DÜZCE ÜNİVERSİTESİ | LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BLOCKCHAIN TABANLI IOT GÜVENLİĞİ VE PERFORMANS ANALİZİ

SELAMİ TERAZİ

YÜKSEK LİSANS TEZİ
SİBER GÜVENLİK ANABİLİM DALI

DANIŞMAN
DOÇ. DR. ARAFAT ŞENTÜRK

DÜZCE, 2024

T.C.

DÜZCE ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

BLOCKCHAIN TABANLI IOT GÜVENLİĞİ VE PERFORMANS ANALİZİ

Selami TERAZİ tarafından hazırlanan tez çalışması aşağıdaki jüri tarafından Düzce Üniversitesi Lisansüstü Eğitim Enstitüsü Siber Güvenlik Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Doç. Dr. Arafat ŞENTÜRK

Düzce Üniversitesi

Jüri Üyeleri

Doç. Dr. Arafat ŞENTÜRK
Düzce Üniversitesi _____

Dr. Öğr. Üyesi Ahmet ALBAYRAK
Düzce Üniversitesi _____

Prof. Dr. Devrim AKGÜN
Sakarya Üniversitesi _____

Tez Savunma Tarihi: 31/10/2024

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını beyan ederim.

31 Ekim 2024

Selami TERAZİ

TEŞEKKÜR

Yüksek Lisans öğrenimimde ve bu tezin hazırlanmasında gösterdiği her türlü destek ve yardımdan dolayı çok değerli hocam Doç. Dr. Arafat ŞENTÜRK'e en içten dileklerimle teşekkür ederim.

Bu çalışma boyunca yardımlarını ve desteklerini esirgemeyen sevgili aileme ve çalışma arkadaşlarıma sonsuz teşekkürlerimi sunarım.

31 Ekim 2024 **Selami TERAZİ**

İÇİNDEKİLER

Sayfa No

ŞEKİL LİSTESİ

Sayfa No

ÇİZELGE LİSTESİ

Sayfa No

KISALTMALAR

ABAC	Attribute-Based Access Control
AC	Access Contract
API	Application Programming Interface
ASPE	Asymmetric Scalar-product Preserving Encryption
CID	Coordinator IoT Device
DABG	Dynamic Application Block Generation
DBACP-IoTSG	Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System
DC	Device Contract
DDoS	Distributed Denial-of-Service
DTM	Distributed Throughput Management
ECC	Elliptic-curve cryptography
ELIB	Efficient Lightweight integrated Blockchain
ESL	Ephemeral Secret Leakage
H-LGM	Hyperledger Fabric-Based Lightweight Group Management
IDS	Intruder Detection System
IIoT	Industrial Internet of Things
IoT	Internet of Things
LSB	Lightweight Scalable Blockchain
MAC	Media Access Control
MitM	Man-in-the-Middle
MSR	Magnetic Stripe Reader
OPNET	OPtimized Network Engineering Tool
PBFT	Practical Byzantine Fault Tolerance
PC	Policy Contract
PKI	Public Key Infrastructure
POW	Proof of Work
SDN	Software Defined Networks
SMs	Respective Smart Meters
TABI	Trust-based ABAC Mechanism for Edge-IoT
TPS	Transaction Per Second
TTP	Trusted Third Party

ÖZET

BLOCKCHAİN TABANLI IOT GÜVENLİĞİ VE PERFORMANS ANALİZİ

Selami TERAZİ

Düzce Üniversitesi
Lisansüstü Eğitim Enstitüsü, Siber Güvenlik Anabilim Dalı
Yüksek Lisans Tezi
Danışman: Doç. Dr. Arafat ŞENTÜRK

Ekim 2024, 50 sayfa

Nesnelerin İnterneti (IoT), çeşitli cihazların birbirine bağlanarak veri alışverişi yapmasını sağlayan bir ağ yapısını ifade etmektedir. Bu teknolojinin benimsenmesi, endüstriyel süreçlerden günlük yaşam aktivitelerine kadar birçok alanda gelişme sağlamaktadır. Ancak, IoT cihazlarının sayısındaki hızlı artış, beraberinde önemli güvenlik sorunlarını da getirmektedir. Özellikle; siber saldırılar, veri ihlalleri ve yetkisiz erişimler, IoT sistemlerinin güvenliğini tehdit eden başlıca unsurlar haline gelmiştir. Bu tez çalışmasında, IoT güvenliğini artırma hedefiyle blockchain teknolojisinin birleşimi incelemekte ve bu bağlamda Hyperledger Fabric'in sağladığı avantajları değerlendirmektedir. Blockchain teknolojisi, özellikle izinli ağ yapısı ve merkeziyetsizlik özellikleri ile IoT sistemlerine büyük katkılar sağlayabilir. Blockchain, verilerin güvenli bir şekilde saklanmasını sağlarken, veri bütünlüğünü ve gizliliğini de artırmaktadır. Hyperledger Fabric, bu güvenlik gereksinimlerini karşılamak için ideal bir platform sunmakta; modüler mimarisi sayesinde organizasyonlara esneklik sağlamaktadır. OPNET benzetim aracı ile blockchain kullanılarak şifrelenen paketleri ileten IoT ağının performansı detaylı bir biçimde analiz edilmektedir. Benzetimler, blockchain teknolojisinin IoT sistemlerine birleşiminin güvenlik seviyelerini nasıl artırabileceğini ve siber tehditlere karşı koruma sağladığını göstermektedir. Ayrıca, bu çalışmada, blockchain kullanılarak şifrelenen paketleri ileten sistemlerin kullanıcıların kimlik doğrulama süreçlerini güvence altına alarak yetkisiz erişimlerin önüne geçme potansiyeli incelenmektedir. Sonuç olarak, bu tez çalışmasında, blockchain teknolojisinin IoT güvenliğini sağlama potansiyelini ortaya koymakta ve endüstriyel uygulamalar için pratik çözümler sunmaktadır. Gelecekte IoT sistemlerinin güvenliğinin sağlanmasında blockchain'in önemli bir rol oynayacağına dair bulgular sunarak, bu alanda daha fazla araştırma yapılmasının gerekliliğini vurgulamaktadır. Bu çalışma hem akademik literatüre katkıda bulunmayı hem de pratik uygulamalar için bir temel oluşturmayı amaçlamaktadır. IoT güvenliğine yönelik bu yaklaşım, yalnızca teknoloji geliştirme sürecinde değil, aynı zamanda endüstriyel uygulamalarda da önemli bir yere sahip olacaktır.

Anahtar Sözcükler: Blockchain, IoT, Siber Güvenlik, Hyperledger Fabric, OPNET

ABSTRACT

BLOCKCHAIN-BASED IOT SECURITY AND PERFORMANCE ANALYSIS

Selami TERAZI

Düzce University
Graduate School, Department of Cyber Security
Master's Thesis
Supervisor: Assoc. Prof. Dr. Arafat ŞENTÜRK

October 2024, 50 pages

The Internet of Things (IoT) refers to a network structure that enables various devices to connect to each other and exchange data. The adoption of this technology has led to improvements in many areas, from industrial processes to daily life activities. However, the rapid increase in the number of IoT devices brings with it significant security challenges. In particular, cyber-attacks, data breaches and unauthorized access have become the main threats to the security of IoT systems. This thesis examines the combination of blockchain technology with the goal of improving IoT security and evaluates the advantages of Hyperledger Fabric in this context. Blockchain technology can make great contributions to IoT systems, especially with its permissioned network structure and decentralization features. Blockchain enables secure storage of data and increases data integrity and confidentiality. Hyperledger Fabric offers an ideal platform to meet these security requirements and provides flexibility to organizations thanks to its modular architecture. With the OPNET simulation tool, the performance of the IoT network that transmits packets encrypted using blockchain is analyzed in detail. The simulations show how the incorporation of blockchain technology into IoT systems can increase security levels and provide protection against cyber threats. Furthermore, this study examines the potential of systems that transmit packets encrypted using blockchain to prevent unauthorized access by securing users' authentication processes. In conclusion, this thesis demonstrates the potential of blockchain technology to secure IoT and provides practical solutions for industrial applications. By presenting findings that blockchain will play an important role in securing IoT systems in the future, it emphasizes the need for further research in this field. This study aims to both contribute to the academic literature and provide a foundation for practical applications. This approach to IoT security will have an important place not only in technology development but also in industrial applications.

Keywords: Blockchain, IoT, Cyber Security, Hyperledger Fabric, OPNET

1. GİRİŞ

IoT cihazlarının sayısı hızla artmaktadır ve 2024 yılı itibarıyla dünya genelinde 17 milyar cihaza ulaşmıştır [1]. Bu sayının 2030 yılına kadar 30 milyara çıkacağı öngörülmektedir [1]. İnternete bağlı bu cihazlar evlerdeki akıllı termostatlardan fabrikalardaki karmaşık endüstriyel kontrol sistemlerine kadar uzanmaktadır [2]. Örneğin sağlık hizmetlerinde IoT cihazları gerçek zamanlı hasta takibine olanak tanıyarak daha hızlı müdahale süreleri ve daha kişiselleştirilmiş bakım sağlamaktadır [3]. Benzer şekilde, üretimde IoT sistemleri makine performansı hakkında gerçek zamanlı veri sağlayarak arıza süresini en aza indirmeye ve üretkenliği artırmaya yardımcı olur [4]. IoT'nin potansiyeli, akıllı altyapının trafik akışını optimize edebileceği, enerji tüketimini azaltabileceği ve kamu güvenliğini artırabileceğine kadar uzanmaktadır [5].

Ancak, birbirine bağlı bu geniş ekosistem aynı zamanda önemli güvenlik risklerini de beraberinde getirmektedir [6]. İnternete bağlı her bir cihaz, siber saldırılar için potansiyel bir giriş noktasını temsil etmektedir [6]. HP firması tarafından yapılan bir araştırma, IoT cihazlarının %70'inin saldırılara karşı savunmasız olduğunu ortaya koyarak IoT sistemlerindeki yaygın güvenlik endişelerini vurgulamıştır [7]. IoT güvenlik açıklarının dikkate değer bir örneği, güvenliği ihlal edilmiş binlerce IoT cihazının dağıtılmış hizmet reddi (DDoS) saldırısı başlatmak için kullanıldığı ve büyük web sitelerini çökerttiği 2016 Mirai botnet saldırısıydı [8]. IoT cihazlarının genellikle uygun güvenlik önlemleri alınmadan konuşlandırılmasıyla, potansiyel ihlaller için saldırı yüzeyi önemli ölçüde genişlemiştir [6]. IoT'deki güvenlik zorlukları, birçok internete bağlı cihazın kısıtlarından dolayı daha da kötüleşmektedir [6]. Geleneksel bilgi işlem sistemlerinin aksine, birçok IoT cihazı sınırlı işlem gücüne ve belleğe sahiptir, bu da güvenlik duvarları ve şifreleme gibi geleneksel güvenlik mekanizmalarının uygulanmasını zorlaştırmaktadır [9]. Bu durum, hafif kriptografi ve kaynak kısıtlı ortamlar için uyarlanmış güvenli iletişim protokollerine giderek daha fazla odaklanılmasına yol açmıştır [9] Ayrıca, IoT cihazlarının basit algılayıcılardan karmaşık makinelere kadar değişen heterojen yapısı, birlikte çalışabilirlik zorlukları oluşturmakta ve farklı platformlarda güvenlik önlemlerini zorlaştırmaktadır [9].

Son yıllarda, blockchain teknolojisi IoT güvenliğini artırmak için umut verici bir araç olarak ortaya çıkmıştır [10]. Başlangıçta Bitcoin gibi kripto para birimlerini oluşturan teknoloji olarak geliştirilen blockchain, bir ağda birden fazla düğümdeki işlemleri kaydeden merkezi olmayan bir defterdir [11]. Şeffaflık, değişmezlik ve merkezi olmayan kontrol özellikleri IoT sistemlerinin güvenliğini sağlamak için ideal bir çözüm haline getirmektedir [12]. Blockchain kullanılarak, IoT cihazları tarafından üretilen veriler saldırıya karşı korumalı bir şekilde kaydedilebilir ve veri bütünlüğü sağlanabilir [12]. Ayrıca, Blockchain'in merkezi olmayan yapısı, merkezi bir otoriteye olan ihtiyacı ortadan kaldırarak sistemdeki tek hata noktası riskini azaltmaktadır [10].

Blockchain ayrıca IoT güvenliği ile ilgili bazı temel zorlukların ele alınmasına da yardımcı olabilir [12]. Örneğin, merkezi bir sunucuya güvenmeden cihazlar arasında güven oluşturarak cihazdan cihaza iletişimi güvence altına almak için kullanılabilir [12]. Bu, özellikle geleneksel kısıtlı istemci-sunucu modeli için önemlidir [13]. Ayrıca, akıllı sözleşmeler (anlaşma şartlarının doğrudan koda yazıldığı kendi kendini yürüten sözleşmeler) IoT sistemlerindeki süreçleri otomatikleştirmek için kullanılabilir, bu da güvenliği ve verimliliği daha da artırır [10]. Örneğin, tedarik zinciri yönetiminde akıllı sözleşmeler, ürünler teslim edildiğinde ödemeleri otomatik olarak tetikleyerek dolandırıcılık riskini azaltabilir [14]. Avantajlarına rağmen, blockchain'in IoT ile entegrasyonunda dezavantajları da vardır. En büyük sorunlardan biri ölçeklenebilirliktir [15]. Bitcoin ve Ethereum gibi geleneksel blockchain ağları, büyük işlem hacimlerinin üstesinden gelmekte zorlanmakta ve bu da onları IoT sistemlerinin yüksek veri çıkışı için verimsiz hale getirmektedir [16]. Bu sorunu ele almak için Hyperledger Fabric gibi yeni blockchain platformları geliştirilmekte ve kurumsal düzeyde uygulamaları destekleyebilecek daha verimli fikir birliği mekanizmaları sunmaktadır [17]. Ek olarak, blockchain ağlarının, özellikle de iş ispatı fikir birliği algoritmalarına dayalı olanların enerji tüketimi, özellikle enerji verimliliğinin kritik olduğu IoT ortamlarında sürdürülebilirlikle ilgili endişeleri artırmaktadır [18].

1.1. SİBER GÜVENLİK

Siber güvenlik; sistemleri, ağları ve programları dijital saldırılardan koruma uygulamasıdır. IoT cihazlarının yaygınlaşmasıyla birlikte, siber güvenlik ortamı evrim geçirerek her zamankinden daha karmaşık hale gelmiştir [8]. IoT cihazları genellikle kısıtlı güvenlik özellikleri ile çalışır ve bu da onları siber suçlular için birincil hedef haline

getirir [19]. Çok sayıda IoT bağlantısı, saldırılar için potansiyel giriş noktalarını artırmakta, gelişmiş ve esnek güvenlik protokolleri gerektirmektedir [20].

Siber tehditlerin katlanarak artması, veri ihlallerini siber güvenlik endişelerinin ön saflarına taşımıştır [9]. IBM'in 2024 raporuna göre, bir veri ihlalinin ortalama maliyeti 4,86 milyon dolar olup, yetersiz güvenlik savunmalarının mali sonuçlarını vurgulamaktadır [21]. Özellikle sağlık ve finans sektörleri, işledikleri hassas kişisel veriler göz önüne alındığında savunmasız durumdadır [21].

Siber güvenlikteki önemli bir gelişme, bir ağın içinde veya dışında, tüm cihazlara uygun kimlik doğrulama olmadan güvenilemeyeceğini varsayan sıfır güven modelinin benimsenmesidir. 1983 yılında kurulan, dünya çapında iş ve teknoloji pazar araştırmaları yapan Forrester Research analiz firması tarafından tanıtılan sıfır güven çerçevesi, her kullanıcının ve cihazın sürekli olarak izlenmesini ve doğrulanmasını vurgulayarak yetkisiz erişim potansiyelini önemli ölçüde azaltmaktadır. Bu model ile kuruluşlar sıkı erişim kontrolleri ve ağ segmentasyonu uygulayarak bir ihlal meydana gelse bile hassas bilgilerin korunmasını sağlar [22].

Modern siber güvenliğin bir diğer kritik yönü de bulut güvenliğidir. Daha fazla firma/şirket/kamu verilerini buluta taşıdıkça, bu verilerin güvenliğini sağlamak en önemli öncelik haline gelmiştir. Bulut ortamları saldırılara karşı savunmasızdır ve verilerin gizliliğinin ve güvenliğinin sağlanması sağlam şifreleme ve çok faktörlü kimlik doğrulama (MFA) protokolleri gerektirir [23]. 1979 yılında kurulan, araştırma ve danışmanlık şirketi olan Gartner tarafından yapılan araştırma, ortaya çıkan tehditleri ele almak ve hassas bilgileri korumak için kapsamlı bulut güvenlik stratejilerine duyulan ihtiyacın altını çizmiştir [24]. Bu nedenle siber güvenlik önlemleri, bulut altyapısını ve verilerini yetkisiz erişime, veri kaybına ve ihlallere karşı güvence altına almayı da kapsamalıdır [25].

Geleneksel siber güvenlik önlemlerine ek olarak, yapay zekâ (YZ) ve makine öğrenmesi (MÖ) gibi yeni teknolojiler de tehditleri gerçek zamanlı olarak tespit etmek ve azaltmak için kullanılmaya başlanmıştır. Bu teknolojiler, ağ trafiği modellerindeki anormallikleri tespit ederek potansiyel tehditler için erken uyarılar sağlamakta ve güvenlik olaylarına müdahale süresini kısaltmaktadırlar. YZ odaklı siber güvenlik sistemleri, saldırılar daha karmaşık hale geldikçe tehditleri önceden tespit etmek ve etkisiz hale getirmek için gerekli hale gelmektedir [26].

Tüm bunların yanında blockchain teknolojisi de siber güvenliği desteklemek için umut verici bir yol sunmaktadır. Blockchain'in merkezi olmayan yapısı, tek bir hata noktasını ortadan kaldırdığı için güvenli kılar. Ayrıca, veri bütünlüğü ve güvenliğini sağlamada da kullanımı önemli ölçüde ilgi görmüştür [27]. Blockchain kayıtlarının değişmezliği, depolanan verilerin ele geçirilmesi veya değiştirilmesinin neredeyse imkânsız olduğu anlamına gelir [28]. Bu da onu IoT ekosistemlerindeki işlemlerin, dijital kimliklerin ve veri alışverişlerinin güvenliğini sağlamada değerli bir araç haline getirir [10]. 2008 yılında Bitcoin'i icat ederek blockchain teknolojisinin temellerini atan Nakamoto tarafından yapılan araştırma, blockchain'in çeşitli uygulamalarda şeffaflığı ve güvenliği nasıl artırabileceğini göstermiştir [11].

IoT cihazlarının sağlık hizmetlerinden akıllı şehirlere kadar günlük sistemlere artan entegrasyonu, gelişmiş siber güvenlik stratejilerine olan ihtiyacı daha da vurgulamaktadır. Bu cihazlar, yenilik ve verimlilik sağlarken, geniş kapsamlı sonuçları olabilecek saldırılara karşı hassastır [2]. Bu cihazların, verilerin ve ağların güvenliğini sağlamak için şifreleme, kimlik doğrulama protokolleri, yapay zekâ odaklı tehdit tespiti ve blockchain gibi gelişmiş teknolojileri birleştiren çok yönlü bir yaklaşım gerekmektedir [29].

1.2. IOT

Nesnelerin İnterneti (IoT), cihazların ve nesnelerin internet aracılığıyla birbirine bağlanmasını ifade eden ve bunların veri toplamasına, paylaşmasına ve otonom olarak hareket etmesine olanak tanıyan dönüştürücü bir kavramdır [30]. IoT; sağlık, tarım, üretim ve akıllı şehirler de dâhil olmak üzere çok sayıda sektörü kapsamakta ve işletmelerin ve bireylerin teknolojiyle etkileşim biçimini temelden değiştirmektedir [20]. IoT kavramı 2000'li yılların başında ortaya çıkmıştır, ancak kökleri RFID (Radyo Frekansı Tanımlama) teknolojisinin nesneleri izleme yöntemi olarak ilgi görmeye başladığı 1980'lere kadar uzanmaktadır [31].

Temelinde IoT, genellikle veri toplayan ve ileten algılayıcılar ve iletişim yetenekleriyle donatılmış, birbirine bağlı fiziksel cihazlardan oluşan bir ağ aracılığıyla çalışır [30]. Bu cihazlar ev aletleri ve giyilebilir cihazlardan endüstriyel makinelere kadar uzanmakta ve her biri geniş bir bağlı sistemler ağının oluşturulmasında önemli bir rol oynamaktadır [32]. IoT'nin en önemli faydalarından biri, operasyonel verimliliği artırma ve maliyetleri

düşürme potansiyelidir [30]. Örneğin, endüstriyel alanda IoT cihazları ekipman performansını gerçek zamanlı olarak izleyebilir, bu da arıza süresini azaltır ve makinelerin ömrünü uzatmasına olanak sağlar [30]. Benzer şekilde, tarımda IoT algılayıcıları toprak koşullarını, hava durumunu ve mahsul sağlığını izleyerek çiftçilerin kaynak kullanımını optimize etmesini ve mahsul verimini artırmasını sağlar [33]. Bu uygulamalar, IoT'nin geleneksel endüstrileri nasıl daha veri odaklı, otomatik sistemlere dönüştürdüğünü göstermektedir.

Bununla birlikte, IoT'nin birçok avantajlarına rağmen, özellikle siber güvenlik alanında çok sayıda zorlukla karşı karşıyadır [6]. IoT cihazlarının sınırlı işlem gücü ve depolama alanına sahip olması, sağlam güvenlik protokollerinin uygulanmasını zorlaştırmaktadır [19]. Ayrıca, IoT cihazlarını her biri farklı standartlara ve iletişim protokollerine sahip olması, heterojen olmasını ve tüm ağın güvenliğini sağlama görevini zorlaştırmaktadır [6]. 2005 yılında kurulan, siber güvenlik alanında dünya çapında tanınan Palo Alto Networks teknoloji firması tarafından yapılan bir araştırma, IoT cihaz trafiğinin %98'inin şifrelenmeden kaldığını ortaya koyarak IoT ağlarında gelişmiş güvenlik önlemlerine duyulan acil ihtiyacı vurgulamıştır [34].

Birlikte çalışabilirlik, IoT için bir başka büyük zorluktur [6]. Farklı üreticilerin cihazları genellikle tescilli iletişim standartlarını kullanır ve bu da cihazların sorunsuz bir şekilde birlikte çalışmasını zorlaştırır [19]. Evrensel standartların eksikliği, IoT sistemlerinin ölçeklenebilirliğini ve etkinliğini engellemektedir. Bu sorunun ele alınması, farklı platformlar ve ekosistemler arasında cihaz uyumluluğunu ve veri paylaşımını teşvik eden endüstri çapında standartların geliştirilmesini gerektirecektir [35].

Bu zorluklara yanıt olarak, blockchain teknolojisi IoT sistemlerinin güvenliğini ve birlikte çalışabilirliğini artırmak için potansiyel bir çözüm olarak önerilmiştir [36]. Blockchain'in merkezi olmayan ve değişmez defteri, IoT verilerini ve işlemlerini yönetmek için şeffaf çerçeve sağlayabilir. Ayrıca, merkezi bir otoriteye olmadan güvenli cihaz kimlik doğrulaması, veri doğrulama ve gerçek zamanlı işleme sağlar [10]. IoT genişlemeye devam ettikçe, akıllı şehirler üzerindeki etkisi de giderek daha belirgin hale gelmektedir [3]. Dünya çapındaki şehirler, daha verimli ve sürdürülebilir ortamlar oluşturmak için IoT'yi kentsel altyapıya entegre etmektedir [3]. Akıllı algılayıcılar trafik akışını, hava kalitesini ve enerji tüketimini izleyerek şehir planlamacılarının kaynak tahsisini optimize etmesine ve çevresel etkiyi azaltmasına olanak tanır [3]. 1926 yılında kurulan, dünya genelindeki lider şirketlere yönetim danışmanlığı hizmeti sunan

McKinsey firmasına göre, IoT tarafından desteklenen akıllı şehir girişimleri 2025 yılına kadar tahmini olarak piyasaya 1,6 trilyon dolarlık bir ekonomik değer katabilir [5]. Bu teknolojilerin potansiyel faydaları arasında trafik sıkışıklığının azaltılması, kamu güvenliğinin iyileştirilmesi ve daha verimli atık yönetim sistemleri yer almaktadır [3].

IoT, giyilebilir cihazların ve uzaktan izleme sistemlerinin hasta sonuçlarını iyileştirdiği ve sağlık hizmeti maliyetlerini düşürdüğü sağlık hizmetlerinde de önemli adımlar atmaktadır. Akıllı saatler, spor takip cihazları ve taşınılabilir tıbbi cihazlar gibi gerçek zamanlı sağlık verileri toplayarak doktorların hastaları uzaktan izlemesine ve potansiyel sağlık sorunlarını kritik hale gelmeden önce tespit etmesine olanak sağlamaktadır [37].

1.3. BLOCKCHAIN

Blockchain teknolojisi, 2008 yılında Satoshi Nakamoto tarafından Bitcoin'in piyasaya sürülmesinden bu yana büyük ilgi gören merkezi olmayan, dağıtılmış bir defter sistemidir. Bir blockchain, her biri kriptografik teknikler kullanılarak güvence altına alınan ve doğrulanan işlemlerin bir listesini içeren bir dizi bloktan oluşur [11]. Blockchain'in birincil yeniliği, işlemleri denetlemek için merkezi bir otoriteye olan ihtiyacı ortadan kaldırırken değişmezlik ve şeffaflık sağlama yeteneğidir [16].

Blockchain kavramı kripto para biriminin ötesinde de uygulanabilmektedir [28]. Örneğin akıllı sözleşmeler, özellikle Ethereum gibi platformlarda blockchain'in temel bir özelliğidir [38]. Önceden tanımlanmış kurallara sahip bu kendi kendini yürüten sözleşmeler, sözleşme şartlarının otomatik ve şeffaf bir şekilde uygulanmasını sağlar [39]. Blockchain, merkezi olmayan yapısı sayesinde tek noktadan hata veya sahtekârlık riskini en aza indirerek finans, tedarik zinciri yönetimi ve sağlık hizmetleri gibi sektörler için cazip hale gelir [40]. Blockchain, tüm katılımcı düğümler arasında blockchain'in tek bir durumu üzerinde anlaşmaya varmak için kullanılan protokoller olan fikir birliği mekanizmaları aracılığıyla çalışır [41]. En yaygın fikir birliği algoritmalarından biri Bitcoin ve diğer bazı blockchain sistemlerinde kullanılan Proof of Work'tür (PoW) [42]. PoW'da katılımcılar ya da madenciler, işlemleri doğrulamak ve zincire yeni bloklar eklemek için karmaşık matematiksel bulmacaları çözerler [42]. Bu süreç ağın güvenli kalmasını ve kurcalanmaya karşı dirençli olmasını sağlar. Ancak PoW'un enerji yoğun olması, daha enerji verimli ve sürdürülebilir olan Proof of Stake (PoS) gibi alternatif fikir birliği mekanizmalarının geliştirilmesine yol açmıştır [43].

Sektörler çeşitli uygulamalar için blockchain teknolojisini hızla benimsemektedir. Tedarik zinciri sektöründe blockchain, ürünlerin üretiminden son tüketiciye kadar izlenebilirliğini sağlayarak dolandırıcılıkla mücadeleye ve şeffaflığı artırmaya yardımcı olmaktadır [44]. Sağlık hizmetlerinde blockchain, güvenli veri paylaşımı ve tıbbi kayıt yönetimi için kullanılmakta ve hasta verilerinin çalınmasına karşı korumalı ve gizli kalmasını sağlamaktadır [45]. Ayrıca, hükümetler dijital kimlik doğrulama, tapu sicil yönetimi ve güvenli oylama sistemleri için blockchain'i araştırmaktadır [28].

Blockchain'in en umut verici uygulamalarından biri, cihaz güvenliğini ve güvenini artırdığı IoT'dir [15]. Blockchain, merkezi olmayan cihaz kimlik doğrulamasını ve güvenli veri alışverişini mümkün kılarak IoT ağlarını siber saldırılara karşı daha dirençli hale getirmektedir [46]. Buna ek olarak, blockchain'in merkezi olmayan finans (DeFi) alanındaki rolü, bankalar gibi geleneksel aracılara ihtiyaç duymadan finansal hizmetlere erişim sağlayarak finans sektörünü dönüştürmektedir [47].

Avantajlarına rağmen blockchain'in zorlukları vardır. Ölçeklenebilirlik en önemli sorunlardan biridir [48]. Katılımcı ve işlem sayısı arttıkça blockchain yavaşlamakta ve daha fazla hesaplama gücü gerektirmektedir [48]. Bu durum, sharding ve Layer 2 protokolleri gibi ölçeklenebilir blockchain çözümlerinin araştırılmasına yol açmıştır [49]. Ayrıca, hükümetler ve kurumlar blockchain tabanlı varlıkların ve hizmetlerin nasıl sınıflandıracaklarını araştırmaktadır [50]. Sonuç olarak blockchain, verilerin dağıtık ağlarda nasıl depolandığı, doğrulandığı ve paylaşıldığı konusunda devrim niteliğinde bir değişimi temsil etmektedir [28]. Uygulamaları hızla genişlemekte, işlemlerin yürütülmesi ve verilerin yönetilmesi için daha güvenli, şeffaf ve verimli bir yol sunarak sektörleri dönüştürmektedir [51]. Teknoloji geliştikçe, blockchain'in yenilikleri ve gelişme potansiyeli de artmaya devam etmektedir.

1.4. ÇALIŞMANIN AMACI

Çalışmanın amacı, Hyperledger Fabric kullanarak bir blockchain ağı oluşturmanın avantajlarını ve dezavantajlarını sunmak ve ardından, OPNET benzetim aracı ile blockchain ile şifrelenmiş paketlerin iletimini sağlayan ZigBee tabanlı IoT ağlarının blockchain teknolojisinden nasıl etkilendiğini analiz etmektir.

1.5. TEZ ORGANİZASYONU

Bu tez çalışması şu bölümler halinde organize edilmiştir: Birinci bölümde, siber güvenlik, IoT ve blockchain teknolojisinden genel bahsedilmiş ve bu teknolojilerin IoT güvenliği üzerindeki etkisi ele alınmıştır. İkinci bölümde, literatürde yer alan IoT güvenliği ve blockchain teknolojisinin entegrasyonu ile ilgili çalışmalar incelenmiştir. Üçüncü bölümde, araştırmada kullanılan Hyperledger Fabric ve OPNET benzetimleri ayrıntılı olarak açıklanmıştır.

Dördüncü bölümde, Hyperledger Fabric ile blockchain ağı kurulmuştur. OPNET ile benzetim senaryoları sunulmuş, elde edilen sonuçlar değerlendirilmiştir. Son bölümde ise, elde edilen bulgular değerlendirilmiş, sonuçlar analiz edilmiş ve gelecekteki çalışmalar için önerilerde bulunulmuştur.

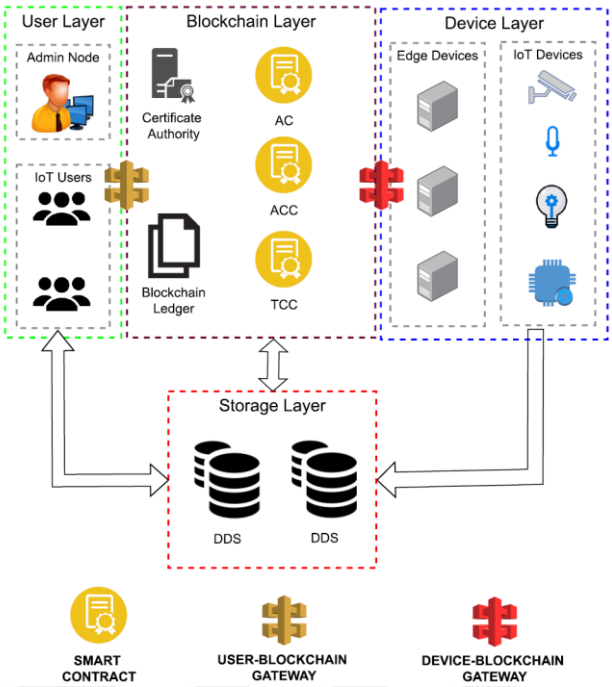
2. İLGİLİ ÇALIŞMALAR

S. Basudan [51] çalışmasında, IoT ve Blockchain'in bir araya gelmesiyle dinamik uygulamalarda güvenli işlemler için ölçeklenebilir bir çerçeve sunmaktadır. Ayrıca, dinamik cihaz yönetimi ve koşullu izlenebilirlik özellikleri ile DABG protokolü, hızlı işlem onayları, veri güvenliği ve gizliliği koruma potansiyeli de sunar. Gelecekte, federatif öğrenme ve gizliliği koruma yöntemlerinin entegrasyonu hedeflenmektedir.

A. Pathak ve arkadaşları [52], IoT ağlarında güvenlik sorunlarını ele almak için blockchain teknolojisinin kullanımına odaklanarak, edge computing teknolojisi ile yüksek işlem yüklerini ve enerji maliyetlerini azaltmayı amaçlamışlardır. Yeni bir Trust-Based Access Control Mechanism olan TABI (bkz. Şekil 2.1), kaynak kısıtlamalı IoT ağlarında uçtan uca güvenlik sağlamayı hedeflemektedir. Ayrıca, mekanizma, erişim kontrolü ve güven değerlendirme mekanizmalarını kullanarak kötü niyetli IoT kullanıcıları ve cihazlarının etkisini azaltmaya yönelmektedir. Gelecekteki çalışmalar, hizmet kalitesini iyileştirmeyi ve kötü niyetli IoT cihazlarını tespit etmeyi amaçlamaktadır.

S. Seshadri ve arkadaşları [53], IoT cihazlarının güvenliğini sağlamak için blockchain tabanlı bir izleme çerçevesi olan IoTCop'ı kullanmaktadırlar. Geleneksel sunuculardan farklı olarak, IoT cihazları coğrafi olarak dağılmış ve fiziksel sistemlere yakın konumlandırılabilir, bu nedenle güvenlik çözümlerinin karmaşıklığına rağmen kaynak kısıtlamalarıyla karşılaşırlar. Çalışma, bir cihazın tehlikeye girebileceğini varsayar ve tehlikeye giren cihazları otomatik olarak izole edebilme ihtiyacını vurgular. Bu amaçla, güvenlik politikalarını uygulamak için blockchain kullanımını önerilmiştir. İzinli bir blockchain (Hyperledger Fabric) ve ek donanım modülleri kullanarak önerilen çerçeve, düşük gecikme süresi ve iş yükü sunar ve mevcut IoT cihazlarının değiştirilmeden çerçeveye katılmasına olanak sağlar.

B. Bera ve arkadaşları [54], IoT destekli akıllı şebeke sistemlerinde yeni bir blockchain tabanlı erişim kontrol protokolü olan DBACP-IoTSG'yi incelemişler. DBACP-IoTSG, güvenli veri iletimini ve özel verinin korunmasını amaçlamaktadır, aynı zamanda diğer benzer şemalara göre daha iyi güvenlik ve düşük iletişim hesap maliyetleri sunmaktadır.



Şekil 2.1. TABI mimarisi [52]

Bir başka çalışma [55], RAFT fikir birliği protokolünü kullanan bir IoT blockchain ağı üzerinde aktif (karıştırma ve taklit) saldırıları ele almaktadır. Karıştırma saldırısı durumunda, kapsama olasılıklarını inceleyerek etkileri değerlendirir. Taklit saldırısını ise iletişim düğmesinin yol kaybını kullanarak tanımlanan yeni bir yöntem önerir ve yanlış alarm, kaçırılan algılama ve yanlış sınıflandırma olasılıklarını en aza indirmeyi amaçlamaktadır. Sonuçlar, karıştırma saldırısı için eşik değerinin arttığını, jammer yoğunluğunun kapsama olasılığını düşürdüğünü, taklit saldırısı içinse iletişim düğmesinin yol kaybının cihaz kimliği olarak kullanılabileceğini ve 10 dB bağlantı kalitesi için %95'ten fazla algılama olasılığı elde edilebileceğini göstermektedir.

Bir başka çalışmada ise [56], IoT için blockchain tabanlı güvenli ve hafif bir kimlik doğrulama şeması önerilmiştir. Önerilen çerçeve, blockchain ve MSR şifreleme algoritmasını birleştirerek merkezi olmayan, gizliliği koruyan ve hafif bir kimlik doğrulama sistemini gerçekleştirmektedir. Ayrıca, önerilen şemanın güvenliği analiz edilmiştir. Şemanın performansını Remix üzerinde uygulayarak ve diğer şemalarla hesaplama ve iletişim maliyetini karşılaştırarak değerlendirilmiştir.

Endüstriyel Nesnelerin İnterneti (IIoT) ağı için güvenli bir çerçeve öneren çalışma [57], güven yönetimi ve blockchain teknolojisinin birleşimini kullanarak, ağdaki kötü amaçlı

cihazların neden olduğu sorunları ele alır. Önerilen model, her IoT cihazının Güven Faktörünü hesaplayarak meşruiyetini belirler ve seçilen Koordinatör IoT Cihazı (CID) tarafından kullanılır. Ayrıca, yerel veri tabanının bilgilerinde değişiklikleri önlemek için bir blockchain tabanlı veri modeli kullanır. Yaklaşım, farklı ağ boyutları ve değerlendirme kriterleri için geniş kapsamlı bir doğrulama ile 91% başarı oranına ulaşmıştır. Bu çerçeve, IIoT ağlarında güvenliği arttırma konusunda etkili bir mekanizma sunmaktadır.

H. Liu ve arkadaşları [58], IoT cihazlarının özelliklerini ele alır ve geleneksel erişim kontrol yöntemlerinin bu büyük ölçekli IoT ortamında yetersiz kalmasını çözmek için Hyperledger Fabric blockchain çerçevesine dayalı bir erişim kontrol sistemi olan Fabric-IoT'u önermektedir. Sistem, cihaz sözleşmesi (DC), politika sözleşmesi (PC) ve erişim sözleşmesi (AC) olmak üzere üç tür akıllı sözleşme içerir. Fabric-IoT, merkezi olmayan, ince taneli ve dinamik erişim kontrol yönetimi sunar. İki grup benzetim deneyi sonuçları, Fabric-IoT'un büyük ölçekli talep ortamında yüksek veri iletim hızını sürdürebildiğini ve veri tutarlılığını sağlamak için dağıtılmış bir sistemde etkili bir şekilde fikir birliğine varabildiğini göstermektedir. Gelecekteki çalışmalar, Fabric-IoT'un ölçeklenebilirliğini iyileştirmeyi ve daha fazla IoT uygulaması entegrasyonunu desteklemeyi hedeflemektedir.

Diğer bir çalışmada [59], IoT cihazlarının veri topladığı bir ağ olan IoT‘nin, hassas bilgileri sızdırma riskini azaltmak amacıyla yetkilendirilmiş kullanıcıların verilere erişmesine izin veren bir erişim kontrolü sunan grupları düzenleme ve yönetme modelini önermektedir. Özellikle, anahtar değiştirme maliyeti azaltılmaktadır. IoT cihazları kaynak açısından sınırlı olduğu için, anahtar değiştirme maliyeti arttıkça ağın ömrü azalabilir. Ayrıca, birden fazla kullanıcı arasında grup iletişimi kullanılmadığında bir sorun vardır. Birden fazla kullanıcının kolayca tüm verilere erişebildiği durumda hassas bilgi sızıntısı artmaktadır. Bu sorunu çözmek için yalnızca verileri paylaşması gereken kullanıcılar Hyperledger Fabric'e dayalı bir grup oluşturur. Yaklaşım, aynı grup anahtarına sahip kullanıcıları gruplandırır ve grup içinde güvenli iletişim bağlantıları kullanarak hassas verileri korur. Ayrıca, yeniden anahtar verme işlemi için güvenilir bir ajan, grup içindeki kullanıcılara yeni bir grup anahtarı gönderir. Bu sayede, verilerin güvenliği garanti altına alınır ve ağ ömrü uzatılır. Performans analizinin sonuçları, önerilen Hyperledger Fabric tabanlı hafif grup yönetimi (H-LGM) yönteminin depolama maliyeti, gecikme ve işleme süresi açısından mevcut yöntemi aştığını göstermektedir.

Başka bir çalışmada ise [60], geleneksel IoT erişim kontrol yöntemlerinin eksikliklerini ele alarak, Hyperledger Fabric blockchain çerçevesi kullanılarak ABAC-HLFBC adlı bir erişim kontrol modeli önermektedir. Bu model, erişimi sunulan özelliklere dayandırarak sağlar, yalnızca ilgili erişim politikalarına uygun özelliklere sahip kullanıcılara erişim izni verir. Önerilen model, Fabric-IoT modeli ile karşılaştırılmış ve performans açısından daha etkili olduğu gösterilmiştir. Çalışma ayrıca gelecekteki çalışma önerilerini de içerir, bu çalışmalar arasında modelin daha fazla organizasyon ve kanal üzerinde uygulanması, güvenlik testleri ve IoT fiziksel cihazlar kullanılarak güvenilirlik ve performans testleri yer alır. Bu çalışma, blockchain tabanlı erişim kontrolünün önemini ve potansiyelini vurgulayan önemli bir kaynaktır.

Diğer bir çalışmada [61], blockchain'in kripto para dışında birçok uygulamasının olduğu vurgulanmaktadır. Özellikle, IoT tabanlı ağlarda blockchain kullanımının analiz edilmesi gerektiği belirtilmektedir. IoT cihazlarının sınırlı yetenekleri ve blockchain protokolünün şifreli veri tabanlı doğası nedeniyle bazı zorluklar yaşandığı ifade edilir. Çalışma, blockchain'in IoT güvenliğine nasıl katkı sağlayabileceğini inceleyerek, blockchain tabanlı IoT yapısının geleneksel bir IoT yapısına göre daha güvenli olduğunu göstermektedir.

Diğer bir çalışma ise [62], hızla gelişen IoT'nin bir sonucu olarak daha fazla IoT cihazının sürekli iletişim halinde olduğu bir ortamda, geleneksel merkezi IoT güvenlik yapılarının veri depolama alanı, veri güvenilirliği, ölçeklenebilirlik, işletme maliyetleri ve sorumluluk değerlendirmesi açısından sınırlı olabileceği bir zemini ele almaktadır. Çalışma, blockchain teknolojisi ve bulut depolama tarafından oluşturulan küçük bir dağıtılmış veritabanına dayalı yeni bir anahtar bilgi depolama çerçevesi önermektedir. Verilerin güvenilirliği, ölçeklenebilirliği ve sorumluluk değerlendirme sorunlarını çözmek amacıyla, tüm şifreli anahtar iletişim verileri bulut sunucusuna yüklenecektir, ancak bu verilerin özetleri "IoT defteri" olarak adlandırılan bir dağıtılmış veritabanına kaydedilecektir. Ayrıca, veri güvenliğini garanti etmek ve etkili bir arama işlevi sağlamak için "IoT defteri" için güvenli arama şemasını tasarlar ve ASPE yaklaşımını kullanır. Bu önerilen şemaların güvenli ve verimli olduğu sentetik veri kümesi üzerinde yapılan deneylerle gösterilir. Bu çerçeve, IoT verilerinin güvenli ve verimli bir şekilde yönetilmesini sağlamaktadır.

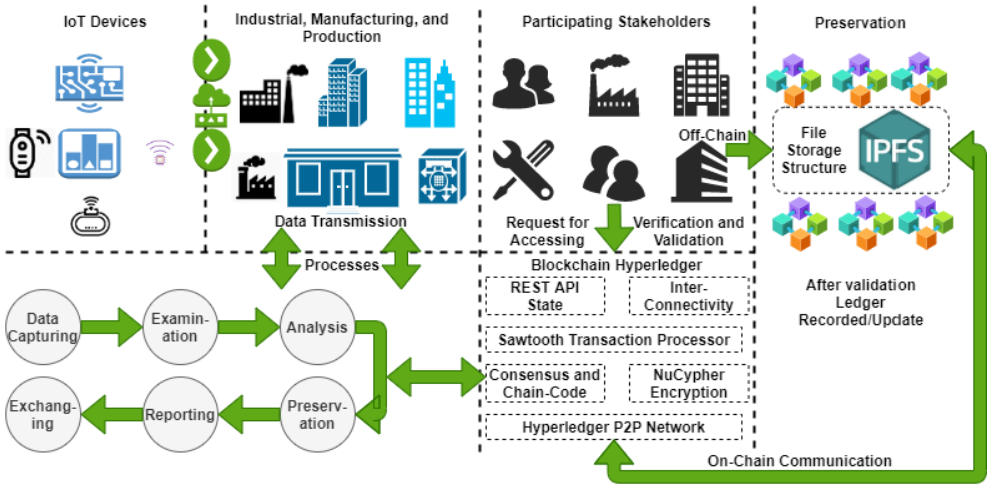
Z. Gong-Guo ve Z. Wan çalışmasında [63], IoT cihazlarının sınırlı kaynakları ve mobilitesi göz önüne alındığında, geleneksel merkezi güvenlik doğrulama yöntemlerinin

IoT ortamındaki güvenlik doğrulamayı desteklemekte zorlandığı bir konteks içinde IoT-chain adlı bir güvenlik kimlik doğrulama sistemi önerilmektedir. IoT-chain, Hyperledger Fabric blockchain çerçevesine dayalı bir özellik tabanlı güvenlik kimlik doğrulama sistemi sunar ve kullanıcılar için güvenlik doğrulama yöntemi uygular. Deney sonuçları, IoT-chain'in yüksek işlem kapasitesini sürdürebildiğini ve dağıtılmış sistemlerde etkili bir şekilde fikir birliğine ulaşabildiğini göstermektedir. Gelecekteki çalışmalar, fikir birliği verimliliği, sistem performansı ve akıllı sözleşmelerin özelleştirilebilirliği gibi alanlarda iyileştirmelere odaklanabilir.

D. Li ve arkadaşları [64], geleneksel IoT güvenliği sorunlarını ele alarak blockchain tabanlı bir kimlik doğrulama ve güvenlik mekanizması önermektedir. Önerilen sistem, cihazlara benzersiz kimlikler tanımlar ve verileri güvenli bir şekilde kaydeder. Düşük maliyeti ve ek güvenlik avantajları ile IoT için uygundur ve gelecekte IoT verilerinin yönetimine odaklanır.

E. Shammar ve arkadaşları [15], IoT ve blockchain entegrasyonunu güvenlik perspektifinden ele almaktadır. Blockchain, IoT alanında merkezi olmayan, güvenilir ve güvenli bir çevre oluşturmak için kullanılabilecek potansiyele sahiptir. Ancak, bu entegrasyonun karmaşıklıklarını derinlemesine inceleyen çok az makale bulunmaktadır. Çalışma [15], 2017-2021 yılları arasında yayınlanan blockchain tabanlı IoT güvenliği çözümlerini incelemekte ve bu alandaki güncel araştırma konularını ve eğilimleri ele almaktadır. Çalışma, IoT ve blockchain entegrasyonunun temel sorunlarını ve zorluklarını incelemekte ve bu zorlukları aşmak için şimdiye kadar yürütülen araştırma çabalarını incelemektedir.

Endüstriyel IoT için Blockchain teknolojisinin güvenlik uygulamalarını inceleyerek, mevcut zorlukları değerlendiren çalışma [36] Şekil 2.2'de görüldüğü gibi bir Blockchain Hyperledger Sawtooth tabanlı çerçeve önerir, bu çerçeve endüstriyel faaliyetlerin güvenli kayıt altına alınmasını ve iletişimini desteklemektedir. Çalışma, akışkan endüstriyel cihaz işlemleri ve veri iletimi için çeşitli protokoller ve zincir kodları sunar. Önerilen çerçevenin endüstriyel, üretim ortamlarında genel amaçlı bir çözüm olarak uygulanabileceği belirtilir. Çalışma, endüstriyel IoT ve Blockchain teknolojisinin birleşimini inceleyerek gelecekteki uygulamalar için umut verici bir yaklaşım sunar.



Şekil 2.2. Blockchain hyperledger sawtooth özellikli gizlilik koruma ve güvenlik çözümü ile önerilen endüstriyel IoT [36]

Bir diğer çalışma ise [12], blockchain teknolojisinin IoT alanında nasıl kullanılabileceğini ve buna ilişkin güvenlik sorunlarını ele almaktadır. IoT teknolojisinin gelişimi, dağıtılmış sistemlerde önemli ilerlemelere yol açmıştır. Blockchain kavramı, ağdaki verileri ve işlemleri depolamak ve paylaşmak için merkezi olmayan bir veri yönetim sistemi gerektirir. Çalışma, potansiyel güvenlik saldırılarını ayrıntılı bir şekilde analiz eden ve bu saldırılara karşı alınabilecek mevcut çözümleri sunan faktörleri ele almaktadır. Ayrıca, blockchain güvenliğini artırma çözümlerini özetleyerek, güvenlik zafiyetlerine karşı kullanılabilecek ana noktaları sunmaktadır. Son olarak, çalışma blockchain-IoT sistemlerine ilişkin açık sorunları ve gelecekteki araştırma yönelimlerini tartışmaktadır.

F. Oikonomou ve arkadaşları ise [65], IoT tabanlı sağlık takip sistemlerinin güvenliğini artırmak için Hyperledger Fabric tabanlı bir blockchain mimarisi önermektedir. Bu öneri, sınırlı işlem gücü, depolama kapasitesi ve pil ömrüne sahip IoT cihazlarının karmaşık işlemleri destekleyememesi sorununu ele almayı amaçlamaktadır. Ayrıca, bu mimari yerel ve global düzeyde veri bütünlüğü ve kullanılabilirlik sağlamayı hedeflemektedir. Gelecekteki çalışmalar, önerilen mimariyi sanal bir ortamda uygulamayı ve işlem hızı, kaynak tüketimi, ağ kullanımı ve gecikme gibi performans metrikleri açısından değerlendirmeyi içerebilir.

Diğer çalışmada ise [66], IoT verilerinin güvenliği ve doğrulanmasını ele alırken önemli veriler sunmaktadır. İlk olarak, IoT verilerinin güvenliğini sağlamak için makine öğrenme algoritmalarıyla veri analizi yapılmıştır. Denemeler, Pearson korelasyonu ve Lojistik Regresyon gibi algoritmaların kullanılmasıyla 80 özellikli IoTID20 veri kümesinden 15 özelliğin seçilmiştir. Bu, hızlı tahmin modellerine ulaşmak için hesaplama yoğunluğunu

azaltmıştır. Çalışma ayrıca AdaBoost ve Random Forest sınıflandırıcılarının en iyi performansa sahip olduğunu ortaya koymuştur. AdaBoost'un doğruluk oranı %96.3, hassasiyet %97.9, geri çağırma %95 ve F1 skoru %96.3 olarak ölçülmüştür. Random Forest ise %96.2 doğruluk, %96.2 hassasiyet, %96.2 geri çağırma ve %96.2 F1 skoruna sahiptir. Ayrıca, blockchain teknolojisi kullanılarak IoT verilerinin güvenli bir şekilde saklandığı gösterilmektedir. Blockchain, güvenilir düğümler tarafından dijital imza kullanarak verilerin doğrulandığı ve verilerin güvenliği için girişlerin karma işlemine dayanmıştır. Sonuçlar, ayrıca örneklem büyüklüğü ile tahmin süresi arasında pozitif bir ilişki olduğunu göstermiştir. Deneyler, Decision Tree ve Naïve Bayes sınıflandırıcılarının zaman tahmininde en iyi sonuçları verdiğini göstermiştir. Ancak IDS'nin %100 doğruluğa sahip olmadığına dikkat çekilerek, gelecekte IDS'nin geliştirilmesi ve diğer blockchain platformlarının incelenmesi önerilmiştir.

Saldırı tespitinde Makine Öğrenmesi yöntemleri inceleyen çalışma [67], UNSW-NB15 veri seti üzerinde yapılan makine öğrenimi yöntemlerinin performans analizini incelemekte ve karşılaştırmaktadır. Rassal Orman algoritması, yapılan testlerde en yüksek doğruluk oranına ulaşmıştır. Ayrıca, reliefF puanlama yöntemi kullanılarak özellik sayısı azaltıldığında performansta artış gözlemlenmiştir. Özellikle, Sinir Ağları algoritması, özellik seçimi sonrasında en yüksek doğruluk oranına sahip olarak belirlenmiştir. Çalışmanın literatürle karşılaştırıldığında, reliefF yönteminin özellik seçiminde kullanılmasının daha iyi sonuçlar elde edilmesine katkı sağladığı görülmektedir. Gelecek çalışmalarda, Birliktelik Kural Çıkarımı ve Topluluk Öğrenimi gibi yöntemlerin kullanılarak daha yüksek doğruluk oranlarına ulaşılması hedeflenmektedir.

Diğer bir çalışma ise [68], IoT güvenliği ve gizliliği için ölçek ve dağınıklık zorluklarını vurgulayarak, enerji ve işlem maliyetleri açısından uygun olmayan blockchain tabanlı bir yaklaşımı ele almaktadır. Akıllı ev örneğinde, POW ve madeni para kavramlarını ortadan kaldırarak hafifletilmiş bir blockchain modeli öneriyor. Çalışmada, akıllı ev katmanının çekirdek bileşenlerini ve işlevlerini ayrıntılı olarak tanımlayarak, önerilen BC tabanlı akıllı ev çerçevesinin güvenliğini analiz edilmiştir. Benzetim sonuçları, önerilen yöntemin düşük maliyetli olduğunu ve düşük kaynaklı IoT cihazları için önemli güvenlik ve gizlilik avantajları sunduğunu göstermektedir.

S. Mohanty ve arkadaşları çalışması [69], Internet of Things (IoT) için özellikle geliştirilmiş olan verimli Hafif Entegre Blockchain (ELIB) modelini sunmaktadır. ELIB

modeli, bir akıllı ev ortamında uygulanmış ve çeşitli IoT senaryolarındaki uygulanabilirliğini doğrulamak için önemli bir örnek olarak kullanılmıştır. ELIB modeli, merkezi bir yöneticiden yararlanarak kaynak kısıtlı akıllı ev kaynaklarına, veri iletimi için paylaşılan anahtarlar oluşturan, gelen ve giden her isteği işleyen bir yapı sunmaktadır. Sunulan ELIB modeli, hafif fikir birliği algoritması, sertifikasız şifreleme ve Dağıtılmış Throughput Yönetimi (DTM) şemasını içeren üç optimizasyonu içermektedir. Farklı senaryolarda yapılan ayrıntılı bir Benzetim, işleme süresi, enerji tüketimi ve iş yükü açısından gerçekleşmektedir. ELIB, karşılaştırma yapılan temel yönteme göre işleme süresinde %50 tasarruf sağlar ve minimum enerji tüketiminde 0.07 mJ elde eder. Elde edilen deneysel sonuçlar, ELIB'nin çeşitli değerlendirme parametreleri altında maksimum performans gösterdiğini göstermektedir.

Diğer bir çalışma ise [70], IoT için optimize edilmiş bir Hafif Ölçeklenebilir Blockchain (LSB) modelini tanıtmaktadır. LSB, akıllı ev senaryosunda incelenmiş ve düşük kaynaklı cihazlar için merkezi bir yönetici kullanarak güvenlik ve gizlilik sağlamaktadır. Algoritmalarla optimize edilen LSB, geniş bir güvenlik analizi sonucunda saldırılara karşı dirençli olduğunu göstermektedir. Benzetimler, LSB'nin bant genişliğini ve işleme süresini azaltarak yüksek performans sunduğunu göstermektedir. LSB'nin gelecekteki çalışmalarında, gerçek dünya performansını değerlendirmek ve farklı uygulama alanlarındaki uygunluğunu araştırmak yer almaktadır.

M. Du ve arkadaşları çalışmasında [71], IoT güvenliği için etkili bir çözüm olan Spacechain adlı üç boyutlu bir blockchain mimarisi tanıtılmaktadır. Heterojenlik ve ölçeklenebilirlik sorunlarına çözüm getirmek amacıyla özgün veri yapıları ve paralel iş akışları tasarlanmıştır. Ayrıca, yüksek iş yükü altında güvenlik ve ağ performansını artırmak için 3D-GHOST fikir birliği mekanizması önerilmiştir. Yapılan detaylı güvenlik analizi ve kapsamlı deneysel doğrulama, Spacechain'in performansını göstermektedir. Gelecek çalışmalar için bazı açık güvenlik sorunları da özetlenmiştir.

Diğer bir çalışma ise [72], IoT güvenliğini artırmak amacıyla geliştirilen üç katmanlı bir blockchain tabanlı IoT güvenlik mimarisi olan IoTchain sunulmaktadır. Kimlik doğrulama, erişim kontrolü, gizlilik koruması, hafif özellik, bölgesel düğüm hataya dayanıklılık, DDoS direnci ve depolama bütünlüğü sağlamak üzere tasarlanan bu mimari, bir kimlik doğrulama katmanı, bir blockchain katmanı ve bir uygulama katmanını içermektedir. Ayrıca, IoTchain'in performansını değerlendirip gerçek bir IoT uygulamasında kullanımını gösterilmiştir.

Bir diğer çalışmada ise [73], IoT cihazlarının güvenliğini artırmak amacıyla Fusion Chain adlı hafif bir blockchain önerilmektedir. Önerilen çözümler sayesinde blockchain'in boyutu önemli ölçüde azalmış, PBFT fikir birliği algoritması kullanılarak düşük hesaplama gücüne ihtiyaç duyulmuş ve PKI şifreleme ile veri gizliliği sağlanmıştır. Fusion Chain'in IoT cihazları için uygun olduğunu gösteren deney sonuçları, veri güvenilirliğini ve bütünlüğünü sağlayarak Mirai botnet ve DDoS saldırıları gibi IoT uygulamalarının güvenlik zafiyetlerini çözebileceğini göstermektedir. Şu anda, Fusion Chain'i kullanarak IoT cihazlarını gruplara bölen bir inter-chain yapılandırılmış blockchain üzerine yüksek işlem hızı (TPS) sağlayan bir hafif blockchain üzerine araştırmalar devam etmektedir.

A. Rajawat ve arkadaşları çalışmasında ise [74], sağlık sektöründeki veri yönetimi sorunlarına yönelik bir çözüm olarak Blockchain tabanlı bir model önerilmektedir. Sağlık IoT cihazlarından elde edilen verilerin güvenliği için kullanılan SHA256 karma algoritmasıyla, her veri değişikliği güvenli bir şekilde doğrulanmakta ve bu sayede sağlık verilerinin güvenliği artırılmaktadır. Önerilen algoritma, her bir bloğa SHA256 karma algoritması uygulayarak, verilerin kötü niyetli kaynaklar tarafından değiştirilememesini sağlamaktadır. Doğrulanabilirlik, uygunluk, kapsamlılık, benzersizlik, sağlamlık ve zorlamaya direnç öncelikleri doğrultusunda tasarlanan bu Blockchain tabanlı model, gelecekteki çalışmalara yönelik çeşitli olanaklar sunmaktadır.

Diğer bir çalışma ise [75], IoT güvenliği için blockchain ve SDN kombinasyonunu içeren yeni bir mimari olan BCSDN-IoT'yi önermektedir. Bu mimari, büyük ölçekli IoT ağlarının karşılaştığı zorlukları ele almak ve yeni hizmet gereksinimlerini karşılamak için geliştirilmiştir. BCSDN-IoT modeli, tehdit önleme, veri koruma ve erişim kontrolü gibi korumaları oluşturmak ve dağıtmak, aynı zamanda önbellek zehirlenmesi, ARP sahteciliği, DDoS/DoS saldırıları gibi ağ saldırılarını saptamak amacıyla tasarlanmıştır. Bu yaklaşım, IoT yönlendirme cihazlarının gerektiğinde en güncel akış kural tablosunu kontrol etmelerine izin vererek saldırı penceresi süresini minimize etmeye odaklanmaktadır. Performans değerlendirmesi, önerilen modelin ölçeklenebilirlik, savunma etkileri, doğruluk oranları ve performans üzerindeki etkilerine dayanmaktadır.

M. Hammi ve arkadaşları çalışmasında [76], IoT için etkili bir merkezi olmayan kimlik doğrulama sistemi olan "Bubbles of Trust" önerilmektedir. Bu yaklaşım, nesnelerin birbirini tanımasını ve doğrulamasını sağlayarak veri bütünlüğünü ve erişilebilirliğini korur. Blockchain'in güvenlik avantajlarına dayanan bu yöntem, güvenli sanal bölgeler

(bubbles) oluşturarak nesnelerin birbirine güvenebileceği bir ortam sağlar. C++ dilini ve Ethereum blockchain kullanarak gerçek bir uygulama sunan çalışmanın sonuçları, IoT güvenlik gereksinimlerini karşılama, etkinlik ve düşük maliyet konularında başarılı olduğunu göstermektedir. Gelecekte, bu sistemin iletişim, güvenlik ve enerji tüketimi gibi alanlarda daha fazla optimize edilmesi planlanmaktadır.

3. MATERYAL VE YÖNTEM

Bu bölümde, blockchain kullanılarak şifrelenen paketleri ileten IoT ağlarının güvenliğini değerlendirmek için tez çalışmasında kullanılan araçlar ve metodolojilerden bahsedilecektir. Yaklaşım, blockchain platformu olan Hyperledger Fabric ile ağ benzetim aracı olan OPNET'i bir arada kullanmaktadır. Hyperledger Fabric, IoT ekosistemlerinde güvenli veri işlemlerini ve yönetimini göstermek için kullanılırken; OPNET, IoT altyapılarındaki ağ dinamiklerini ve potansiyel güvenlik açıklarını benzetimini sağlamaktadır. Bu araçlar ile birlikte, IoT güvenliğinde blockchain'in etkinliğini değerlendirmek için kapsamlı bir çerçeve oluşturmaktadır.

3.1. HYPERLEDGER FABRIC

Hyperledger Fabric, yüksek düzeyde gizlilik, güvenlik ve ölçeklenebilirlik sunarak işletmelerin özel ihtiyaçlarını karşılamak üzere tasarlanmış açık kaynaklı bir blockchain çerçevesidir. İzinsiz ağlarda çalışan Bitcoin ve Ethereum gibi halka açık blockchainlerin aksine, Hyperledger Fabric izinli bir model sunar; yani katılımcıların ağa katılmalarına izin verilmeden önce tanımlanmaları ve doğrulanmaları gerekir [77]. Bu kurulum, sağlık hizmetleri, finans ve tedarik zinciri yönetimi gibi sıkı yasal uyumluluk ve sağlam veri koruması gerektiren sektörler için özellikle yararlıdır. Çerçeve modülerdir ve farklı sektörlerin benzersiz gereksinimlerine göre uygulanmasında esneklik sağlar.

3.1.1. İzinli Ağ

Hyperledger Fabric'in tanımlayıcı özelliklerinden biri izinli ağ modelidir. Kimlik doğrulaması olmadan herkesin katılmasına izin veren halka açık blockchainlerin aksine Hyperledger Fabric, her katılımcının bir Üyelik Hizmeti Sağlayıcısı (MSP) aracılığıyla incelenmesini gerektirir [17]. MSP, her katılımcının kimliği olarak hizmet veren dijital sertifikalar vermekten sorumludur. Bu kimlik tabanlı yaklaşım, yalnızca güvenilir ve bilinen varlıkların ağ ile etkileşime girebilmesini sağlayarak hesap verebilirliğin çok önemli olduğu kurumsal kullanım durumları için idealdir [78].

İzinli model ayrıca işletmelerin daha sıkı erişim kontrol politikaları uygulamasına olanak tanır. İzinsiz bir ağda, herhangi bir katılımcı tüm işlem geçmişini görüntüleyebilir ve bu da hassas verilerle uğraşan kuruluşlar için zorluk teşkil eder. Buna karşılık Hyperledger Fabric, belirli verilere kimlerin erişebileceği üzerinde ayrıntılı kontrol sağlayarak Genel Veri Koruma Yönetmeliği (GDPR) gibi gizlilik düzenlemelerine uyumluluk sağlar [79]. Bu kurulum özellikle veri güvenliğinin çok önemli olduğu finans ve sağlık gibi sektörlerde kullanışlıdır. Ayrıca, ağın izinli yapısı, katılımcıların doğrulanabilir kimlikler altında çalışması gerektiğinden, hileli faaliyetlere karşı ekstra bir koruma katmanı sağlar [80]. İzinli ağlar ayrıca farklı kuruluşlar arasında daha yüksek derecede birlikte çalışabilirlik sağlar. Tüm katılımcılar incelendiğinden ve bilindiğinden, bir konsorsiyumdaki varlıklar arasında güven tesis etmek daha kolay hale gelir. Örneğin, bir tedarik zinciri ağında üreticiler, tedarikçiler ve lojistik sağlayıcılar, her bir kuruluşla ayrı ayrı güven ilişkileri geliştirmeye gerek kalmadan aynı blockchain ağına katılabilir. Bu, karmaşıklığı azaltır ve yüksek güvenlik standartlarını korurken iş birliğini teşvik eder [81].

3.1.2. Modüler Mimari

Hyperledger Fabric'in bir diğer özelliği de blockchain teknolojisini benimsemek isteyen işletmeler için önemli bir esneklik sunan modüler mimarisidir. Mimari, kuruluşların kendi özel ihtiyaçlarına bağlı olarak fikir birliği algoritmaları, kimlik yönetim sistemleri ve akıllı sözleşmeler gibi çeşitli bileşenler arasından seçim yaparak kendi blockchain ağlarını özelleştirmelerine olanak tanır [82]. Örneğin, kuruluşlar performans ve güvenlik ihtiyaçlarına göre farklı fikir birliği mekanizmaları seçebilir. Bazı işletmeler çökme hatasına toleranslı (CFT) fikir birliği mekanizmasını tercih ederek hız ve verimliliğe öncelik verebilirken, daha yüksek güvenlik gerektiren diğerleri daha sağlam bir Bizans hatasına toleranslı (BFT) protokolü seçebilir [83]. Bu esneklik Hyperledger Fabric'i finans, lojistik ve üretim gibi farklı gereksinimleri olan sektörler için cazip bir seçenek haline getirmektedir. Modülerlik, gizlilik özelliklerine de uzanır. Hyperledger Fabric, daha geniş blockchain ağı içinde yalnızca belirli katılımcıların erişebileceği kanallar-özel alt ağlar oluşturulmasına izin verir [84]. Bu, kuruluşların verilerini bölümlere ayırmasına olanak tanıyarak hassas bilgilerin yalnızca yetkili taraflarla paylaşılmasını sağlar. Örneğin, bir sağlık hizmetleri ağında, farklı hastaneler aynı blockchaine katılabilir, ancak her hastanenin hasta verilerinin güvenli bir şekilde depolandığı ve yalnızca yetkili personel tarafından erişilebildiği kendi kanalı olabilir [85].

3.1.3. Akıllı Sözleşmeler (Chaincode)

Hyperledger Fabric'teki Chaincode, Ethereum gibi diğer blockchain platformlarındaki akıllı sözleşmelerin eşdeğeridir. Bunlar, anlaşma koşullarının doğrudan koda yazıldığı ve önceden tanımlanmış koşullar karşılandığında işlemlerin otomatik olarak yürütülmesine izin veren kendi kendini yürüten sözleşmelerdir [10]. Hyperledger Fabric'te chaincode kullanımı son derece çok yönlüdür ve kuruluşların işlemlerin ağ üzerinde nasıl işleneceğini yöneten karmaşık iş kuralları tanımlamasına olanak tanır [10].

Chaincode'u diğer blockchainlerdeki akıllı sözleşmelerden ayıran şey, Solidity gibi alana özgü diller yerine Go, Java ve JavaScript gibi genel amaçlı programlama dillerinde yazılabilmesidir [86]. Bu özellik, geliştiriciler yeni beceriler öğrenmeye gerek kalmadan blockchain uygulamaları oluşturmak için yaygın olarak bilinen programlama dillerini kullanabildiğinden, işletmeler için benimseme engelini azaltır. Örneğin bir finans kurumu, belirli risk parametreleri karşılandığında fonları otomatik olarak dağıtan bir kredi onay sistemi oluşturmak için chaincode kullanabilir [38].

Chaincode ayrıca katılımcılar arasında güveni de kolaylaştırır. İzinli bir ağda, ilgili tüm taraflar aynı chaincode'a erişebilir ve doğrulayabilir, bu da şeffaflığı sağlar ve aracılara olan ihtiyacı azaltır. Bu özellikle üreticiler, tedarikçiler ve perakendeciler gibi birden fazla tarafın güvenini koruyarak işbirliği yapması gereken tedarik zinciri yönetiminde kullanışlıdır. Chaincode, tüm katılımcıların aynı verilere ve iş kurallarına erişmesini sağlayan ortak bir doğruluk kaynağı görevi yapar [87].

3.1.4. Veri Gizliliği

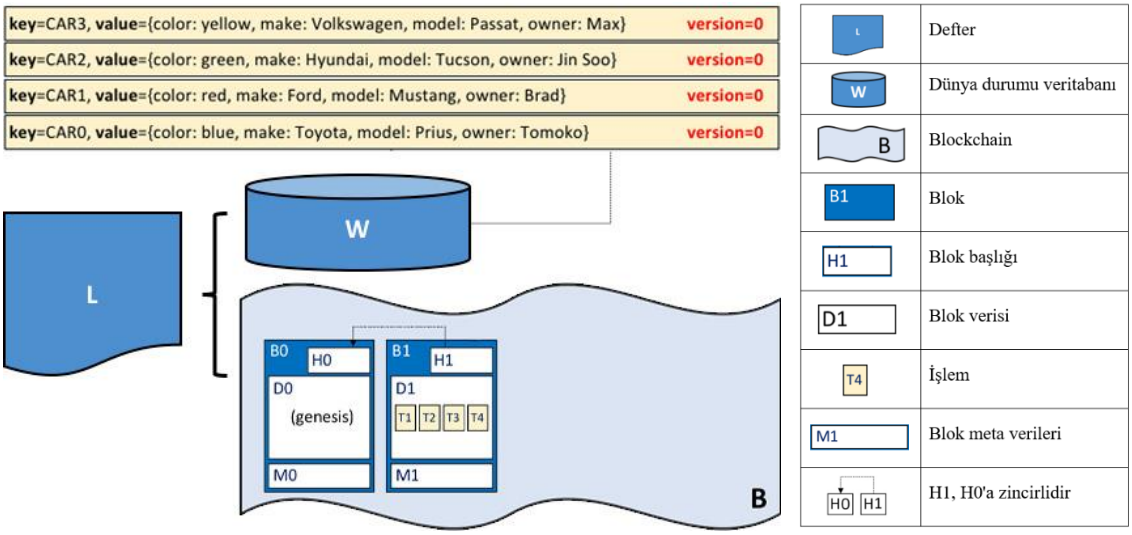
Veri gizliliği, Hyperledger Fabric'in kritik bir yönüdür ve onu hassas bilgileri işleyen endüstriler için uygun hale getirir. Hyperledger Fabric'te veri gizliliğini sağlamaya yönelik birincil mekanizmalardan biri kanalların kullanılmasıdır. Kanal, yalnızca yetkili katılımcıların verilere erişebildiği özel bir alt ağdır [88]. Bu, kuruluşların hassas verileri tüm blockchain ağına ifşa etmeden belirli taraflarla paylaşmasına olanak tanır; bu durum, hasta gizliliğinin yasal olarak zorunlu olduğu sağlık hizmetleri gibi sektörlerde özellikle önemli olan bir özelliktir [89].

Hyperledger Fabric, kanallara ek olarak Özel Veri Koleksiyonları (PDC'ler) adı verilen bir özellik de sunmaktadır. PDC'ler, kuruluşların hassas verileri zincir dışında depolamasına izin verirken, doğrulama amacıyla verilerin bir özetini zincir üzerinde tutar [90]. Bu, gerçek veriler gizli tutulurken diğer katılımcıların bilgilerin bütünlüğünü

doğrulamasına izin verdiği için ek bir güvenlik katmanı sağlar. Bu özellik, mevzuata uygunluğun sıkı veri koruma önlemleri gerektirdiği finans ve sigorta gibi sektörler için oldukça önemlidir [91].

3.1.5. Defter (Ledger)

Hyperledger Fabric ağın temel yapı taşları olan defter (Ledger), dünya durum veritabanı (World State Database) ve blockchain'in organize edildiği aşamalar Şekil 3.1'de göstermektedir.

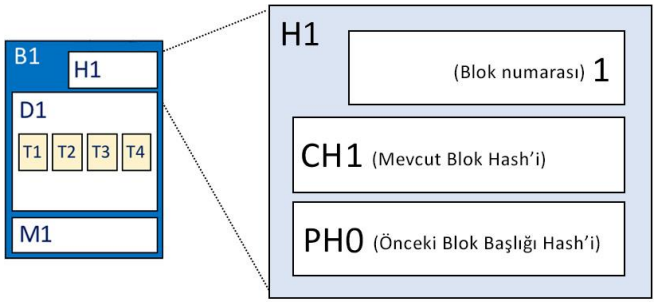


Şekil 3.1. Hyperledger Fabric'de defter ve blockchain yapısı [92]

Defter (L), iki ana bileşenden oluşmaktadır; bunlar blockchain ve dünya durum veritabanıdır [92]. Blockchain, gerçekleşen işlemlerin bloklar halinde kaydedildiği bir yapıdır [92]. Şekil 3.1'de gösterilen dünya durum veritabanı (W), her bloktaki işlemler sonucunda güncellenen mevcut varlık durumlarını tutar. Örneğin, arabaların renk, marka, model ve sahip bilgileri gibi varlık bilgileri dünya durum veri tabanında saklanır ve her işlemle bu bilgiler güncellenir.

Şekil 3.1'deki blockchain yapısında, birinci blok (B0) "genesis" olarak adlandırılır ve zincirin başlangıç bloğudur. Bloklar ardışık olarak eklenir ve her blok, blok başlığı, blok verisi ve blok meta verilerinden oluşur. Blok başlığı, Şekil 3.2'de gösterildiği gibi bir önceki bloğa referans verir. Blok başlığı üç bileşenden oluşur; blok numarası, mevcut blok hash'i ve önceki blok başlığı hash'i. Blok numarası, 0'dan (genesis bloğu) başlayarak, blockchain'e eklenen her yeni blok için 1 artan bir tamsayıdır. Mevcut blok hash'i, mevcut blokta yer alan tüm işlemlerin hash'idir ve blok içeriğinin bütünlüğünü

sağlar. Önceki blok başlığı hash'i ise bir önceki blok başlığının hash'ini gösterir. Bu alanlar, blok verilerini kriptografik olarak hash'leyerek dâhili olarak türetilir. Böylece her blok, komşusuna ayrılmaz bir şekilde bağlı hale gelir ve değiştirilemez bir defter oluşturur [92].



Şekil 3.2. Blok başlığı yapısı [92]

Blok verisi (D1), sırayla dizilmiş işlemlerin bir listesini içerir. Blok meta verileri ise, bir bloktaki işlemlerle ilgili ek bilgiler içerir. Örneğin, bloğun oluşturma zamanı, hangi işlemlerin geçerli olup olmadığı ve işlemler için kullanılan imzaların detayları gibi veriler blok meta verilerinde yer alır. Bu meta veriler, bloktaki işlemlerin düzgün bir şekilde işlendiğini ve blok zincirine doğru bir şekilde eklendiğini doğrulamak için kullanılır [92].

Bu yapı, her yeni işlem gerçekleştiğinde blokların sıralı bir şekilde blockchain'e eklenmesini sağlar ve aynı zamanda dünya durum veritabanı da güncellenerek mevcut varlıkların son halini yansıtır. Blockchain yapısının ardışık ve değiştirilemez yapısı, ağın güvenliğini sağlar ve işlemlerin şeffaf ve izlenebilir olmasına olanak tanır. Defterin kopyası, Şekil 4.2'de gösterildiği gibi her bir "committing peer" üzerinde saklanır. Bu, ağdaki her bir düğümün defterin tam bir kaydına sahip olmasını sağlar ve bu şekilde ağın bütünlüğü ve güvenliği korunur.

3.2. OPNET

OPNET, iletişim ağlarının, protokollerinin ve cihazlarının performansını modellemek ve analiz etmek için kullanılan güçlü bir benzetim aracıdır. İlk olarak MIL 3, Inc. tarafından geliştirilen ve daha sonra Riverbed Technology tarafından satın alınan OPNET [93], kullanıcıların çeşitli ağ yapılandırmalarını test etmelerine, trafik yüklerinin benzetimini gerçekleştirmeye ve farklı ağ protokollerini gerçek dünya ortamlarına dağıtmadan önce etkilerini değerlendirmelerine imkan tanır [94].

OPNET, araştırmacıların yönlendiriciler, anahtarlar, sunucular ve mobil cihazlar olmak üzere önceden tanımlanmış ağ bileşenlerinden oluşan kapsamlı kütüphanesini kullanarak ayrıntılı ağ modelleri oluşturmalarını sağlar. Bu modeller, Yerel Alan Ağları (LAN), Geniş Alan Ağları (WAN) ve kablosuz ağlar gibi çok çeşitli ağ türlerini benzetimini gerçekleştirebilir ve kullanıcıların farklı ağ kurmalarını ile gecikme, verim ve paket kaybı gibi performans ölçümlerini değerlendirmelerine olanak sağlar [95].

OPNET'in temel özelliklerinden biri, gerçek dünya trafik modellerinin benzetimlerini sağlamak ve farklı ağ yapılandırmalarının çeşitli yükler altında nasıl performans gösterdiğini analiz etmektir. Özellikle yüksek trafik senaryolarında veya ağ kaynaklarının sınırlı olduğu ortamlarda ağ performansını optimize etmek için kullanışlıdır. OPNET, TCP/IP, UDP ve çeşitli kablosuz iletişim standartları gibi ağ protokollerinin performansını incelemek için akademik ve endüstriyel araştırmalarda yaygın olarak kullanılmaktadır [95]. Yazılım, araştırmacıların farklı protokol yapılandırılmasını sağlamak ve değişikliklerin genel ağ performansını nasıl etkilediğini ölçmelerine olanak tanır. Özellikle sinyal paraziti, bant genişliği sınırlamaları ve cihaz hareketliliğinin ağ verimliliğini önemli ölçüde etkileyebildiği kablosuz ağlarda önemlidir. Bu değişkenleri OPNET benzetim aracında tanımlayarak, araştırmacılar gerçek dünya dağıtımlarında performansı artırmak için ağ parametrelerini optimize edebilirler [95].

Ayrıca OPNET, benzetim sonuçlarını analiz etmek için güçlü araçlar sağlar. Kullanıcıların ağ performansını gerçek zamanlı olarak izlemelerine olanak tanıyan ayrıntılı raporlar ve görselleştirmeler oluşturur. Bu raporlar, farklı ağ yapılandırmalarının ve protokollerinin etkinliğini değerlendirmek için gerekli olan paket teslim oranı, uçtan uca gecikme, titreşim ve verim gibi metrikleri içerir [95]. Ağ performansını bu şekilde görselleştirme yeteneği, potansiyel sorunları belirlemeyi ve ağ tasarımını optimize etmeyi kolaylaştırır.

Geleneksel kablolu ve kablosuz ağlara ek olarak OPNET, Nesnelerin İnterneti (IoT) gibi gelişmekte olan teknolojilerin de benzetimini sağlamaktadır. IoT ağları, farklı protokoller üzerinden iletişim sağlayan çok sayıda bağlı cihazladır ve OPNET bu sistemleri modellemek ve çeşitli koşullar altında performanslarını test etmek için de kullanılır. Bu yetenek, performans veya güvenilirlikten ödün vermeden büyük hacimli verileri işleyebilen ölçeklenebilir IoT ağları geliştirmek için oldukça önemlidir [96].

OPNET'in bir diğer önemli uygulaması da Hizmet Kalitesi (QoS) yönetimidir. OPNET, kullanıcıların farklı QoS politikalarının benzetimini gerçekleştirmesini ve bunların ağ performansı üzerindeki etkilerini ölçmelerine olanak tanır. Özellikle video akışı ve VoIP gibi belirli trafik türlerinin diğer veri türlerinden daha yüksek öncelik gerektirdiği ortamlarda önemlidir. Ağ yöneticileri, OPNET'te QoS politikaları, kritik trafiğin yüksek kaliteli hizmet seviyelerini korumak ve gerekli kaynakları almasını sağlamak için yapılandırmalarında daha detaylı çalışabilirler [97].

4. DENEYSEL ÇALIŞMA

Bu bölümde, Hyperledger Fabric ağı başarıyla çalıştırılmış ve ardından Postman aracılığıyla etkileşimler gerçekleştirilmiştir. Bir kullanıcı kaydedilmiş ve ilgili token (anahtar) elde edilmiştir. Bu token kullanılarak, her biri benzersiz bir işlem kimliği oluşturan araç kayıtları blockchain'e eklenmiştir.

Bu süreci bir IoT ortamda benzetimini gerçekleştirmek için Şekil 4.1'de görüldüğü üzere blockchain paketlerinin boyutunu OPNET'in paket boyutu ayarlama özelliği kullanılarak temsil edilmiştir. Bu işlem daha önce literatürde [98] [99] ve [100] çalışmalarında gerçekleştirilmiştir. Bu varsayım literatürde, yaklaşık 2500 byte olan ortalama paket boyutuna dayanmaktadır [98]. Bu boyut OPNET'in paket boyutu özelliğine yansıtılarak benzetilen blockchain paket iletimleriyle tutarlılık sağlanmıştır. Belirli parametreler ayarlanarak, farklı ağ koşulları benzetilerek dört farklı senaryo gerçekleştirilmiş ve sonuçlar karşılaştırılmıştır.

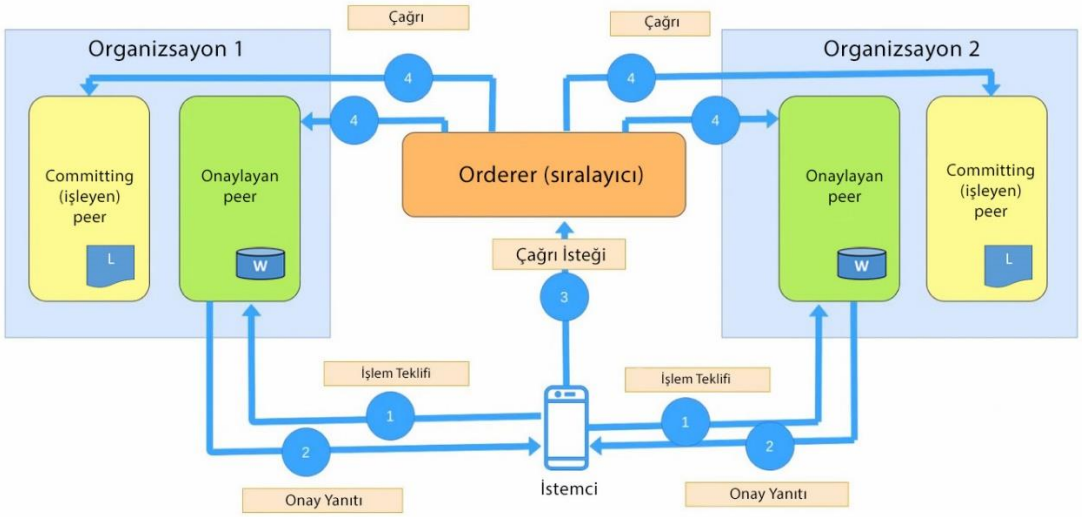
Şekil 4.1 IoT-Blockchain ortamı

4.1. HYPERLEDGER FABRIC İLE AĞ KURULUMU VE VERİ İŞLEMLERİ

Öncelikle bir Hyperledger Fabric ağının kurulumu ve veri işlemleri gerçekleştirildi. Organizasyonlar, peer'lar ve orderer dâhil olmak üzere çeşitli bileşenlerin rollerini ve etkileşimlerini vurgulayarak ağ mimarisinin bir taslağı oluşturuldu. Daha sonra, kullanıcı kaydı, kanal oluşturma, yönetimi, chaincode dağıtımı ve çağırma gibi kritik işlemler için belirli API'lerin kullanımı vurgulanarak istemci tarafından veri işlemlerinin uygulanması gözlemlendi. Fabcar.go kodu, örnek araç/araba kayıtlarının eklenmesini ve bu kayıtlar üzerinde işlem yapılmasını sağlayarak blockchain ağıyla nasıl etkileşim kurulabileceğini gösteren bir uygulama olarak hizmet vermektedir.

4.1.1. Ağ Mimarisi ve Bileşenleri

Hyperledger Fabric ağı içindeki bir işlemin onaylanıp blockchain'e eklenmesi ve mevcut blockchain'e yeni blokların eklenme süreci Şekil 4.2'de gösterilmektedir [101]. Şekil 4.2'de gösterilen ağ diyagramı, iki organizasyon, her birinin sahip olduğu peer'lar ve fikir birliği sürecinde kritik rol oynayan orderer (sıralayıcı) arasındaki etkileşimi göstermektedir.



Şekil 4.2. Hyperledger Fabric'de işlem akışı [101]

4.1.1.1. Organizasyonlar

Hyperledger Fabric ağında, organizasyonlar, blockchain ağına katılan bağımsız varlıkları temsil eder. Her organizasyon, işlemleri doğrulamak ve onaylamakla sorumlu olan kendi peer'larını işletir.

4.1.1.2. Peer

- Onaylayan Peer: Bu özel peer'lar, işlem tekliflerini gösterir ve onaylar. Bir istemci işlem teklifi sunduğunda, onaylayan peer'lar, dünya durum veri tabanına (W) erişerek chaincode'u çalıştırır ve işlemi gösterir. Ardından, bir onay yanıtı üretirler. Bu yanıt, benzetim sonuçlarını ve bir imzayı içerir. Onay yanıtı, işlemin geçerliliği için kritiktir ve ağın onay politikasıyla uyumlu olmalıdır. Onaylayan peer'lar tam bir defter tutmazlar; sadece mevcut dünya durum veri tabanını kullanarak işlemleri değerlendirirler.
- Committing Peer: Committing peer'lar, orderer'dan alınan onaylanmış işlemleri doğrulamak ve blockchain defterine (L) işlemekten sorumludur. İşlemler

doğrulandıktan sonra, deftere kaydedilir ve dünya durumu veritabanı buna göre güncellenir. Committing peer'lar işlemleri göstermez; bunun yerine, ağın bütünlüğünü korumak ve güncel bir defter sağlamak amacıyla doğrulama ve kayıt işlemlerini gerçekleştirirler.

4.1.1.3. İstemci

İstemci, ağda işlem sürecini başlatan varlıktır. İşlem teklifini ağın onaylayan peer'larına gönderir. Gerekli onayları topladıktan sonra, işlem isteğini orderer'a iletir.

4.1.1.4. İşlem Akışları

- İşlem Teklifi: İstemci, işlem teklifini onaylayan peer'lara gönderir.
- Onay Yanıtı: Onaylayan peer'lar, işlem teklifini çalıştırır, bir onay yanıtı oluşturur ve istemciye geri gönderir.
- Invocation Request (Çağrı İsteği): İstemci, gerekli onayları toplar ve orderer'a bir çağrı isteği gönderir.
- Sıralama ve Onaylama: Orderer, işlemleri sıralar, bloklar oluşturur ve bunları committing peer'lara dağıtır. Committing peer'lar, işlemleri doğrular ve deftere işler, dünya durumunu buna göre günceller.

4.1.1.5. Orderer (Sıralayıcı)

Orderer, blockchain'in tutarlılığını sağlamada kritik bir rol oynar. Onaylanmış işlemleri toplar, bloklar halinde sıralar ve bu blokları committing peer'lara dağıtır. Orderer, tüm peer'ların aynı işlem sırasını almasını sağlayarak ağın bütünlüğünü korur.

4.1.1.6. Fikir Birliği Mekanizması

Raft fikir birliği algoritması, Hyperledger Fabric'de kullanılan birincil fikir birliği mekanizmasıdır. Raft, deterministik işlem sıralaması sağlayan bir çökme hata toleranslı (CFT) fikir birliği protokolüdür. Byzantine Hata Tolerant (BFT) algoritmalarından farklı olarak, Raft, katılımcıların genellikle güvenilir olduğu senaryolara odaklanır. Orderer'lar arasında bir lider seçerek işlem sıralama sürecini yönetir. Liderin başarısız olması durumunda, yeni bir lider otomatik olarak seçilir, bu da kesinti olmadan sürekli bir çalışma sağlar.

4.1.2. Blockchain Ağının Çalışma Mekanizması

Hyperledger Fabric ağını başlatmak için, birden fazla Docker konteynerini yönetmeye yardımcı olan Docker Compose'dan yararlanan bir komut kullanılır. Bu konteynerler, Fabric ağının peer'lar ve orderer gibi farklı bileşenlerini temsil eder ve bunların tümü bir YAML yapılandırma dosyasında tanımlanır.

4.1.3. Kanal Oluşturma

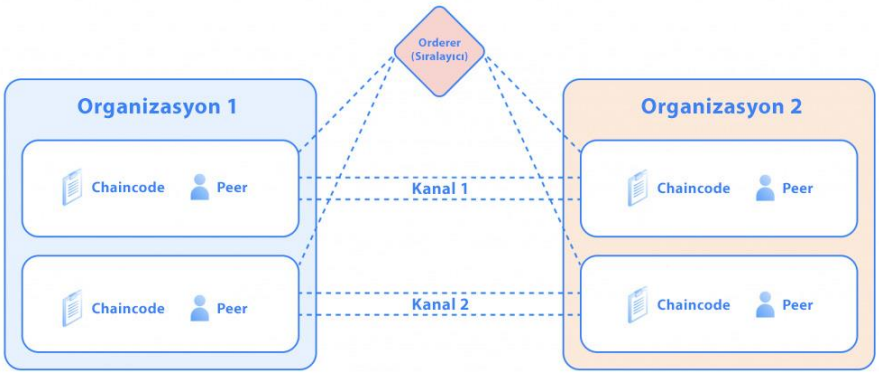
Ağ içinde bir iletişim kanalı oluşturmak için bir komut dosyası kullanılır. Kanallar, belirli katılımcıların özel olarak iletişim kurmasına ve işlem yapmasına izin vererek veri gizliliği ve ayrımı sağlar. Kanalın yapılandırması tanımlandıktan sonra oluşturulur ve farklı kuruluşlardan peer'lara katılmaları talimatı verilir.

Şekil 4.3'te organizasyonlar arasında Kanal 1 ve Kanal 2 olmak üzere iki ayrı kanal bulunmaktadır. Bu kanallar, belirli organizasyonların güvenli ve özel bir şekilde iletişim kurmasına olanak tanır.

4.1.4. Chaincode'u Dağıtma

Kanal kurulduktan sonra, Şekil 4.3'te görüldüğü üzere ağdaki bütün peer'lara chaincode'u dağıtılır. Chaincode, Go veya JavaScript gibi dillerde yazılır ve işlemlerin nasıl ele alınacağını yönetir. Süreç, chaincode'un paketlenmesini, peer'lara yüklenmesini ve ilgili tüm kuruluşlardan onay alınmasını içerir. Onaydan sonra chaincode aktif hale gelir ve ağ işlemlerini yönetir.

Her adım ağın, kanalların ve akıllı sözleşmelerin doğru şekilde yapılandırılmasını ve güvenli ve verimli bir şekilde etkileşime girebilmesini sağlar.



Şekil 4.3. Kanallar ve chaincode [102]

4.1.5. Sisteme Yeni Bir Blok Ekleme

Örnek olarak araba isimli bir blok kullanılmıştır, ancak bu işlem herhangi bir varlık kaydı için de uygulanabilir. Şekil 4.5'te, araba isimli blok örnek olarak gösterilmiştir, kaydedilecek veri türü sisteme veya kullanıcıya göre değişebilir.

4.1.5.1. Kullanıcı Kaydı ve Token Verme

İstemciler, /users API endpoint aracılığıyla kullanıcıları kaydedebilir. Bu işlem, bir kullanıcı adı ve organizasyon adı sağlamayı gerektirir. Başarılı bir kayıt işleminin ardından sistem, istemciye bir JSON Web Token (JWT) verir (bkz. Şekil 4.4). Bu token kimlik doğrulama, kanal yönetimi ve chaincode etkileşimleri gibi diğer hassas işlemleri gerçekleştirmek için gereklidir.


```
{
"username": "Selami",
"orgName":"Org1"
}
============================
"message": "Selami enrolled Successfully",
"token": "eyJhbGci0iJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MjQw
MjQzNzksInVzZXJuYW1lIjoiU2VsYW1pIiwib3JnTmFtZSI6Ik9yZzEiLCJpYX
QiOjE3MjM500gzNz1.vQGKB3n6c8cs9IKHW2RPhBzmq6HgXP2b19iLD1Z480"
```


Şekil 4.4. Kullanıcı oluşturma ve JWT elde etme

4.1.5.2. Örnek Blok Oluşturma

Bu işlev, defterde bir örnek olarak "araba" isimli blok için benzersiz bir ID oluşturarak başlar. Bu örnek, özellikle araç bilgileriyle ilgili bir işlemi temsil eder. Fabcar.go chaincode'u kullanılarak, her bir araç için belirli veriler (marka, model, renk ve sahibi) bir blok içinde kaydedilir.

İlk adımda, istemci uygulaması, Hyperledger Fabric ağına bir işlem teklifi gönderir. Bu işlem, belirli bir araç verisi için bir blok oluşturma talebini içerir. Peer düğümleri bu teklifi onaylar ve işlem sıralayıcıya (orderer) iletilir. Orderer, onaylanan işlemi diğer işlemlerle birleştirir ve zincire yeni bir blok ekler.

Şekil 4.5. "Araba" kaydı oluşturma

4.2. OPNET İLE AĞ BENZETİMİ

Bu bölümde, bir blockchain ortamını yansıtan ZigBee tabanlı bir IoT ağının benzetimi ayrıntılı olarak açıklanmaktadır.

4.2.1. Kullanılan Parametreler

Benzetim senaryolarında, veri paketlerinin güvenilirliğini artırmak amacıyla literatürdeki birçok çalışmada [103] ACK mekanizması etkinleştirildiği için bu çalışmada da aynı şekilde yapılmıştır. Ayrıca, benzetim zamanı da birçok çalışmada [104] 15 dakika sürdüğü için bu çalışmada da aynı şekilde ayarlanmıştır.

4.2.2. Performans Metrikleri

Performansı değerlendirmek için seçilen metrikler şu şekildedir;

- Uçtan Uca Gecikme (sn): Bir veri paketinin kaynak cihazdan hedefe ağ üzerinden geçmesi için geçen toplam süreyi yakalar. Genellikle hızlı yanıt sürelerinin gerekli olduğu IoT uygulamalarında veri teslimatının zamanında yapılıp yapılmadığını değerlendirmek için oldukça önemlidir [103].
- Gönderilen Veri Trafiği (bit/sn): Verilerin bir cihazdan saniye başına bit cinsinden iletilme hızını ölçer. Bu metriğin izlenmesi, ağ üzerinden ne kadar veri gönderildiğini anlamak için gereklidir. Bu sayede, ağ verimliliği ve kapasite kullanımı anlaşılmaktadır [105].
- Alınan Veri Trafiği (bit/sn): ZigBee cihazları tarafından saniyede ne kadar verinin başarıyla alındığını gösterir. Ağ güvenilirliğini ve paket teslim başarısını değerlendirmeye yardımcı olur [105].

- Verim (bit/sn): Verim, ağ üzerinden başarılı veri iletiminin gerçek oranıdır. Ağın ne kadar verimli kullanıldığını temsil eder. Verim, ağın yük altında veri iletimini ne kadar iyi idare ettiğini yansıttığı için ağ performansının temel bir göstergesidir [105].

4.3. GERÇEKLEŞTİRİLEN SENARYOLAR

Senaryolar, blockchain kullanılarak şifrelenen paketleri ileten IoT ağlarının güvenliği ve belirlenen bazı durumların performansını değerlendirmek amacıyla seçilmiştir.

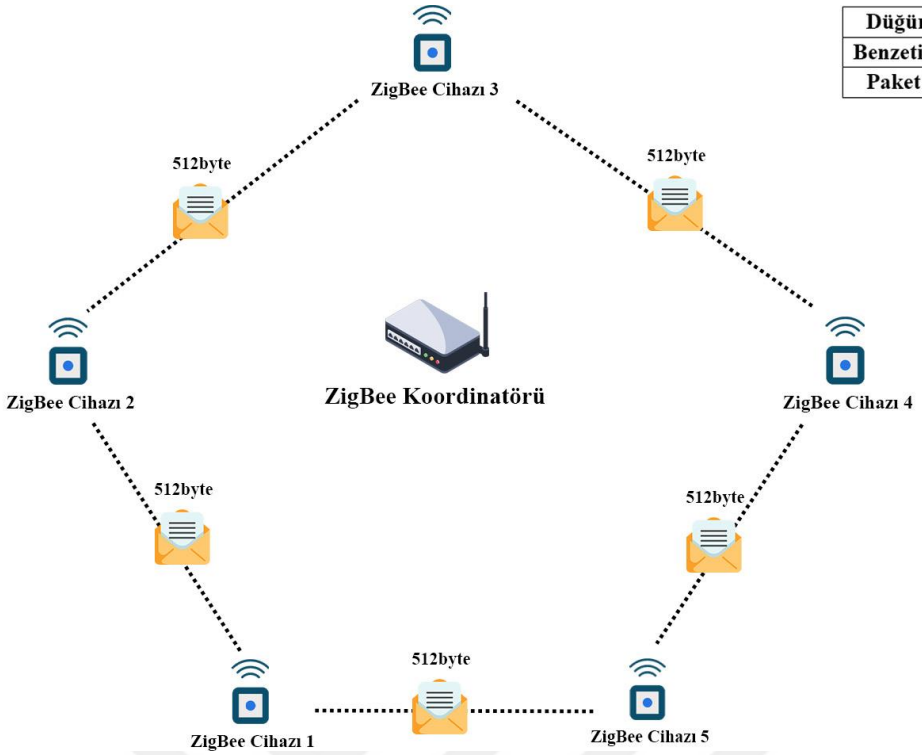
Senaryolarda karşılaştırma işlemleri için paketler, blockchain kullanılmadan doğrudan ve blockchain kullanılarak şifrelenip iletilerek yapılmıştır. Blockchain kullanılarak şifrelendiği varsayılan paketlerin boyutu önceki çalışmalardan [98] elde edilen bilgilere dayanarak 2500byte olarak ayarlanmıştır. Blockchain kullanılmadan iletilen paketlerin boyutu ise standart kablosuz ağlarda paket boyutu olan 512byte olarak ayarlanmıştır [106].

Senaryolar bölümünde; blockchain kullanılmadan paketleri ileten ağ yapısına “standart” ve blockchain kullanılarak şifrelenen paketleri ileten ağ yapısına ise “blockchain kullanılarak” ifade edilmiştir.

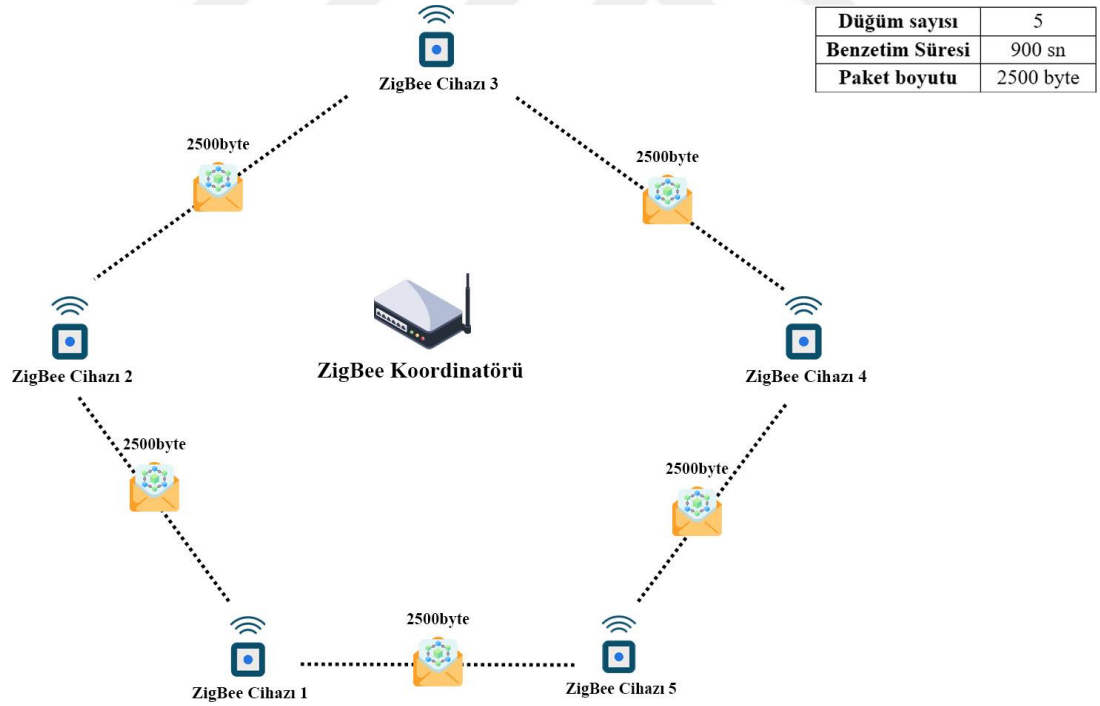
4.3.1. Senaryo 1 ve Senaryo 2

Senaryo 1 ve 2’de, OPNET kullanılarak beş uç cihaz ve bir merkezi ZigBee koordinatörü olmak üzere altı cihaz Şekil 4.6 ve Şekil 4.7’de görüldüğü gibi konumlandırılmıştır. Cihaz sayısı seçimi, [107] ve [108] çalışmalardan yola çıkılarak beş olarak belirlenmiştir. Çünkü bu bölümde düşük cihaz yoğunluğunda ağın performansını test etmek amacıyla seçilmiştir.

Senaryo 1’de paketler herhangi bir işlem yapılmadan doğrudan kablosuz ağ üzerinde iletimi sağlanmaktadır ancak senaryo 2’de paketler blockchain kullanılarak şifrelendikten sonra iletilmektedir.

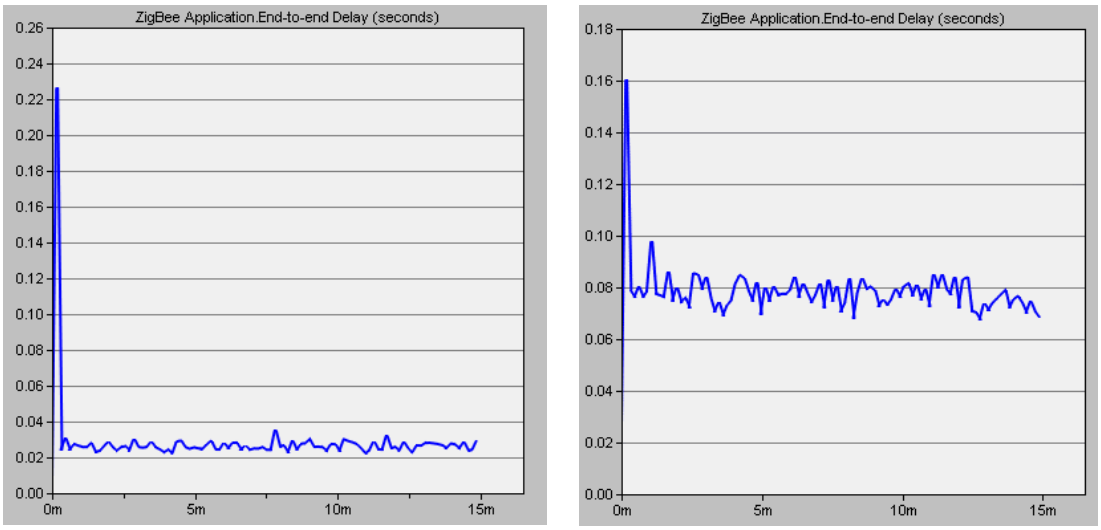


Şekil 4.6. Senaryo 1'in topolojisi



Şekil 4.7. Senaryo 2'nin topolojisi

Şekil 4.8'de görüldüğü üzere, senaryo 1'de uçtan uca gecikme 0.02 ile 0.04 saniye arasında iken, senaryo 2'de bu değer 0.07 ile 0.10 saniye arasında değişmektedir.

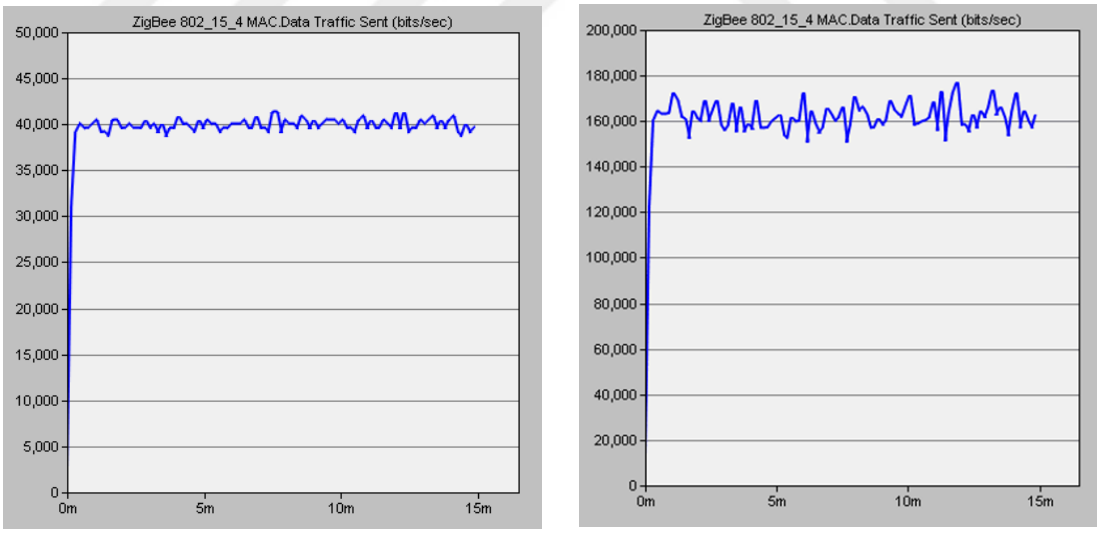


(a) (b)

Şekil 4.8. Uçtan uca gecikme

(a) Senaryo 1 – "standart" (b) Senaryo 2 – "blockchain kullanılarak"

Şekil 4.9'da görüldüğü üzere, gönderilen veri trafiği senaryo 1'de 39.000 bit/sn ile 42.000 bit/sn arasında değişiklik göstermektedir. Senaryo 2'de ise bu değerler, 150.000 ile 180.000 bit/sn arasında değişmektedir.

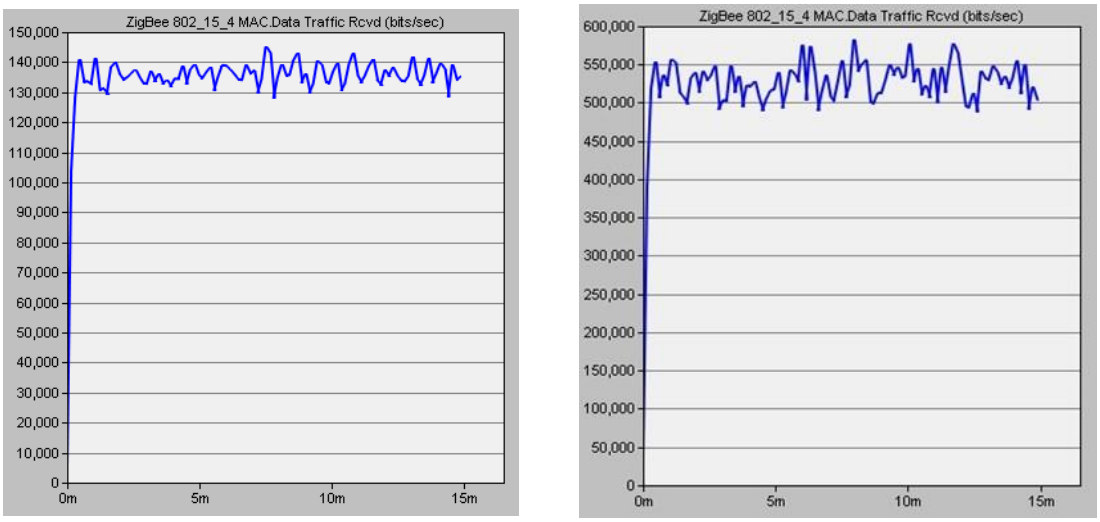


(a) (b)

Şekil 4.9. Gönderilen veri trafiği

(a) Senaryo 1 – "standart" (b) Senaryo 2 – "blockchain kullanılarak"

Şekil 4.10'da görüldüğü üzere, alınan veri trafiği senaryo 1'de 130.000 bit/sn ile 145.000 bit/sn arasında değişmektedir. Senaryo 2'de ise alınan veri trafiği, 500.000 bit/sn ile 600.000 bit/sn arasında değişiklik göstermektedir.

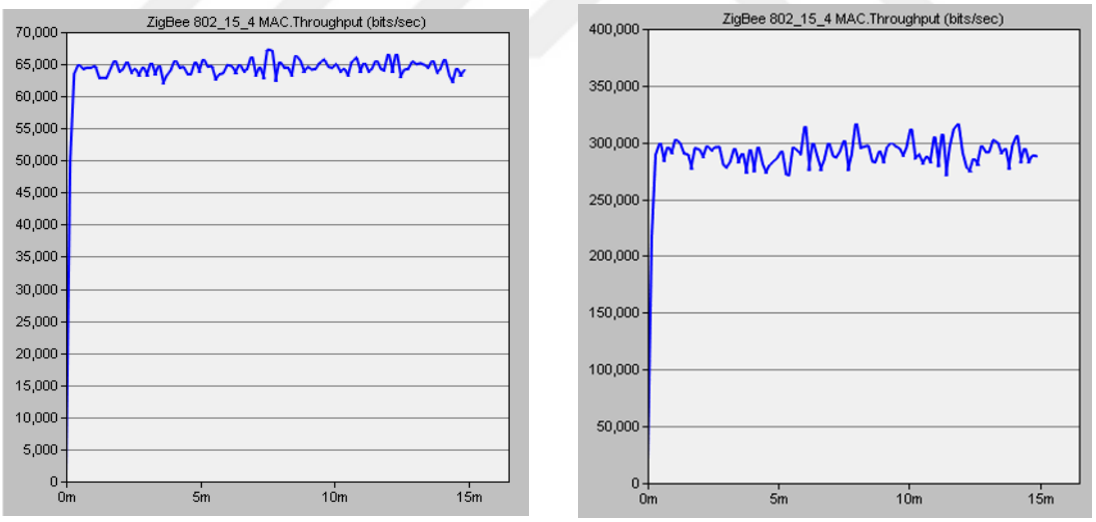


(a) (b)

Şekil 4.10. Alınan veri trafiği

(a) Senaryo 1 – "standart" (b) Senaryo 2 – "blockchain kullanılarak"

Şekil 4.11'de görüldüğü üzere, verim senaryo 1'de 63.000 bit/sn ile 68.000 bit/sn arasında değişim göstermektedir. Senaryo 2'de ise verim, 270.000 ile 320.000 bit/sn arasında dalgalanmaktadır.



(a) (b)

Şekil 4.11. Verim

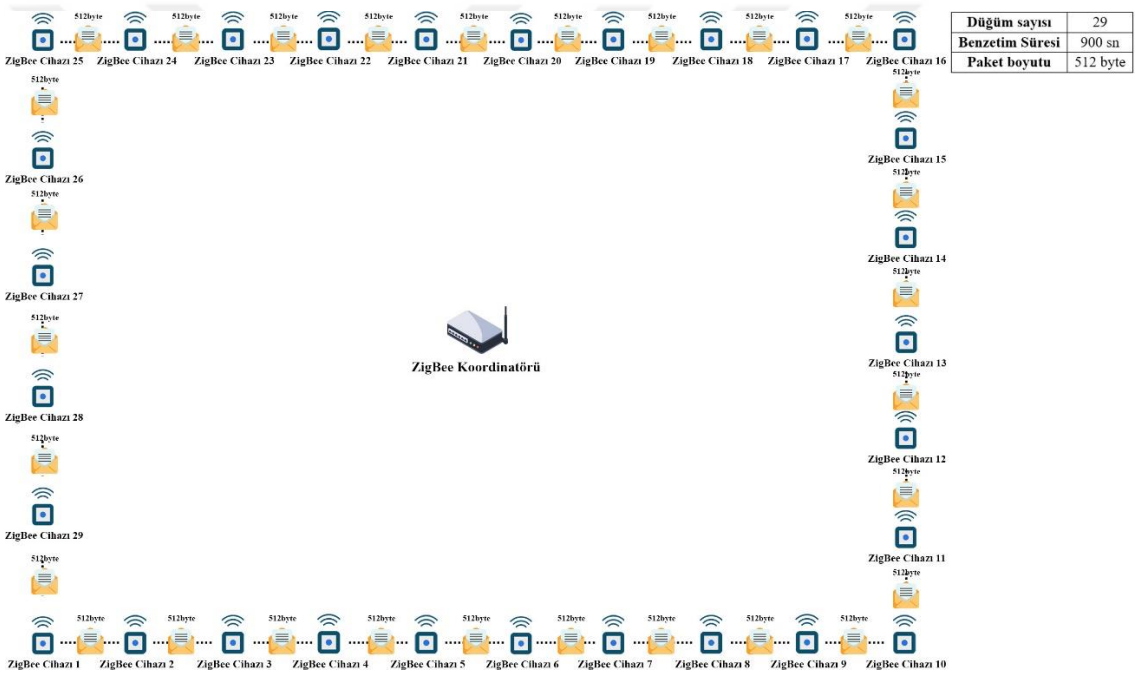
(a) Senaryo 1 – "standart" (b) Senaryo 2 – "blockchain kullanılarak"

4.3.2. Senaryo 3 ve Senaryo 4

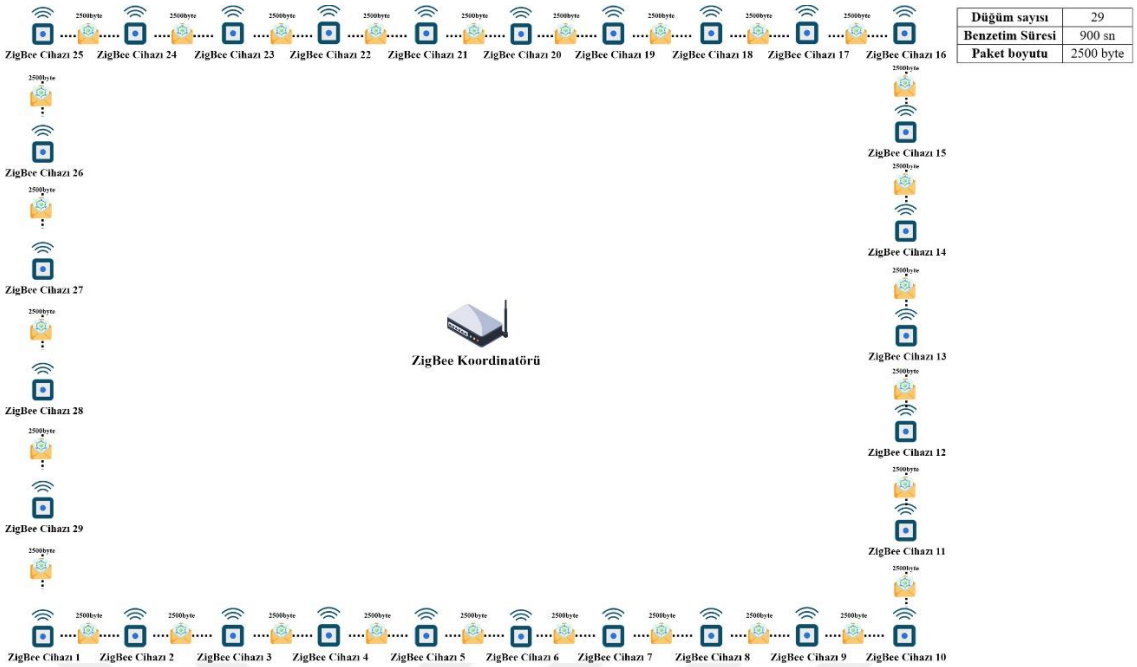
Senaryo 3 ve 4'te, Şekil 4.12 ve Şekil 4.13'te görüldüğü gibi ağ karmaşıklığı 24 cihaz daha eklenerek artırılmış, toplam 29'a çıkarılmış. Cihaz sayısı seçimi, [107] ve [108] çalışmalardan yola çıkılarak 29 olarak belirlenmiştir. Çünkü bu bölümde orta cihaz yoğunluğunda ağın performansını test etmek amacıyla seçilmiştir.

Senaryo 3'te paketler herhangi bir işlem yapılmadan doğrudan kablosuz ağ üzerinde iletimi sağlanmaktadır, ancak senaryo 4'te paketler blockchain kullanılarak şifrelendikten sonra iletilmektedir.

Bu senaryolarda, paket boyutu ilk iki senaryoda olduğu gibi blockchain kullanılarak şifrelenen paketlerde 2500byte, standart paketlere ise 512byte olarak ayarlanmıştır.

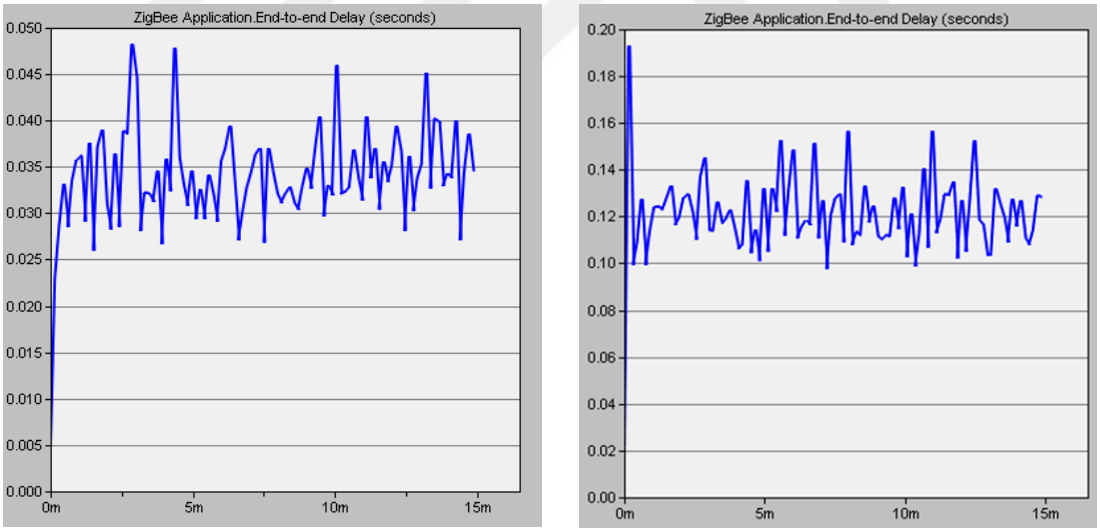


Şekil 4.12. Senaryo 3'ün topolojisi



Şekil 4.13. Senaryo 4'ün topolojisi

Şekil 4.14'te görüldüğü üzere, uçtan uca gecikme senaryo 3'te 0.026 ile 0.048 saniye arasında dalgalanmaktadır. Senaryo 4'te ise 0.10 ile 0.16 saniye arasında değişmektedir.

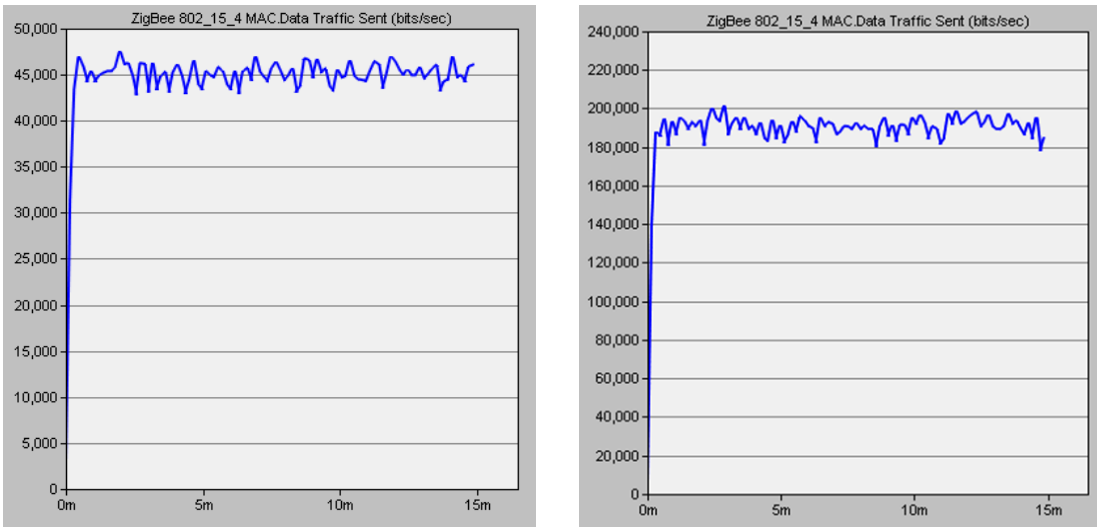


(a) (b)

Şekil 4.14. Uçtan uca gecikme

(a) Senaryo 3 – "standart" (b) Senaryo 4 – "blockchain kullanılarak"

Şekil 4.15'te görüldüğü üzere, gönderilen veri trafiği senaryo 3'te 43.000 bit/sn ile 47.000 bit/sn arasında değişim göstermektedir. Senaryo 4'te ise bu değer, 180.000 ile 200.000 bit/sn arasında değişiklik göstermektedir.

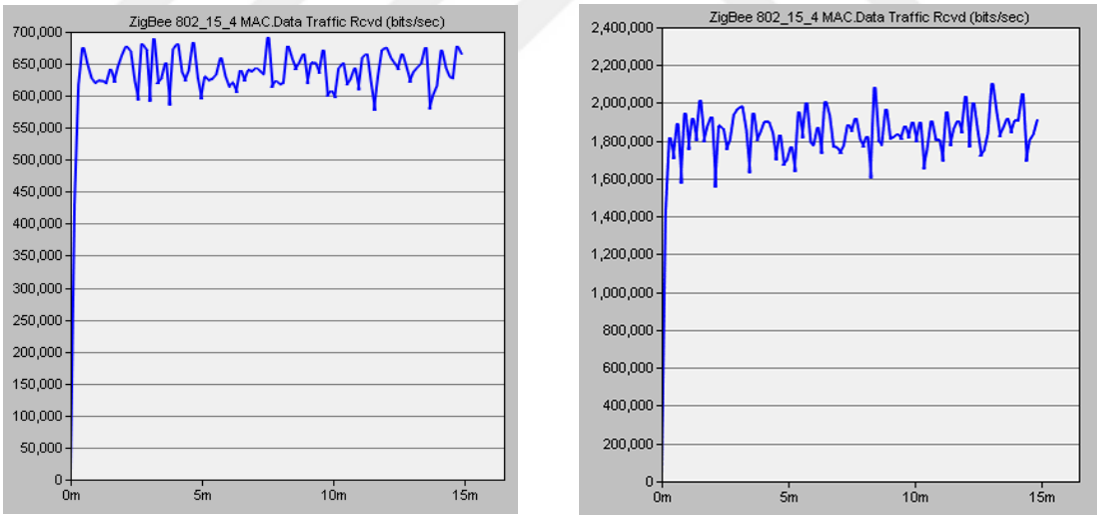


(a) (b)

Şekil 4.15. Gönderilen veri trafiği

(a) Senaryo 3 – "standart" (b) Senaryo 4 – "blockchain kullanılarak"

Şekil 4.16'da anlaşıldığı üzere, alınan veri trafiği senaryo 3'te 560.000 bit/sn ile 700.000 bit/sn arasında değişim göstermektedir. Senaryo 4'te ise bu değer, 1.600.000 bit/sn ile 2.100.000 bit/sn arasında seyretmektedir.

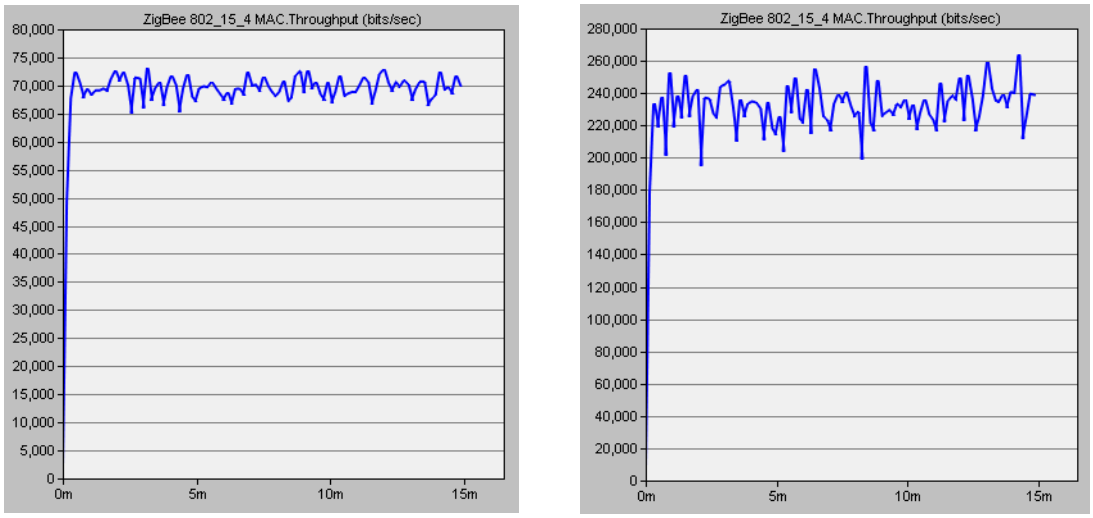


(a) (b)

Şekil 4.16. Alınan veri trafiği

(a) Senaryo 3 – "standart" (b) Senaryo 4 – "blockchain kullanılarak"

Şekil 4.17'de görüldüğü üzere, verim senaryo 3'te 65.000 bit/sn ile 73.000 bit/sn arasında değişim göstermektedir. Senaryo 4'te ise verim, 200.000 bit/sn ile 260.000 bit/sn arasında seyretmektedir.



(a) (b)

Şekil 4.17. Verim

(a) Senaryo 3 – "standart" (b) Senaryo 4 – "blockchain kullanılarak"

4.4. PERFORMANS DEĞERLENDİRMESİ

Senaryoların temel amacı, blockchain kullanılmadan doğrudan ve blockchain kullanılarak şifrelenip iletilen paketlerin IoT ağlarda güvenlik ve performans açısından karşılaştırılmasını sağlamaktır. Blockchain, yapısı gereği güvenli bir sistem sunmaktadır [44]. Verilerin güvenliği, bütünlüğü ve gizliliği blockchain tarafından güvence altına alınmaktadır. Ancak bu güvenlik özellikleri, ağın performansında bazı ek yükler oluşturmaktadır.

Gerçekleştirilen ilk iki senaryoda, blockchain kullanılarak şifrelenen paketleri ileten ağ, blockchain kullanılmadan paketleri ileten ağ ile az sayıda cihaz kullanılarak karşılaştırılmıştır. İlk senaryoda, blockchain kullanılmadan paketleri ileten ağlarda uçtan uca gecikme, gönderilen ve alınan veri trafiği ile verim daha yüksek performans göstermiştir. Örneğin, uçtan uca gecikme senaryo 1'de 0.02 ile 0.04 saniye arasında değişirken, senaryo 2'de blockchain kullanılarak şifrelenen paketleri ileten ağlarda bu değer 0.07 ile 0.10 saniye arasında dalgalanmıştır. Aynı şekilde, gönderilen veri trafiği senaryo 1'de 39.000 bit/sn ile 42.000 bit/sn arasında iken, senaryo 2'de 150.000 ile 180.000 bit/sn arasında değişmiştir.

Senaryo 3 ve 4'te cihaz sayısı arttırılmış ve toplamda 29 cihaz ile testler gerçekleştirilmiştir. Senaryo 3'te, blockchain kullanılmadan paketleri ileten ağlarda uçtan

uca gecikme 0.026 ile 0.048 saniye arasında iken, Senaryo 4'te blockchain kullanılarak şifrelenen paketleri ileten ağlarda gecikme 0.10 ile 0.16 saniye arasında gözlemlenmiştir. Gönderilen ve alınan veri trafiği, daha fazla cihaz ile birlikte büyük ölçüde artmıştır. Senaryo 3'te alınan veri trafiği 560.000 bit/sn ile 700.000 bit/sn arasında iken, senaryo 4'te 1.600.000 bit/sn ile 2.100.000 bit/sn arasında değişmiştir. Bu durum, blockchain kullanılarak şifrelenen paketleri ileten ağların daha fazla veri yükü oluşturduğunu göstermektedir. Aynı şekilde verimlilik de blockchain kullanılmadan paketleri ileten ağlarda daha yüksektir; senaryo 3'te 65.000 bit/sn ile 73.000 bit/sn arasında iken, senaryo 4'te 200.000 ile 260.000 bit/sn arasında dalgalanmıştır.

Bu değerlendirmeler sonucunda, blockchain teknolojisi kullanılarak şifrelenen paketleri ileten ağların güvenlik avantajlarına rağmen performans açısından bazı dezavantajlar oluşturduğu görülmektedir. Ancak güvenlik ihtiyacının kritik olduğu uygulamalarda, iletilen paketlerde blockchain kullanımı güvenli bir çözüm olarak tercih edilebilir.

Çizelge 4.1'de, dört senaryoların önemli performans ölçütleri bakımından karşılaştırılması sunulmaktadır.

Çizelge 4.1. Dört senaryonun karşılaştırılması

Metrik	**Senaryo 1** "standart"	**Senaryo 2** "blockchain kullanılarak"	**Senaryo 3** "standart"	**Senaryo 4** "blockchain kullanılarak"
Düğüm sayısı	5	5	29	29
Benzetim Süresi	900 sn	900 sn	900 sn	900 sn
Paket boyutu	512 byte	2500 byte	512 byte	2500 byte
Uçtan uca gecikme (ortalama)	0,03 sn	0,08 sn	0,035 sn	0,12 sn
Gönderilen veri trafiği (ortalama)	40.000 bit/sn	160.000 bit/sn	45.000 bit/sn	190.000 bit/sn
Alınan veri trafiği (ortalama)	137.000 bit/sn	525.000 bit/sn	650.000 bit/sn	1.800.000 bit/sn
Verim (ortalama)	64.000 bit/sn	280.000 bit/sn	68.000 bit/sn	230.000 bit/sn

5. SONUÇ

Bu tez çalışmasında, IoT güvenliğini artırmak için blockchain teknolojisi kullanılmıştır. Süreç, bir blockchain ağı kurmayı, IoT işlemlerini benzetim aracılığıyla kullanmayı ve gerçek dünyadan esinlenen senaryoları kullanarak sonuçları doğrulamayı içermektedir. IoT ortamlarında blockchain'in pratik potansiyelleri; kullanıcıları doğrulama, kaydetme, nesne kayıtlarını ekleme ve alma gibi eylemleri gerçekleştirmektir. Bu güvenli, merkezi olmayan yaklaşım veri bütünlüğünü güçlendirerek hassas bilgilerin sıklıkla alınıp verildiği IoT sistemleri için ideal bir çözüm haline getirmektedir.

Blockchain'in etkin kullanımının bulgulardan biri de, verilerin şeffaflığını ve izlenebilirliğini sağlamasıdır. Cihazların otonom olarak iletişim kurduğu bir IoT ortamında, veri doğruluğunun sağlanması ve zararlarının önlenmesi oldukça önemlidir. Blockchain'in bu etkileşimler için değişmez bir defter tutma rolü, güvenli IoT ağları için güçlü bir temele dayanır. Ayrıca, işlem geçmişlerini alma ve sahiplik kayıtlarını güvenli ve doğrulanmış bir şekilde değiştirme yeteneği, sistemin lojistik, akıllı şehirler ve bağlı cihazlar gibi sektörlerdeki faydasını desteklemektedir.

Gelecekteki çalışmalarda, bulgular blockchain'in IoT güvenliğini geliştirmede büyük bir potansiyele sahip olduğunu göstermektedir. Bununla birlikte, faydalarını tam olarak ortaya çıkarmak için daha çeşitli ortamlarda ek araştırma ve testler gereklidir. Daha verimli bir benzetim modeli geliştirmek ve gerçek dünyadaki IoT verilerini ve koşullarını dâhil etmek, daha iyi performans değerlendirmelerine olanak sağlayacaktır. Ek olarak, ağın IoT ağlarındaki dinamik koşullara tepkisini daha da optimize etmek için MÖ veya YZ tabanlı yaklaşımların dâhil edilmesi, uygulanabilirliğini artırabilir.

Sonuç olarak, blockchain ve IoT birleşimi, sağlam güvenlik mekanizmaları ve veri bütünlüğü güvencesi sunarak alanda gelişme sağlamaktadır. Daha fazla optimizasyon ve ölçeklenebilirlik değerlendirmeleriyle, blockchain özellikli IoT sistemleri güvenli cihaz iletişimi, veri yönetimi ve otomatik karar verme süreçleri için endüstri standardı haline gelebilir.

6. KAYNAKLAR

[1] "How Many IoT Devices Are There(2024-2032)". Erişim 22 Temmuz 2024. https://www.demandsage.com/number-of-iot-devices/

[2] D. Miorandi, S. Sicari, F. De Pellegrini, ve I. Chlamtac, "Internet of things: Vision, applications and research challenges", *Ad Hoc Networks*, c. 10, sy 7, ss. 1497-1516, Eyl. 2012.

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista, ve M. Zorzi, "Internet of things for smart cities", *IEEE Internet Things J*, c. 1, sy 1, ss. 22-32, Şub. 2014.

[4] I. Lee ve K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises", *Bus Horiz*, c. 58, sy 4, ss. 431-440, Tem. 2015.

[5] L. Woetzel, J. Remes, B. Boland, ve K. Lv, "Smart city technology for a more liveable future | McKinsey", Haz. 2018. Erişim 13 Eylül 2024. https://www.mckinsey.com/capabilities/operations/our-insights/smart-cities-digital-solutions-for-a-more-livable-future

[6] S. Sicari, A. Rizzardi, L. A. Grieco, ve A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead", *Computer Networks*, c. 76, ss. 146-164, Oca. 2015.

[7] HP, "Internet of Things Research Study", 2014.

[8] C. Kolias, G. Kambourakis, A. Stavrou, ve J. Voas, "DDoS in the IoT: Mirai and other botnets", *Computer (Long Beach Calif)*, c. 50, sy 7, ss. 80-84, 2017.

[9] R. H. Weber ve E. Studer, "Cybersecurity in the Internet of Things: Legal aspects", *Computer Law and Security Review*, c. 32, sy 5, ss. 715-728, Eki. 2016.

[10] K. Christidis ve M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things", *IEEE Access*, c. 4, ss. 2292-2303, 2016.

[11] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, Erişim 13 Eylül 2024. www.bitcoin.org

[12] S. Singh, A. S. M. Sanwar Hosen, ve B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network", *IEEE Access*, c. 9, ss. 13938-13959, 2021.

[13] A. Reyna, C. Martín, J. Chen, E. Soler, ve M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities", *Future Generation Computer Systems*, c. 88, ss. 173-190, Kas. 2018.

[14] A. Bahga, V. K. Madisetti, A. Bahga, ve V. K. Madisetti, "Blockchain Platform for Industrial Internet of Things", *Journal of Software Engineering and Applications*, c. 9, sy 10, ss. 533-546, Eki. 2016.

[15] E. A. Shammar, A. T. Zahary, ve A. A. Al-Shargabi, "A Survey of IoT and Blockchain Integration: Security Perspective", *IEEE Access*, c. 9, ss. 156114-156150, 2021.

[16] Z. Zheng, S. Xie, H. Dai, X. Chen, ve H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, ss. 557-564, Eyl. 2017.

[17] E. Androulaki *vd.*, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains", *Proceedings of the 13th EuroSys Conference, EuroSys 2018*, c. 2018-January, Oca. 2018.

[18] A. de Vries, "Bitcoin's Growing Energy Problem", *Joule*, c. 2, sy 5, ss. 801-805, May. 2018.

[19] R. H. Weber, "Internet of Things - New security and privacy challenges", *Computer Law and Security Review*, c. 26, sy 1, ss. 23-30, Oca. 2010.

[20] J. Gubbi, R. Buyya, S. Marusic, ve M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions", *Future Generation Computer Systems*, c. 29, sy 7, ss. 1645-1660, Eyl. 2013.

[21] IBM, "Cost of a data breach", 2024. Erişim: 13 Eylül 2024. [Çevrimiçi]. Erişim adresi: https://www.ibm.com/reports/data-breach

[22] J. Kindervag, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture", 2010. Erişim 13 Eylül 2024. https://www.forrester.com/report/Build-Security-Into-Your-Networks-DNA-The-Zero-Trust-Network-Architecture/RES57047

[23] M. Ali, S. U. Khan, ve A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges", *Inf Sci (N Y)*, c. 305, ss. 357-383, Haz. 2015

[24] K. Panetta, "Gartner Top Security and Risk Trends for 2021". Erişim 13 Eylül 2024. https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021

[25] "Top Threats to Cloud Computing", 2020, Erişim 13 Eylül 2024. https://cloudsecurityalliance.org

[26] M. Ozkan-Okay *vd.*, "A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions", *IEEE Access*, c. 12, ss. 12229-12256, 2024.

[27] G. Zyskind, O. Nathan, ve A. S. Pentland, "Decentralizing privacy: Using

blockchain to protect personal data", *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, ss. 180-184, Tem. 2015

[28] W. Mougayar ve Vitalik Buterin, "The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology | Wiley", s. 208, 2016, Erişim 13 Eylül 2024. https://www.wiley.com/en-be/The+Business+Blockchain%3A+Promise%2C+Practice%2C+and+Application+of+the+Next+Internet+Technology-p-9781119300311

[29] M. K. Aiden, S. M. Sabharwal, S. Chhabra, ve M. Al-Asadi, "AI and Blockchain for Cyber Security in Cyber-Physical System", ss. 203-230, 2023, doi: 10.1007/978-3-031-31952-5_10.

[30] M. Wu, T. J. Lu, F. Y. Ling, J. Sun, ve H. Y. Du, "Research on the architecture of Internet of Things", *ICACTE 2010 - 2010 3rd International Conference on Advanced Computer Theory and Engineering, Proceedings*, c. 5, 2010.

[31] "That 'Internet of Things' Thing", *RFID JOURNAL*, Haz. 2009, Erişim 13 Eylül 2024. https://www.rfidjournal.com/expert-views/that-internet-of-things-thing/73881/

[32] J. Holler, V. Tsiatsis, C. Mulligan, S. Avesand, S. Karnouskos, ve D. Boyle, "From Machine-To-Machine to the Internet of Things", *From Machine-To-Machine to the Internet of Things*, ss. 1-331, 2014.

[33] P. Nayak, K. Kavitha, ve C. Mallikarjuna Rao, "IoT-Enabled Agricultural System Applications, Challenges and Security Issues", *Studies in Big Data*, c. 63, ss. 139-163, 2020.

[34] "2020 Unit 42 IoT Threat Report". Erişim 13 Eylül 2024. https://unit42.paloaltonetworks.com/iot-threat-report-2020/

[35] L. Da Xu, W. He, ve S. Li, "Internet of things in industries: A survey", *IEEE Trans Industr Inform*, c. 10, sy 4, ss. 2233-2243, Kas. 2014.

[36] A. Ayub Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz, ve S. Kot, "Internet of Things (IoT) Security With Blockchain Technology: A State-of-the-Art Review", *IEEE Access*, c. 10, ss. 122679-122695, 2022.

[37] J. Wan *vd.*, "Wearable IoT enabled real-time health monitoring system", *EURASIP J Wirel Commun Netw*, c. 2018, sy 1, ss. 1-10, Ara. 2018.

[38] K. S. Arikumar, A. Deepak Kumar, C. Gowtham, ve S. B. Prathiba, "Decentralized loan management application using smart contracts on block chain", *Advances in Parallel Computing*, c. 38, ss. 106-110, Eki. 2021.

[39] V. Buterin, "A Next Generatıon Smart Contract & Decentralızed Applıcatıon Platform", *white paper*, c. 3, sy 37, ss. 1-2, Oca. 2014.

[40] S. Saberi, M. Kouhizadeh, J. Sarkis, ve L. Shen, "Blockchain technology and its

relationships to sustainable supply chain management", *Int J Prod Res*, c. 57, sy 7, ss. 2117-2135, Nis. 2019.

[41] A. Baliga, "Understanding Blockchain Consensus Models", 2017.

[42] P. R. Nair ve D. R. Dorai, "Evaluation of performance and security of proof of work and proof of stake using blockchain", *Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021*, ss. 279-283, Şub. 2021.

[43] S. King ve S. Nadal, "PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake", 2012.

[44] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy", *Telecomm Policy*, c. 41, sy 10, ss. 1027-1038, Kas. 2017.

[45] T. T. Kuo, H. E. Kim, ve L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications", *Journal of the American Medical Informatics Association*, c. 24, sy 6, ss. 1211-1220, Kas. 2017.

[46] A. Dorri, S. S. Kanhere, R. Jurdak, ve P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home", *2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017*, ss. 618-623, May. 2017.

[47] F. Schär, "Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets", *SSRN Electronic Journal*, Mar. 2020, doi: 10.2139/SSRN.3571335.

[48] K. Croman *vd.*, "On scaling decentralized blockchains (A position paper)", *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, c. 9604 LNCS, ss. 106-125, 2016.

[49] V. Buterin, "Sharding FAQ". Erişim 13 Eylül 2024. https://vitalik.eth.limo/general/2017/12/31/sharding_faq.html

[50] A. Zohar, "Bitcoin: Under the hood", *Commun ACM*, c. 58, sy 9, ss. 104-113, Eyl. 2015.

[51] S. Basudan, "A Scalable Blockchain Framework for Secure Transactions in IoT-Based Dynamic Applications", *IEEE Open Journal of the Communications Society*, 2023, doi: 10.1109/OJCOMS.2023.3307337.

[52] A. Pathak, I. Al-Anbagi, ve H. J. Hamilton, "TABI: Trust-Based ABAC Mechanism for Edge-IoT Using Blockchain Technology", *IEEE Access*, c. 11, ss. 36379-36398, 2023.

[53] S. S. Seshadri *vd.*, "IoTCop: A Blockchain-Based Monitoring Framework for Detection and Isolation of Malicious Devices in Internet-of-Things Systems",

IEEE Internet Things J, c. 8, sy 5, ss. 3346-3359, Mar. 2021.

[54] B. Bera, S. Saha, A. K. Das, ve A. V. Vasilakos, "Designing blockchain-based access control protocol in iot-enabled smart-grid system", *IEEE Internet Things J*, c. 8, sy 7, ss. 5744-5761, Nis. 2021.

[55] H. M. Buttar, W. Aman, M. M. U. Rahman, ve Q. H. Abbasi, "Countering Active Attacks on RAFT-Based IoT Blockchain Networks", *IEEE Sens J*, c. 23, sy 13, ss. 14691-14699, Tem. 2023.

[56] X. Yang *vd.*, "Blockchain-Based Secure and Lightweight Authentication for Internet of Things", *IEEE Internet Things J*, c. 9, sy 5, ss. 3321-3332, Mar. 2022.

[57] G. Rathee, F. Ahmad, N. Jaglan, ve C. Konstantinou, "A Secure and Trusted Mechanism for Industrial IoT Network Using Blockchain", *IEEE Trans Industr Inform*, c. 19, sy 2, ss. 1894-1902, Şub. 2023.

[58] H. Liu, D. Han, ve D. Li, "Fabric-iot: A Blockchain-Based Access Control System in IoT", *IEEE Access*, c. 8, ss. 18207-18218, 2020.

[59] J. Maeng, Y. Heo, ve I. Joe, "Hyperledger Fabric-Based Lightweight Group Management (H-LGM) for IoT Devices", *IEEE Access*, c. 10, ss. 56401-56409, 2022.

[60] E. A. Shammar, A. T. Zahary, ve A. A. Al-Shargabi, "An Attribute-Based Access Control Model for Internet of Things Using Hyperledger Fabric Blockchain", *Wirel Commun Mob Comput*, c. 2022, 2022, doi: 10.1155/2022/6926408.

[61] R. Kaur ve A. Ali, "A Novel Blockchain Model for Securing IoT Based Data Transmission", *International Journal of Grid and Distributed Computing*, c. 14, sy 1, ss. 1045-1055, Nis. 2021.

[62] H. Zhang, X. Zhang, Z. Guo, H. Wang, D. Cui, ve Q. Wen, "Secure and Efficiently Searchable IoT Communication Data Management Model: Using Blockchain as a New Tool", *IEEE Internet Things J*, c. 10, sy 14, ss. 11985-11999, Tem. 2023.

[63] Z. Gong-Guo ve Z. Wan, "Blockchain-based IoT security authentication system", *Proceedings - 2021 International Conference on Computer, Blockchain and Financial Development, CBFD 2021*, ss. 415-418, 2021.

[64] D. Li, W. Peng, W. Deng, ve F. Gai, "A blockchain-based authentication and security mechanism for IoT", *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, c. 2018-July, Eki. 2018, doi: 10.1109/ICCCN.2018.8487449.

[65] F. P. Oikonomou, J. Ribeiro, G. Mantas, J. M. C. S. Bastos, ve J. Rodriguez, "A Hyperledger Fabric-based Blockchain Architecture to Secure IoT-based Health Monitoring Systems", *2021 IEEE International Mediterranean Conference on Communications and Networking, MeditCom 2021*, ss. 186-190, 2021.

[66] R. Shahin ve K. E. Sabri, "A Secure IoT Framework Based on Blockchain and Machine Learning", *International Journal of Computing and Digital Systems*, c. 11, sy 1, ss. 671-683, 2022.

[67] Y. Türkyilmaz ve A. Şentürk, "Saldırı Tespitinde Makine Öğrenmesi Yöntemlerinin Performans Analizi", *Avrupa Bilim ve Teknoloji Dergisi*, c. 32, sy 32, ss. 107-112, Ara. 2021.

[68] A. Dorri, S. S. Kanhere, R. Jurdak, ve P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home", *2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017*, ss. 618-623, May. 2017.

[69] S. N. Mohanty *vd.*, "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy", *Future Generation Computer Systems*, c. 102, ss. 1027-1037, Oca. 2020.

[70] A. Dorri, S. S. Kanhere, R. Jurdak, ve P. Gauravaram, "LSB: A Lightweight Scalable Blockchain for IoT security and anonymity", *J Parallel Distrib Comput*, c. 134, ss. 180-197, Ara. 2019.

[71] M. Du *vd.*, "Spacechain: A three-dimensional blockchain architecture for IoT security", *IEEE Wirel Commun*, c. 27, sy 3, ss. 38-45, Haz. 2020.

[72] Z. Bao, W. Shi, D. He, ve K.-K. R. Chood, "IoTChain: A Three-Tier Blockchain-based IoT Security Architecture", Haz. 2018, Erişim 02 Aralık 2023. https://arxiv.org/abs/1806.02008v2

[73] D. Na, S. Park, J. Prieto, ve F. De La Prieta, "Fusion Chain: A Decentralized Lightweight Blockchain for IoT Security and Privacy", *Electronics 2021, Vol. 10, Page 391*, c. 10, sy 4, s. 391, Şub. 2021.

[74] A. S. Rajawat, R. Rawat, K. Barhanpurkar, R. N. Shaw, ve A. Ghosh, "Blockchain-Based Model for Expanding IoT Device Data Security", *Advances in Intelligent Systems and Computing*, c. 1319, ss. 61-71, 2021.

[75] Y. Abbassi ve H. Benlahmer, "BCSDN-IoT: Towards an IoT security architecture based on SDN and Blockchain", *International journal of electrical and computer engineering systems*, c. 13, sy 2, ss. 155-163, Şub. 2022.

[76] M. T. Hammi, B. Hammi, P. Bellot, ve A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT", *Comput Secur*, c. 78, ss. 126-142, Eyl. 2018.

[77] C. Cachin, "Architecture of the Hyperledger Blockchain Fabric", Tem. 2016.

[78] A. Baliga, "Understanding Blockchain Consensus Models", 2017.

[79] "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL", Official Journal of the European Union. Erişim 24 Eylül 2024.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[80] J. Sousa, A. Bessani, ve M. Vukolic, "A byzantine Fault-Tolerant ordering service for the hyperledger fabric blockchain platform", *Proceedings - 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2018*, ss. 51-58, Tem. 2018

[81] A. Kamilaris, A. Fonts, ve F. X. Prenafeta-Boldú, "The rise of blockchain technology in agriculture and food supply chains", *Trends Food Sci Technol*, c. 91, ss. 640-652, Eyl. 2019.

[82] C. Gorenflo, S. Lee, L. Golab, ve S. Keshav, "FastFabric: Scaling Hyperledger Fabric to 20,000 Transactions per Second", *ICBC 2019 - IEEE International Conference on Blockchain and Cryptocurrency*, ss. 455-463, May. 2019.

[83] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication", *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, c. 9591, ss. 112-125, 2016

[84] "Channels — hyperledger-fabricdocs master documentation". Erişim 24 Eylül 2024. https://hyperledger-fabric.readthedocs.io/en/release-2.0/channels.html

[85] Q. Wang ve S. Qin, "A Hyperledger Fabric-Based System Framework for Healthcare Data Management", *Applied Sciences 2021, Vol. 11, Page 11693*, c. 11, sy 24, s. 11693, Ara. 2021.

[86] "Chaincode Tutorials — hyperledger-fabricdocs master documentation". Erişim 25 Eylül 2024. https://hyperledger-fabric.readthedocs.io/en/release-2.0/chaincode.html

[87] K. Wannenwetsch, I. Ostermann, R. Priel, F. Gerschner, ve A. Theissler, "Blockchain for Supply Chain Management: A Literature Review and Open Challenges", *Procedia Comput Sci*, c. 225, ss. 1312-1321, Oca. 2023

[88] "Private data — hyperledger-fabricdocs master documentation". Erişim 25 Eylül 2024. https://hyperledger-fabric.readthedocs.io/en/release-2.0/private-data/private-data.html

[89] S. Khezr, M. Moniruzzaman, A. Yassine, ve R. Benlamri, "Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research", *Applied Sciences 2019, Vol. 9, Page 1736*, c. 9, sy 9, s. 1736, Nis. 2019.

[90] P. Thakkar, S. Nathan, ve B. Viswanathan, "Performance benchmarking and optimizing hyperledger fabric blockchain platform", *Proceedings - 26th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, MASCOTS 2018*, ss. 264-276, Kas. 2018.

[91] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, ve J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems", *IEEE Trans Knowl*

Data Eng, c. 30, sy 7, ss. 1366-1385, Tem. 2018

[92] "Ledger — hyperledger-fabricdocs master documentation". Erişim 17 Ekim 2024. https://hyperledger-fabric.readthedocs.io/en/release-2.0/ledger/ledger.html

[93] "Riverbed to Acquire OPNET Technologies, Inc. | Business Wire". Erişim 25 Eylül 2024. https://www.businesswire.com/news/home/20121029005605/en/Riverbed-to-Acquire-OPNET-Technologies-Inc.

[94] Xinjie Chang, "Network simulations with OPNET", ss. 307-314, Oca. 2003.

[95] Z. Lu ve H. Yang, "Unlocking the power of OPNET modeler", *Unlocking the Power of OPNET Modeler*, c. 9780521198745, ss. 1-238, Oca. 2012.

[96] M. Chen, Y. Miao, ve I. Humar, *OPNET IoT Simulation*. Springer Singapore, 2019. doi: 10.1007/978-981-32-9170-6.

[97] H. A. Mohammed, A. H. Ali, ve H. J. Mohammed, "The Affects of Different Queuing Algorithms within the Router on QoS VoIP application Using OPNET", *International journal of Computer Networks & Communications*, c. 5, sy 1, ss. 117-124, Şub. 2013.

[98] X. Li, Y. Wang, P. Vijayakumar, D. He, N. Kumar, ve J. Ma, "Blockchain-Based Mutual-Healing Group Key Distribution Scheme in Unmanned Aerial Vehicles Ad-Hoc Network", *IEEE Trans Veh Technol*, c. 68, sy 11, ss. 11309-11322, Kas. 2019.

[99] K. N. Qureshi, G. Jeon, M. M. Hassan, M. R. Hassan, ve K. Kaur, "Blockchain-Based Privacy-Preserving Authentication Model Intelligent Transportation Systems", *IEEE Transactions on Intelligent Transportation Systems*, c. 24, sy 7, ss. 7435-7443, Tem. 2023.

[100] S. M. Pournaghi, M. Bayat, ve Y. Farjami, "MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption", *J Ambient Intell Humaniz Comput*, c. 11, sy 11, ss. 4613-4641, Kas. 2020.

[101] "Introduction — Hyperledger Fabric Docs main documentation". Erişim 23 Eylül 2024. https://hyperledger-fabric.readthedocs.io/en/release-2.5/whatis.html

[102] "Hyperledger Fabric Tutorial - Enterprise Blockchain Solution". Erişim 08 Ekim 2024. https://chainstack.com/picking-an-enterprise-blockchain-protocol-to-develop-on-hyperledger-fabric/

[103] I. S. Hammoodi, B. G. Stewart, A. Kocian, ve S. G. McMeekin, "A comprehensive performance study of OPNET modeler for ZigBee wireless sensor networks", *NGMAST 2009 - 3rd International Conference on Next Generation Mobile Applications, Services and Technologies*, ss. 357-362, 2009.

[104] A. Jarjis ve G. Kadir, "Blockchain Authentication for AODV Routing Protocol", *2020 2nd International Conference on Blockchain Computing and Applications, BCCA 2020*, ss. 78-85, Kas. 2020.

[105] S. Kaur MTech Scholar, A. Faridkot, P. Harinderpal Singh Assistant Professor, ve P. Gurjeevan Singh, "Examine the Performance of different Topologies using Opnet 14.5 in ZigBee Sensor Network", *Int J Comput Appl*, c. 108, sy 7, ss. 1-5, Ara. 2014.

[106] X. Li, M. Peng, J. Cai, C. Yi, ve H. Zhang, "OPNET-based modeling and simulation of mobile Zigbee sensor networks", *Peer Peer Netw Appl*, c. 9, sy 2, ss. 414-423, Mar. 2016.

[107] K. Malarvizhi, M. Brindha, ve M. Kumar, "Evaluation of energy efficient routing in wireless multimedia sensor networks", *2nd International Conference on Electronics and Communication Systems, ICECS 2015*, ss. 1387-1391, Haz. 2015.

[108] T. F. Silva ve D. G. Costa, "Centralized Algorithms for Redundant Coverage Maximization in Wireless Visual Sensor Networks", *IEEE Latin America Transactions*, c. 14, sy 7, ss. 3378-3384, Tem. 2016.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Selami TERAZİ

Yabancı Dili : Arapça, İngilizce

ÖĞRENİM DURUMU

Derece	Alan	Okul/Üniversite	Mezuniyet Yılı
Y. Lisans	Siber Güvenlik	Düzce Üniversitesi	2024
Lisans	Bilgisayar Müh.	Düzce Üniversitesi	2022
Lise	Sayısal	Um Alqura Lisesi	2018

TEZDEN ÇIKAN YAYIN

A. Şentürk and S. Terazi, “IoT security with blockchain: A review”, *EJRnD*, vol. 3, no. 4, pp. 117–132, Dec. 2023.