciri tabanlı ödül sistemlerinin ölçeklenebilirlik ve performansını iyileştirmek önemli bir hedef olacaktır.

Bu çalışma blok zinciri teknolojisinin ödül sistemleri için potansiyelini ve avantajlarını detaylı bir şekilde analiz etmiştir. Gelecekte, daha fazla araştırma ve geliştirme çalışmalarıyla birlikte, blok zinciri tabanlı ödül sistemlerinin daha da geliştirilerek yaygınlaştırılması mümkün olacaktır. Bununla birlikte, sistem erişimini kolaylaştırmak amacıyla bir mobil uygulama geliştirilmesi ve toplumun farklı kesimlerine yönelik sistemin uygulanması, toplumsal gelişim ve çevre farkındalığı gibi konulara daha fazla dikkat çekilebilmesini sağlayacaktır.

KAYNAKLAR

- [1] E. Yavuz and H. Avunduk, "TEDARİK ZİNCİRİ YÖNETİMİNDE BLOK ZİNCİR TEKNOLOJİSİNİN KULLANIMI," *Izmir Democracy University Social Sciences Journal*, vol. 4, no. 1, pp. 33-56, 2021.
- [2] M. Di Pierro, "What is the blockchain?", *Computing in Science & Engineering*, vol. 19, no. 5, pp. 92-95, 2017.
- [3] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," *Applied Innovation*, vol. 2, no. 6-10, pp. 71-81, 2016.
- [4] M. Morsidi, S. Tajuddin, R.K. Patchmuthu, and S.H.S. Newaz, "Blockchain-based Reward System: a Means for Providing Incentive to Students for Teaching Feedback," in *International Conference on Electronics, Communications and Information Technology (ICECIT)*, pp. 1-5, 2021.
- [5] A. Ceylan, "Blockchain Technology Applications in Education," *Journal of Educational Technology & Online Learning*, vol. 3, no. 2, pp. 168-176, 2020.
- [6] E. Koc, "TEDARİK ZİNCİRİ İZLENEBİLİRLİĞİ VE SÜRDÜRÜLEBİLİRLİĞİNDE YENİ PARADİGMA: BLOK ZİNCİR," *Bingöl Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, vol. 20, pp. 417-438, 2020.
- [7] J. Yuan and L. Njilla, "Lightweight and Reliable Decentralized Reward System using Blockchain," *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops, Vancouver, BC, Canada,,* pp. 1-6, 2021.
- [8] M. Li, J. Weng, A. Yang, W. Lu, Y. Zhang, L. Hou, et al., "Crowdbc: A blockchain-based decentralized framework for crowdsourcing", *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 6, pp. 1251-1266, 2019.
- [9] A. F. Mendi, "Blok zincir Mimarisi ve Getirdiği Fırsatlar," *Avrupa Bilim ve Teknoloji Dergisi*, Özel Sayı , pp. 181-186, 2021.
- [10] G. Wood, "Ethereum: A secure decentralized generalized transaction ledger", *Ethereum project yellow paper*, vol. 151, pp. 1-32, 2014.

- [11] C. Tanas, S. Delgado-Segura and J. Herrera-Joancomartí, "An integrated reward and reputation mechanism for mcs preserving users' privacy" in *Data Privacy Management and Security Assurance, Cham:Springer International Publishing*, pp. 83-99, 2016.
- [12] T. Wernbacher and V. Stix, "Cycle4Value: A Blockchain-based Reward System to Promote Cycling and Reduce CO2 Footprint," *Sustainability*, vol. 13, no. 7, p. 3825, 2021.
- [13] Yang, X., Chen, Y., & Chen, X. "Effective scheme against 51% attack on proof-of-work blockchain with history weighted information." *In 2019 IEEE International Conference on Blockchain* , pp. 261-265, 2019.
- [14] M. Aslan ve M. C. Kasapbaşı , "Blok Zinciri Platformları, Fikir Birliği Mekanizmaları ve Ağın Güvenlik Analizi", *Haliç Üniversitesi Fen Bilimleri Dergisi*, c. 5, sayı. 1, ss. 43-72, Mar. 2022
- [15] M. Birim, H. E. Arı, and E. Karaarslan, "GoHammer Blockchain Performance Test Tool," *Journal of Emerging Computer Technologies*, vol. 1, no. 2, pp. 31-33, 2021.
- [16] K. Öncü, "Software Development Methodology Selection with Human Resource Management Approach and a New System Design on Database: Blockchain Application," *Quantrade Journal of Complex Systems in Social Sciences*, vol. 1, no. 1, pp. 28-39, 2019.