T.R.
SAKARYA UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

A BLOCKCHAIN-BASED ENHANCED SECURITY SYSTEM FOR IOT PLATFORMS

MSc THESIS

Abdullah AL MOKDAD

Computer and Information Engineering Department

Computer Engineering Program

AUGUST 2023

T.R.
SAKARYA UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

A BLOCKCHAIN-BASED ENHANCED SECURITY SYSTEM FOR IOT PLATFORMS

MSc THESIS

Abdullah AL MOKDAD

Computer and Information Engineering Department

Computer Engineering Program

Thesis Advisor: Doç.Dr. Ünal ÇAVUŞOĞLU

AUGUST 2023

The thesis work titled “A Blockchain-Based enhanced security system for IoT platforms” prepared by Abdullah Al-Mokdad was accepted by the following jury on 25/08/2023 by unanimously of votes as a MSc THESIS in Sakarya University Graduate School of Natural and Applied Sciences, Computer and Information Engineerıng department, Computer and Information Engineering programe.

Thesis Jury

Head of Jury :	**Prof. Dr Devrim AKGÜN** Sakarya University	....
Jury Member :	**Dr. Öğr Üyesi Selman HIZAL** Sakarya University of Applied Sciences	....
Jury Member :	**Doç.Dr. Ünal ÇAVUŞOĞLU** (Advisor) Sakarya University	....

STATEMENT OF COMPLIANCE WITH THE ETHICAL PRINCIPLES AND RULES

I declare that the thesis work titled "A BLOCKCHAIN-BASED ENHANCED SECURITY SYSTEM FOR IOT PLATFORMS ", which I have prepared in accordance with Sakarya University Graduate School of Natural and Applied Sciences regulations and Higher Education Institutions Scientific Research and Publication Ethics Directive, belongs to me, is an original work, I have acted in accordance with the regulations and directives mentioned above at all stages of my study, I did not get the innovations and results contained in the thesis from anywhere else, I duly cited the references for the works I used in my thesis, I did not submit this thesis to another scientific committee for academic purposes and to obtain a title, in accordance with the articles 9/2 and 22/2 of the Sakarya University Graduate Education and Training Regulation published in the Official Gazette dated 20.04.2016, a report was received in accordance with the criteria determined by the graduate school using the plagiarism software program to which Sakarya University is a subscriber, I have received an ethics committee approval document ,I accept all kinds of legal responsibility that may arise in case of a situation contrary to this statement.

(05 / 08 / 2023)

( )

Abdullah Al-Mokdad

To my parents brothers, and sisters I am extremely grateful each one of you, for their unwavering support and encouragement throughout my academic journey.

ACKNOWLEDGMENTS

Before and after everything, I thank Allah Almighty for the blessing of completing this work and for everything

I am extremely grateful to my supervisor, Dr. Ünal, for his valuable guidance, insights, and encouragement throughout this work.

I am deeply indebted to my mentors and professors at the university who have imparted their knowledge and expertise to me and have played a crucial role in shaping my academic and professional career. I am also grateful to my colleagues and friends for their support and camaraderie during this project. Finally, I would like to express my sincere appreciation to the university, the college, and all the staff members for providing me with the necessary resources and facilities to complete this project successfully.

Abdullah Al-Mokdad

TABLE OF CONTENTS

Sayfa

ACKNOWLEDGMENTS ix
TABLE OF CONTENTS... x
ABBREVIATIONS xii
LIST OF TABLES xiv
LIST OF FIGURES xvi
SUMMARY.. xviii
ÖZET……... xxi
1. INTRODUCTION.. 1
1.1. Overview 1
1.2. Problem Statement... 2
1.3. Objective.. 3
1.4. Research Questions 3
1.5. Literature Review 4
1.6. Organization 9
2. THEORETICAL BACKGROUND... 11
2.1. Blockchain Technology.. 11
2.1.1. Overview of blockchain 11
2.1.2. Blockchain characteristics... 12
2.1.3. Blockchain basic elements 14
2.1.4. Blockchain types 15
2.1.5. Ethereum 16
2.2. Internet of Things 17
2.2.1. Overview about internet of things... 17
2.2.2. Importance of internet of things.. 19
2.2.3. Architecture of internet of things 20
2.2.4. Challenges for internet of things 21
2.3. Exploring the Impact of Blockchain Technology on IoT............................ 23
3. TOOLS AND LIBRARIES 31
3.1. NPM & Node.js.. 31
3.2. Ganache 32
3.3. Truffle... 33
3.4. Ethers.js 33
3.5. HTML, CSS & JavaScript... 34
4. IMPLEMENTATION.. 35
4.1. System Diagram 35
4.2. Smart Contract... 36
4.3. Web Interface 38
4.4. JavaScript Functions.. 40
5. RESULTS AND DISCUSSION.. 43

5.1. Results 43
5.2. Discussion 44
6. CONCLUSION AND RECOMMENDATIONS 47
6.1. Conclusion 47
6.2. Future Work 48
REFERENCES 49
CURRICULUM VITAE 55

ABBREVIATIONS

IOT	: Internet of Things
BC	: Blockchain technology
DDOS	: Distributed denial of service
P2P	: Peer to Peer
ITS	: Intelligent Transportation Systems
HTML	: Hyper text Markup Language
CSS	: Cascading Style Sheets
POW	: Proof of Work
POS	: Proof of Stake
DPoS	: Delegated Proof of Stake
PBFT	: Practical Byzantine Fault Tolerance
DApps	: Decentralized applications
EVM	: Ethereum Virtual Machine
IIoT	: Industrial Internet of Things
Wi-Fi	: Wireless Fidelity
GDPR	: General Data Protection Regulation
BIoT	:blockchain Based Internet of Things
V2V	: Vehicle to Vehicle
V2I	: Vehicle to Infrastructure
NPM	: Node Package Manager
APIs	: Application Programming Interfaces
I/O	:Input / Output
ENS	: Ethereum Name Service
ABI	: Application Binary Interface
URL	: Uniform Resource Locators

LIST OF TABLES

Page

Table 1.1. Literature Review. 7
Table 1.2. (Continued) Literature Review. 8
Table 1.3. (Continued) Literature Review. 9

LIST OF FIGURES

Page

Figure 2.1. Blockchain Elements. 14
Figure 2.2. BIOT Architecture in Supply Chain Management [59]. 23
Figure 2.3. BIOT Architecture in Smart Energy Grid [61]. 24
Figure 2.4. BIOT Architecture in Healthcare [63]. 24
Figure 2.5. BIOT Architecture in Smart Home [65]. 25
Figure 2.6. BIOT Architecture in Autonomous Vehicles [67]. 26
Figure 2.7. BIOT Architecture in Food Traceability [69]. 26
Figure 2.8. BIOT Architecture in Smart City [71]. 27
Figure 2.9. BIOT Architecture in Waste Management [73]. 28
Figure 2.10. BIOT Architecture in Citizen Identity [75]. 29
Figure 3.1. Ganache Main Screen. 32
Figure 4.1. System Diagram. 36
Figure 4.2. Smart Contract Code. 38
Figure 4.3. Smart Contract Migrations Result. 38
Figure 4.4. Smart Contract Web Interface. 39
Figure 4.5. Web Server Script. 40

A BLOCKCHAIN-BASED ENHANCED SECURITY SYSTEM FOR IOT PLATFORMS

SUMMARY

With technology advancing at an unprecedented pace, the world is currently experiencing a profound transformation driven by the rapid growth of the Internet of Things and the emergence of blockchain technology. The Internet of Things has emerged as a powerful force, connecting numerous devices and sensors to collect and exchange vast amounts of data. However, effectively managing and securing this sensor data presents significant challenges. Concurrently, blockchain technology has gained considerable attention for its potential to revolutionize data management and ensure trust and transparency across various domains. The convergence of IoT and blockchain holds immense promise for addressing the limitations of traditional data management systems.

This study aims to address the challenges associated with efficient sensor data management. It proposes the integration of blockchain technology with a user-friendly web-based interface to enhance data management, security, and reliability. To achieve this, by building a local blockchain network using ganache, smart contract writen in solidity language, a user-friendly web interface was developed utilizing HTML, CSS, and JavaScript, and connect them with virtual sensors. The virtual sensor send reading to the web interface. This interface collect the reading from differante sensor and send it to the smart contract. The system leverages smart contracts on the Ethereum blockchain to ensure data integrity, automate processes, and enhance security.

The integration of blockchain technology offers significant benefits for sensor data management. By utilizing the decentralized nature of the blockchain, the system provides a robust infrastructure for storing and retrieving sensor readings. Smart contracts enable tamper-proof data transactions, ensuring transparency and immutability of the data stored on the blockchain.

The implementation of the proposed system has yielded promising results. The web interface facilitates seamless interaction with sensor data, improving user experience and accessibility. The integration of smart contracts ensures secure and verifiable data transactions, reducing the risk of data manipulation, and enhancing trust in the system. The integration of blockchain technology in sensor data management has proven to be effective in improving data security, reliability, and accessibility. The developed web interface and smart contract integration provide a solid foundation for future advancements in the field. Future work could involve deploying the system on a real blockchain network and connecting it to real sensors through oracles, further enhancing its practicality and real-world applicability.

This thesis contributes to the advancement of sensor data management systems, offering potential applications in various domains that require reliable and secure data handling. By combining blockchain technology, a user-friendly web interface, and smart contracts, the thesis provides a comprehensive solution for enhanced sensor data management.

IOT PLATFORMLARI IÇIN BLOCKCHAIN TABANLI GELIŞMIŞ GÜVENLIK SISTEMI

ÖZET

Internet of Things (IoT), birbirine bağlı olan robotlar, akıllı telefonlar, otomobiller, insansız hava araçları, endüstriyel kontrol sistemleri ve diğer elektronik cihazlar gibi fiziksel cihazların birbirine bağlanmasıyla oluşan ve ulaşım, enerji, sağlık, endüstri, ticaret ve finans gibi alanlarda iş ve görev süreçlerinin dönüşümünü destekleyen bir dizi teknolojidir. IoT, bu bileşenlerin veri alışverişine imkan tanıyan tanımlanmış bir ağ üzerinden bağlantı kurulan bir yapıdır.

Herhangi bir IoT sistemi üç ana katmandan oluşur: algılama, ağ ve uygulama katmanı. Bu katman, çevreleyen ortamdan veri toplar ve yararlı ve anlamlı bilgiler sağlar. Bu katmandaki cihazlar doğrudan bağlı değildir, ancak merkezi bir ağ geçidi aracılığıyla bağlanırlar. Ağ katmanı, tüm IoT bileşenlerini İnternet'e bağlar. Bu katmanda, önceki bahsedilen ağ geçidine ara katman rolü oynayan farklı iletişim teknolojileri aracılığıyla algılama katmanı ile ağ katmanı arasında iletişim olasılığını sağlar. Uygulama katmanı, akıllı şehir, sağlık, otomobiller, akıllı telefonlar ve diğerleri gibi sensörler tarafından alınan verilerden faydalanmak için çeşitli IoT uygulamalarını içerir.

IoT'deki temel süreç, farklı cihazların ilgili verileri bağımsız olarak takas etmesidir ve veri akışlarına odaklanarak dijital ve fiziksel alanlar arasındaki sınırları daha da bulanıklaştırır. Bununla birlikte, IoT güvenlik ve verimlilik konularında ciddi sınırlamalarla karşı karşıyadır.

Blok zinciri teknolojisi veya dağıtık defter teknolojisi, sürekli olarak artan bir veri kümesini kontrol etmek için kullanılan dağıtık ve merkezi olmayan bir işlem defteridir. Bir işlemi deftere kaydetmek için blok zinciri ağındaki ilgili düğümler anlaşmalı ve anlaşmalarını imzalamalıdır. Bir dizi işlem bir bloğa gruplandırılır ve bu blok zincirindeki her bir bloğa önceki bloğa bir zaman damgası ve karma fonksiyonu eklenir.

Karma fonksiyonu bloğun verilerinin bütünlüğünü ve inkâr edilemezliğini doğrular. Ayrıca, tüm katılan düğümlerin güncel kalması için her kullanıcının orijinal defterin bir kopyası vardır ve tüm düğümler yeni değişikliklerle senkronize edilir ve güncellenir. Blok zinciri, işlem yapan tüm düğümler arasında işlemlerin ayrıntılarını paylaştığı için daha yüksek bir şeffaflık seviyesi sunar. Blok zinciri çerçevesinde güvenilir işlemlerin yapılması için üçüncü bir tarafa ihtiyaç yoktur. Ayrıca, blok zinciri, kötü niyetli eylemlere karşı sistemleri korumak için genel anahtar altyapısını kullanarak daha iyi bir güvenlik sağlar.

Teknolojinin hızlı ilerlemesi, özellikle nesnelerin interneti ve blok zinciri alanlarında, çeşitli endüstrilerde yeni bir olasılık ve potansiyel çağını başlatmıştır. Bu dönüştürücü değişim, IoT'nin dikkate değer yetenekleri tarafından desteklenir ve büyüyen cihaz ve sensör sayısını sorunsuz bir şekilde birleştirerek veri üretiminde muazzam bir artışa

yol açar. Bu cihazların birbirine bağlanması, veri toplama, alışveriş ve analizi için sonsuz olanaklar sunar. Ancak, sensör verilerinin hacmi ve karmaşıklığı arttıkça, bu değerli kaynağın etkili bir şekilde yönetilmesi ve güvence altına alınması giderek zorlaşmaktadır.

Aynı zamanda, blok zinciri teknolojisi, veri yönetimi uygulamalarını devrimleştirebilecek potansiyeli nedeniyle geniş çapta ilgi görmektedir. Blok zinciri, merkezi olmayan ve değiştirilemez bir defter olarak işlem kaydedip doğrulama konusunda güvenli bir platform sağlar. Blok zincirini Nesnelerin İnterneti ile entegre etmek, geleneksel veri yönetim sistemlerinin doğasında bulunan sınırlamaları ele alarak güçlü bir sinerji ortaya çıkarır. Blok zinciri teknolojisinin entegrasyonu, sensör verilerinin yönetimi için çeşitli cazip avantajlar sunar. Blok zincirinin merkezi olmayan doğasını kullanarak sistem, sensör okumalarını sorunsuz bir şekilde depolamak ve almak için dayanıklı ve sağlam bir altyapı oluşturur. Akıllı sözleşmelerin gücünden yararlanmak, değişmez veri işlemlerine imkân tanır ve blok zincirinde depolanan tüm veriler için benzersiz bir şeffaflık ve değişmezlik seviyesi sağlar. Bu dönüştürücü değişim, veri güvenliğini artırmakla kalmaz, aynı zamanda her işlemin kaydedildiği ve denetlenebilir olduğu bir güven ve güvenilirlik ortamı oluşturarak sistemin bütünlüğüne ilişkin tartışmasız bir kayıt oluşturur.

Bu çalışma, verimli sensör verisi yönetimi ile ilgili zorlukları ele almaya yönelik hedefler taşımaktadır. Veri yönetimi, güvenlik ve güvenilirliği artırmak için blok zinciri teknolojisinin kullanıcı dostu bir web tabanlı arayüzle entegrasyonunu önermektedir. Bu amaca ulaşmak için Ganache kullanılarak yerel bir blok zinciri ağı oluşturuldu, Solidity dilini kullanarak akıllı bir sözleşme geliştirildi ve HTML, CSS ve JavaScript kullanılarak kullanıcı dostu bir web arayüzü oluşturuldu. Bu sistem, web arayüzüne okumalar gönderen sanal sensörlerle bağlantı kurularak uygulandı. Arayüz, farklı sensörlerden okumaları toplar ve bunları akıllı sözleşmeye gönderir. Sistem, Ethereum blok zincirindeki akıllı sözleşmeleri kullanarak veri bütünlüğünü sağlar, süreçleri otomatikleştirir ve güvenliği artırır.

Önerilen sistemin uygulanması önemli ve umut verici sonuçlar vermiştir. Kullanıcı dostu web arayüzü, sensör verileriyle etkileşimi teşvik eden sezgisel ve sorunsuz bir deneyim sunar. Artan erişilebilirlik ve geliştirilmiş kullanıcı deneyimi, sensör verisi yönetiminin tam potansiyelinin gerçekleştirilmesi için temel unsurlardır. Akıllı sözleşmelerin sorunsuz entegrasyonuyla, sistem veri işlemleri için güvenli ve doğrulanabilir bir ortam sağlar, veri manipülasyonuyla ilişkili riskleri etkili bir şekilde azaltır ve sistem içinde genel bir güven hissi oluşturur. Blok zinciri teknolojisinin sensör verisi yönetiminde sunulan somut faydalar, veri güvenliğini, güvenilirliğini ve erişilebilirliğini önemli ölçüde artırır.

Ayrıca, web arayüzünün geliştirilmesi ve akıllı sözleşmelerin başarılı bir şekilde entegrasyonu, alanda gelecekteki ilerlemeler için sağlam bir temel oluşturur. Bu araştırmanın evrimsel yolculuğunun bir sonraki mantıklı adımı, sistemin gerçek bir blok zinciri ağı üzerinde dağıtılmasıdır.

Gerçek dünya sensörlerine bağlanarak, sistemin pratiklik ve gerçek dünya uygulanabilirliği daha da artırılabilir. Bu heyecan verici ilerleme, farklı alanlarda ve endüstrilerde sensör verilerinin yönetiminde blok zinciri teknolojisinin tam potansiyelini açma yolunu açar.

Sonuç olarak, nesnelerin interneti ve blok zincirinin birleşimi, sensör verisi yönetimi alanında büyük umut vaat etmektedir. Blok zinciri teknolojisinin kullanıcı dostu bir web arayüzü ve akıllı sözleşmelerle entegrasyonu, verimli veri yönetimi, güvenlik ve güvenilirlik konularındaki zorluklara etkili bir çözüm sunar. Bu devrim niteliğindeki sistemın uygulanması, veri güvenliğini, erişilebilirliğini ve güvenilirliğini önemli ölçüde artırma yeteneğini göstermektedir. Daha ileri gelişmeler ve gerçek dünya uygulamaları ortaya çıktıkça, nesnelerin interneti ve blok zinciri birlikteliği, daha sürdürülebilir ve akıllı bir gelecek için büyük bir potansiyele sahip olmaya devam edecektir.

1. INTRODUCTION

With the increasing adoption of IoT devices and the rapid advancements in blockchain technology, exploring their integration is vital for creating secure, scalable, and trustworthy IoT ecosystems that can drive innovation and create new business opportunities.

1.1. Overview

The rapid proliferation of Internet of Things (IoT) devices has led to an exponential growth in data generation, revolutionizing industries and transforming our daily lives. These devices, equipped with various sensors, gather vast amounts of real-time data from the physical world, providing valuable insights and enabling innovative applications across sectors such as healthcare, transportation, agriculture, and smart cities[1, 2]. For instance, IoT devices in healthcare can monitor patients' vital signs and transmit the data to healthcare providers in real-time, facilitating remote patient monitoring and early detection of health issues. Similarly, in transportation, IoT sensors in vehicles can collect data on traffic conditions, enabling efficient traffic management and improving overall transportation systems' performance. However, the increasing volume and sensitivity of IoT sensor readings pose significant challenges in terms of data security, privacy, and integrity.

Traditional centralized storage solutions often struggle to address these concerns effectively, leaving the IoT ecosystem vulnerable to cyber threats and data manipulation [3, 4]. With centralized storage, data is stored in a single location, making it a prime target for hackers and unauthorized access. Furthermore, the centralized nature makes it difficult to ensure data integrity and prevent tampering. Blockchain technology offers a potential solution to address these challenges by providing a decentralized and tamper-proof framework for storing IoT sensor data. By leveraging cryptographic techniques and distributed consensus mechanisms, blockchain can offer a robust and transparent system for securing and maintaining the integrity of IoT data [5, 6]. The integration of blockchain technology with IoT devices has the potential to enhance data security, privacy, and immutability, thus ensuring the reliability and trustworthiness of IoT systems.

1.2. Problem Statement

The integration of IoT devices and the secure storage of their sensor readings is a critical issue in the IoT landscape. Existing centralized storage solutions face limitations in terms of scalability, security, and trust, hindering their ability to handle the vast and sensitive data generated by IoT devices [6, 7]. Scalability is a significant concern because the number of IoT devices and the data they generate continue to increase rapidly. Centralized systems struggle to scale effectively to handle this influx of data, leading to performance issues and potential data loss. Additionally, the centralized nature of these systems raises security and trust issues. A single point of failure in the centralized architecture makes the entire system vulnerable to attacks, compromising the confidentiality and integrity of IoT data.

Ensuring the security, privacy, and integrity of IoT sensor readings is crucial for maintaining the reliability and trustworthiness of IoT systems. Without robust security measures, IoT data becomes susceptible to unauthorized access, tampering, and malicious attacks, potentially leading to severe consequences such as privacy breaches, data manipulation, and compromised system functionality [8, 9] . For example, unauthorized access to medical IoT devices could result in the exposure of sensitive patient information, leading to privacy violations and identity theft. Similarly, tampering with sensor readings in critical infrastructure systems, such as transportation or energy, can disrupt operations and pose risks to public safety.

To address these challenges, the integration of blockchain technology with IoT devices offers a promising solution. Blockchain's decentralized and tamper-proof nature provides a more secure and reliable alternative to traditional centralized storage systems. By distributing data across a network of nodes and employing consensus mechanisms, blockchain ensures that data remains secure and cannot be easily altered without detection. Moreover, the transparent nature of blockchain allows for auditing and traceability of data, enhancing data integrity and trust [5, 6].

However, to effectively leverage blockchain for IoT data storage, several research questions need to be addressed, including the integration mechanisms, potential benefits, and limitations, as well as the design considerations and challenges involved in implementing blockchain-based IoT data storage systems. These research questions are critical in determining the feasibility and practicality of utilizing blockchain technology for securing IoT sensor readings and establishing a foundation for developing robust and reliable IoT systems.

1.3. Objective

The primary objective of this study is to explore the integration of blockchain technology and the Ethereum network with IoT devices to harness the combined benefits of enhanced security and integrity for sensor readings. This research aims to develop a comprehensive understanding of how these two technologies can be effectively utilized to create a robust and reliable system for storing IoT sensor data. Specifically, the objectives include:

- examining the integration mechanisms and design considerations involved in developing a smart contract on the Ethereum network for secure storage of IoT sensor readings.
- creating a web interface that seamlessly communicates with the smart contract, enabling convenient interaction with the stored sensor readings.
- evaluating the benefits and limitations of integrating blockchain technology with IoT devices for storing sensor reading.

By achieving these objectives, this research aims to contribute to the advancement of IoT systems by leveraging the security and integrity features provided by the integration of blockchain technology and the Ethereum network.

1.4. Research Questions

To guide the research process, the following research questions will be addressed:

- How can the integration of blockchain technology and the Ethereum network enhance the security and integrity of IoT sensor readings?

- How can a web interface be effectively implemented to facilitate communication with the smart contract and enable convenient interaction with the stored sensor readings?
- What are the benefits and limitations of integrating blockchain technology with IoT devices for storing sensor reading?
- In which domains and industries can this integrated system be applied effectively to improve IoT data security and integrity?
- How does the integrated system perform in terms of security, integrity, efficiency, and usability?

By addressing these research questions, this study aims to provide insights into the effective integration of blockchain technology and the Ethereum network with IoT devices, assess the advantages and limitations of this approach, explore potential application domains, and contribute to the understanding and application of secure IoT data storage solutions.

1.5. Literature Review

The following literature review examines a collection of research papers that delve into the integration of blockchain and IoT. These papers explore the diverse applications, benefits, and challenges of employing blockchain-based solutions in the realm of IoT. By analyzing these studies, we gain valuable insights into the current state of blockchain-based solutions for IoT:

"A Survey on Blockchain-Based Solutions for the Internet of Things":

This survey paper provides a comprehensive overview of blockchain-based solutions for the Internet of Things (IoT). It explores various applications and use cases where blockchain technology can enhance the security, privacy, and reliability of IoT systems. Specifically, it discusses the storage of sensor data on the blockchain as one of the potential applications. The paper highlights the benefits of using blockchain, such as immutability, decentralized consensus, and tamper resistance, to ensure the integrity and authenticity of IoT sensor data. It also examines the challenges and open research issues in integrating blockchain and IoT [7].

"Securing the Internet of Things Using Blockchain Technology":

This paper focuses on the security aspects of IoT and proposes a framework that utilizes blockchain technology to enhance data storage and access control in IoT systems. It discusses the vulnerabilities of traditional centralized architectures used in IoT and presents blockchain as a solution to address those vulnerabilities. The paper explains how sensor data can be stored on the blockchain to ensure its integrity and prevent unauthorized tampering. It also discusses the concept of smart contracts and their role in enabling secure interactions and data exchange in IoT networks [8].

"Blockchain-Enabled Fog Nodes for Secure IoT Applications":

This article introduces a framework that combines blockchain and fog computing to enhance the security and privacy of IoT applications. It explores the use of blockchain for secure data storage, retrieval, and sharing in IoT systems. The paper highlights the benefits of using fog nodes, which act as intermediary entities between IoT devices and the blockchain network, to enable efficient and secure data management. It discusses the architecture, protocols, and mechanisms involved in leveraging blockchain and fog computing for IoT security, with a focus on the storage and management of sensor data [9].

"A Blockchain-Based Data Integrity Protection Mechanism for IoT Data":

This paper presents a specific mechanism for ensuring the integrity of IoT data using blockchain technology. It proposes a distributed ledger system that employs blockchain to protect the integrity of sensor data generated by IoT devices. The paper explains how the data is hashed, signed, and stored on the blockchain to prevent tampering and provide a verifiable record of data integrity. It discusses the design and implementation details of the proposed mechanism, emphasizing the use of blockchain for data protection in IoT environments [10].

"Blockchain Solutions for IoT Security: A Review":

This review paper provides a comprehensive overview of blockchain solutions for IoT security. It covers various aspects, including data storage, access control, authentication, and privacy preservation. The paper explores different approaches and techniques used to leverage blockchain in IoT systems, highlighting their benefits, challenges, and potential applications. It provides insights into how blockchain can enhance the security and trustworthiness of IoT sensor data by ensuring data integrity, enabling secure access control, and facilitating secure interactions among IoT devices [11].

"Blockchains and Smart Contracts for the Internet of Things":

This paper explores the use of blockchain and smart contracts for securing IoT systems. It discusses how blockchain technology can provide a decentralized and trusted infrastructure for IoT data storage and management. It examines the benefits of using smart contracts to automate interactions and enforce security policies in IoT networks. The paper also discusses various blockchain architectures and their applicability to IoT, highlighting the potential advantages and challenges of integrating blockchain with the Internet of Things [12].

"A Taxonomy of Blockchain-Based Systems for Architecture Design":

This paper presents a taxonomy of blockchain-based systems and their applications. It categorizes different types of blockchain architectures, such as public, private, and consortium blockchains, and discusses their suitability for various domains, including the Internet of Things. The paper explores the architecture design considerations when integrating blockchain with IoT systems, focusing on data storage, security, and privacy aspects. It provides insights into the different blockchain-based approaches that can be used to store and secure IoT sensor data [13].

"Blockchain in Internet of Things: Challenges and Solutions":

This article addresses the challenges and solutions related to applying blockchain in IoT systems. It discusses the integration of blockchain with IoT for secure data storage, privacy preservation, and data integrity. The paper examines the scalability, performance, interoperability, and energy efficiency challenges associated with blockchain and proposes potential solutions to overcome these challenges in the context of IoT applications. It also discusses the considerations for selecting appropriate consensus mechanisms and smart contract platforms for IoT and blockchain integration [14].

"Blockchain-based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems in Smart Cities":

This paper focuses on the application of blockchain for secure and dynamic key management in intelligent transportation systems (ITS) within smart cities. It addresses the challenges in key management for heterogeneous ITS and proposes a blockchain-based solution. The paper discusses how blockchain can enhance security, privacy, and data integrity in IoT-enabled transportation systems. It highlights the relevance of blockchain in securely storing and managing IoT sensor data in the context of intelligent transportation systems [15].

"Toward Blockchain-Based Intelligent Transportation Systems":

This article explores the potential of blockchain-based intelligent transportation systems (ITS). It discusses the benefits of using blockchain for secure data sharing, transaction verification, and privacy protection in IoT-enabled transportation systems. The paper examines how blockchain technology can improve the efficiency and security of transportation systems within smart cities. It emphasizes the role of blockchain in storing and securing IoT sensor data in the context of intelligent transportation applications [16].

Table 1.1. Literature Review.

Study Title	Benefits	Challenges	Focus Areas
"A Survey on Blockchain-Based Solutions for IoT"	Overview of diverse App	Integration challenges.	Applications, security, privacy, challenges.
"Securing the IoT Using BC"	Enhancing data storage and access control.	Scalability concerns.	Security, vulnerabilities, blockchain role.

Table 1.2. (Continued) Literature Review.

Study Title	Benefits	Challenges	Focus Areas
"Blockchain-Enabled Fog Nodes for Secure IoT Applications"	Security enhancement through fog computing.	Protocol complexities.	Security, fog computing, data storage.
"A Blockchain-Based Data Integrity Mechanism for IoT"	Specific mechanism for data integrity.	Implementation details.	Data integrity, blockchain mechanism.
"Blockchain Solutions for IoT Security: A Review"	Comprehensive review of IoT security.	Implementation complexities.	Security, authentication, privacy.
"Blockchains and Smart Contracts for IoT"	Decentralization for secure IoT.	Smart contract complexity.	Decentralization, smart contracts.
"A Taxonomy of Blockchain-Based Systems for Architecture"	Taxonomy of blockchain architectures.	Design considerations.	Architecture design, suitability.
"Blockchain in IoT: Challenges and Solutions"	Addressing challenges of BC in IoT.	Scalability, interoperability.	Challenges, scalability, energy efficiency.

Table 1.3. (Continued) Literature Review.

Study Title	Benefits	Challenges	Focus Areas
"Blockchain-Based Key Management for Intelligent Transport"	Key management in intelligent transportation.	Heterogeneity challenges.	Key management, transportation systems.
"Toward Blockchain-Based Intelligent Transportation"	Potential of blockchain in transportation systems.	Integration challenges.	Transportation systems, security, privacy.

1.6. Organization

This document is organized into several sections to provide a clear and coherent presentation of the research conducted. The following sections outline the structure and content of each chapter:

1. Introduction: This chapter provides an overview of the research project, including the problem statement, objectives, research questions, and a review of the relevant literature.
2. Theoretical Background: In this chapter, the theoretical foundations of the study are discussed. It covers an introduction to blockchain technology, including its characteristics, basic elements, types, and an overview of Ethereum. Additionally, it explores the concept of the Internet of Things (IoT), its importance, architecture, and challenges. The chapter concludes by examining the impact of blockchain technology on IoT.

3. Tools and Libraries: This chapter focuses on the tools and libraries used in the implementation of the research project. It provides an overview of NPM and Node.js, Ganache, Truffle, Ethers.js, as well as HTML, CSS, and JavaScript.
4. Implementation: This chapter delves into the implementation details of the research project. It discusses the development of the smart contract, the creation of the web interface, and the implementation of JavaScript functions.
5. Results and Discussion: This chapter presents the results obtained from the research project and provides a comprehensive analysis and discussion of those results. It explores the findings in relation to the research objectives and research questions.
6. Conclusion and Recommendations: This chapter summarizes the main findings of the study and draws conclusions based on the results. It also offers recommendations for future work and further research in the field.

The document concludes with a References section that lists all the sources cited throughout the document

2. THEORETICAL BACKGROUND

2.1. Blockchain Technology

2.1.1. Overview of blockchain

Blockchain technology is a distributed ledger system that enables secure and transparent record-keeping of transactions across multiple parties. It gained prominence with the advent of Bitcoin in 2009, introduced by the pseudonymous individual or group known as Satoshi Nakamoto [20]. Since then, blockchain has evolved beyond cryptocurrencies and found applications in various industries.

At its core, a blockchain is a chain of blocks, with each block containing a list of transactions. These transactions are verified, recorded, and linked together using cryptographic algorithms, ensuring their immutability and integrity [21]. Blockchain operates on a decentralized network, where multiple participants, known as nodes, collectively maintain and validate the ledger [22].

One of the key features of blockchain is its decentralized consensus mechanism. Instead of relying on a central authority, blockchain achieves consensus through consensus protocols like Proof-of-Work (PoW) or Proof-of-Stake (PoS). PoW, introduced in the Bitcoin blockchain, involves miners competing to solve complex mathematical puzzles to validate transactions and add them to the blockchain [23]. PoS, on the other hand, selects validators based on their stake in the network, reducing the energy consumption associated with PoW [24].

Blockchain technology offers several advantages. Its transparency allows participants to view all transactions stored on the ledger, fostering trust and accountability [22] . The immutability of blockchain ensures that once a transaction is recorded, it cannot be altered without the consensus of the network [21]. This feature enhances data integrity and can be particularly useful in applications where tamper-proof records are critical.

The structure of a blockchain ensures robust transaction security by incorporating key elements. Each block within the blockchain possesses its own distinct identification, originality, and includes a cryptographic hash of the preceding block [25]. This arrangement guarantees the integrity of transactions. Furthermore, network participants verify each transaction, leading to its inclusion and subsequent logging in the blockchain. The chronological order of transactions, along with their accompanying timestamps, enhances the reliability of the system. Importantly, the immutability of recorded transactions stems from their direct linkage to the preceding block, rendering any modifications practically impossible. the use of this structured approach underscores the blockchain's reputation as a reliable and secure technology[26].

Moreover, blockchain technology enables programmable contracts known as smart contracts. Smart contracts are self-executing agreements with the terms of the contract directly written into the code [27]. They automate the execution and enforcement of agreements, eliminating the need for intermediaries and reducing costs [22].

While blockchain technology has gained significant attention, it also faces challenges such as scalability, privacy, and regulatory considerations [28]. However, ongoing research and development aim to address these issues and unlock the full potential of blockchain in various sectors.

Basically, blockchain technology provides a decentralized and secure framework for recording and validating transactions. With its transparent and immutable nature, it has the potential to revolutionize industries beyond finance. As the technology continues to evolve, further exploration and adoption of blockchain are expected to reshape how we interact and transact in the digital world.

2.1.2. Blockchain characteristics

Blockchain technology is characterized by several key features that contribute to its unique properties and functionalities:

Decentralization: One of the fundamental characteristics of blockchain is its decentralized nature. Instead of relying on a central authority or intermediary, blockchain operates through a distributed network of nodes. This decentralized architecture ensures that no single entity has control over the entire system, promoting transparency, resilience, and reducing the risk of single points of failure [20].

Transparency and Immutability: Blockchain offers transparency by providing a public ledger that records all transactions and data exchanges. Once recorded, the data is nearly impossible to alter or tamper with, thanks to cryptographic hashing and the consensus mechanism used to validate and confirm transactions. This immutability enhances trust, accountability, and auditability within the blockchain network [20, 24].

Security: Blockchain leverages cryptographic techniques to ensure the security of data and transactions. Each transaction is digitally signed, and the decentralized consensus mechanism verifies and validates the integrity of the transactions. Additionally, the distributed nature of blockchain and its consensus protocols make it highly resilient to malicious attacks [20, 24].

Trust and Verifiability: Blockchain technology enables trust among participants by eliminating the need for intermediaries and relying on transparent, verifiable transactions. The decentralized consensus mechanism ensures that all participants reach a shared agreement on the validity of transactions, removing the need for trust in a centralized authority [20, 24].

Tamper Resistance: Once a transaction is recorded on the blockchain, it becomes extremely difficult to alter or delete. The immutability of the blockchain prevents unauthorized modifications, providing a tamper-resistant and reliable record of transactions and data [20].

Smart Contracts: Smart contracts are self-executing contracts with predefined rules and conditions written into the blockchain. They automate and enforce the execution of agreements, eliminating the need for intermediaries and enhancing the efficiency of transactions. Smart contracts enable trustless and autonomous interactions between parties, ensuring that the agreed-upon conditions are met before any actions are executed [24].

Privacy: While blockchain is often associated with transparency, there are also mechanisms for preserving privacy. Techniques such as encryption and zero-knowledge proofs can be employed to protect sensitive information while still maintaining the integrity and security of the blockchain [24].

Interoperability: Blockchain technology has the potential to enable interoperability between different systems and platforms. By establishing common standards and protocols, blockchain networks can facilitate seamless data exchange and collaboration across disparate systems, enhancing efficiency and reducing friction in various industries [25].

2.1.3. Blockchain basic elements

The blockchain basic elements are showen in Figure 2.

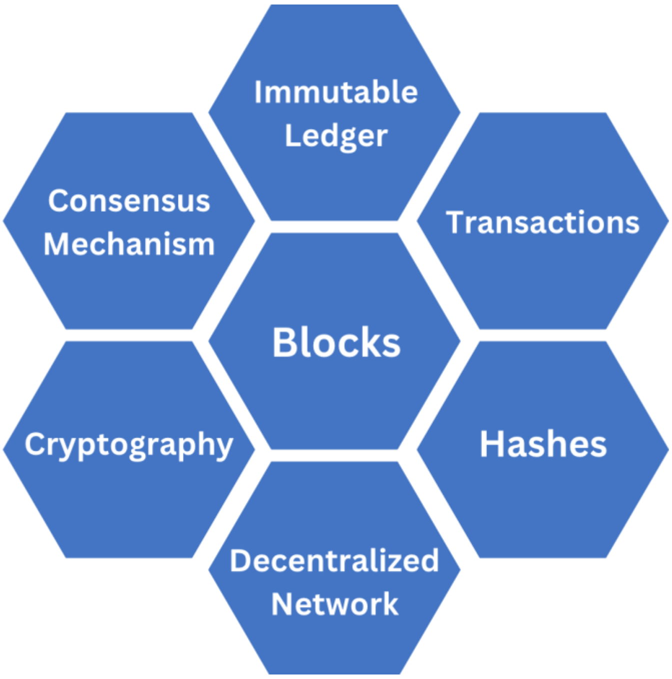


Figure 2.1. Blockchain Elements.

Blocks: Each block contains a collection of transactions. It serves as a unit of data storage and has a unique identifier and linked together in a specific order to form a chain. Each block contains the hash of the previous block, creating a chronological sequence of blocks.

Transactions: Transactions represent the exchange of data or assets between participants in the blockchain network. They are recorded and stored in blocks.

Hashes: Each block contains a cryptographic hash, which is a unique alphanumeric string generated by applying a hash function to the data within the block. The hash ensures the integrity and security of the block.

Decentralized Network: Blockchain operates on a decentralized network of nodes, where multiple participants maintain copies of the blockchain and validate transactions. This decentralized structure ensures trust and security.

Immutable Ledger: Once a block is added to the blockchain, its contents cannot be altered or deleted. This immutability ensures the integrity and reliability of the recorded data.

Cryptography: Blockchain relies on cryptographic algorithms to secure and authenticate transactions and participants' identities. Public-private key pairs and digital signatures are commonly used cryptographic techniques in blockchain systems

Consensus Mechanism: Consensus mechanisms establish agreement among participants on the validity and order of transactions. There are Different consensus listed as follows:

- Proof of Work (PoW) is a consensus mechanism used by Bitcoin and Ethereum 1.0. It involves a competition among all nodes to construct blocks by solving mathematical puzzles known as mining. Transaction fees in PoW are determined based on the supply and demand of transactions, with miners prioritizing those with higher fees. However, PoW has the drawback of being expensive in terms of computational power, which can be a disincentive for miners if the value of awarded coins drops below the energy costs. This mechanism is widely known but costly[29].
- Proof of Stake (PoS), on the other hand, does not require high computational power. In PoS, validators' mining rewards and influence over the network are proportional to the number of coins they hold and lock. This mechanism is significantly cheaper than PoW, resulting in lower transaction fees[29]. Examples of blockchains utilizing PoS include Ethereum 2.0, Cardano, Solana, and Polkadot.

Other consensus mechanisms such as Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Elapsed Time, Proof of Weight, Proof of Burn, Proof of Capacity, and Proof of Space also exist, but they are not as widely adopted as PoW and PoS.

2.1.4. Blockchain types

There are 4 types of blockchains available :

1. Public Blockchain: This type is open to anyone and allows anyone to participate in the network, validate transactions, and create new blocks.

Examples include Bitcoin and Ethereum. These blockchains are decentralized and provide a high level of transparency and security [20].

2. Private Blockchain: this type is restricted to a specific group of participants who are given permission to access and validate transactions. These blockchains are often used by organizations to maintain control over the network and keep sensitive data private [24].
3. Consortium Blockchain: This type is governed by a consortium or group of organizations that collectively make decisions about the network. These blockchains offer a balance between the openness of public blockchains and the control of private blockchains. Consortium members validate transactions and maintain the network's integrity [29].
4. Hybrid Blockchain: this type combines elements of both public and private blockchains. They allow for a public-facing layer where certain transactions and data can be shared openly, while also maintaining a private layer for sensitive or confidential information. Hybrid blockchains provide flexibility and can be tailored to specific use cases [22].

2.1.5. Ethereum

Ethereum is a decentralized, open source blockchain platform that enables the creation and execution of smart contracts and decentralized applications (DApps) [25]. Proposed by Vitalik Buterin in 2013 and launched in 2015, Ethereum aims to provide a platform for developers to build and deploy smart contracts, which are self-executing contracts with predefined rules and conditions [25, 30].

One of the key features of Ethereum is its ability to execute Turing-complete code, allowing for complex computational tasks [22]. This feature sets Ethereum apart from Bitcoin, which primarily serves as a digital currency with limited scripting capabilities [22]. Ethereum operates through a decentralized network of nodes that collectively validate and record transactions [31].

Ethereum has its native cryptocurrency called Ether (ETH), which serves as both a medium of exchange and an incentive for participants in the network [4]. Ether is used as "gas" to pay for computational resources required to execute smart contracts on the Ethereum Virtual Machine (EVM), the runtime environment for smart contracts on the Ethereum network [25].

Developers can build decentralized applications on the Ethereum platform using programming languages like Solidity. Solidity is specifically designed for writing smart contracts and is the primary language used in Ethereum development. DApps built on Ethereum can range from financial applications like decentralized exchanges and lending platforms to gaming, decentralized governance systems, and more [25].

Ethereum's vision extends beyond financial applications, aiming to provide a decentralized infrastructure for various industries [25]. It enables secure and transparent interactions, eliminates the need for intermediaries, and fosters innovation using smart contracts and blockchain technology [25].

In summary, Ethereum is a decentralized blockchain platform that enables the creation and execution of smart contracts and DApps [25]. With its ability to execute Turing-complete code, Ether cryptocurrency, and support for various programming languages, Ethereum provides a flexible and robust platform for decentralized innovation [25].

2.2. Internet of Things

2.2.1. Overview about internet of things

The Internet of Things (IoT) refers to a vast network of interconnected physical objects or "things" that are embedded with sensors, software, and connectivity capabilities, enabling them to collect and exchange data over the internet [32]. These objects can range from everyday devices such as smartphones, wearables, and home appliances to more complex systems like industrial machinery, transportation systems, and smart cities.

The IoT ecosystem consists of several key components. First, there are the physical objects themselves, which are equipped with sensors and actuators to capture data from the surrounding environment and interact with it. Next, there is the connectivity layer that enables these objects to communicate with each other and with cloud-based platforms or other computing systems [33]. This connectivity can be achieved through various means, including Wi-Fi, Bluetooth, cellular networks, or specialized IoT protocols.

The collected data from IoT devices is transmitted to cloud-based platforms or edge computing systems, where it is stored, processed, and analyzed [34]. Advanced analytics techniques, such as machine learning and artificial intelligence, can be applied to derive valuable insights from the data, enabling informed decision-making and automation.

The applications of IoT span across various domains and industries. In the healthcare sector, IoT devices can be used for remote patient monitoring, medication adherence tracking, and emergency response systems [35]. In agriculture, IoT sensors can monitor soil moisture levels, weather conditions, and crop health, enabling optimized irrigation and resource management [37]. Smart homes leverage IoT devices to automate lighting, temperature control, and security systems, enhancing convenience and energy efficiency [32].

Industrial applications of IoT, often referred to as Industrial Internet of Things (IIoT) or Industry 4.0, include predictive maintenance, asset tracking, supply chain optimization, and real-time monitoring of manufacturing processes [38]. Smart cities utilize IoT technologies to enhance urban services, including smart transportation systems, waste management, and energy optimization [33].

Despite its vast potential, the IoT faces several challenges. Security and privacy concerns are major considerations due to the sheer volume of data generated and exchanged by IoT devices [39]. Interoperability and standardization issues arise from the multitude of devices and communication protocols used in the IoT ecosystem [40]. Scalability and managing the massive influx of data from billions of connected devices pose additional challenges [36].

Looking ahead, the future of IoT holds immense possibilities. As advancements in technology continue, we can expect increased connectivity, improved data analytics capabilities, and more sophisticated IoT applications. The integration of 5G networks will provide higher bandwidth and lower latency, enabling real-time communication and supporting applications that demand instant responsiveness [34]. Edge computing will become more prevalent, allowing data processing and analysis to occur closer to the source, reducing latency and improving efficiency [34].

Basically, the Internet of Things (IoT) represents a transformative technology that connects physical objects to the digital world, enabling data-driven insights, automation, and innovation across various industries. It offers a plethora of applications, ranging from healthcare and agriculture to smart homes and industrial automation. However, challenges related to security, interoperability, and scalability need to be addressed to fully unlock the potential of IoT.

2.2.2. Importance of internet of things

The Internet of Things (IoT) holds significant importance in today's world due to its transformative impact on various aspects of our lives. Here are some key reasons highlighting the importance of IoT:

- Enhanced Efficiency and Automation: IoT enables the seamless integration of physical devices with digital systems, allowing for automation and improved efficiency across industries. Connected devices gather and transmit data, enabling real-time monitoring, predictive analytics, and intelligent decision-making [32]. This leads to streamlined processes, reduced manual intervention, and optimized resource utilization.
- Improved Quality of Life: IoT technology brings convenience and improved quality of life to individuals. Smart homes equipped with IoT devices allow for remote control of appliances, lighting, security systems, and temperature, enhancing comfort and energy efficiency [33]. Wearable IoT devices enable personalized health monitoring, fitness tracking, and timely medical interventions [34]. IoT-based assistive technologies also benefit people with disabilities, providing them with greater independence and accessibility [37].
- Advanced Healthcare and Well-being: IoT has the potential to revolutionize the healthcare industry. Connected medical devices and wearables enable remote patient monitoring, early detection of health issues, and personalized treatment plans [34]. IoT-enabled systems facilitate telemedicine, connecting patients with healthcare professionals regardless of geographic location [39]. This technology also supports efficient management of healthcare facilities and inventory, enhancing patient care and reducing costs [40].
- Smart Cities and Sustainable Development: IoT plays a crucial role in the development of smart cities, where connected devices and sensors enhance the efficiency of urban services. IoT-based solutions enable smart transportation systems, efficient energy management, optimized waste management, and intelligent infrastructure [41]. By monitoring and analyzing data from various

sources, cities can make informed decisions to improve sustainability, reduce traffic congestion, and enhance public safety [36].

- Industrial Transformation: The Industrial Internet of Things (IIoT) drives digital transformation in industries by connecting machines, equipment, and systems. IIoT enables predictive maintenance, real-time monitoring of production processes, and optimized supply chain management [35]. This technology increases productivity, minimizes downtime, and improves overall operational efficiency, leading to cost savings and better competitiveness [36].
- Environmental Sustainability: IoT contributes to environmental sustainability by enabling smart energy management, efficient resource utilization, and environmental monitoring. Connected sensors can monitor air and water quality, detect environmental hazards, and facilitate early warning systems for natural disasters [38]. IoT-based solutions promote smart agriculture, optimizing water usage, crop monitoring, and reducing wastage, contributing to sustainable farming practices [37].
- Data-driven Insights and Innovation: IoT generates massive amounts of data from connected devices, which, when properly analyzed, provide valuable insights for businesses, policymakers, and researchers. The analysis of IoT data using advanced analytics techniques such as machine learning and artificial intelligence can uncover patterns, trends, and correlations, driving innovation and informed decision-making in various domains [33].

The Internet of Things holds immense importance as it revolutionizes industries, improves efficiency, enhances quality of life, and promotes sustainability. However, addressing challenges related to security, privacy, interoperability, and scalability is crucial to fully harness the potential of IoT and ensure its responsible and ethical deployment.

2.2.3. Architecture of internet of things

The architecture of the Internet of Things (IoT) consists of several layers and components that work together to enable connectivity, data exchange, and functionality.

The Internet of Things (IoT) architecture consists of five essential layers, as the following[42]:

- Perception Layer: This layer involves the use of sensors at the physical level to detect and gather data about the surrounding environment [43]. Various types of sensors, such as temperature and motion sensors, capture real-world data and convert it into digital signals for further processing.
- Data Link Layer: The data link layer employs different protocols, including Bluetooth, ZigBee, Wi-Fi, and others, to establish communication between devices and facilitate data transmission to the network layer [44]. These protocols ensure efficient and reliable data transfer within the IoT ecosystem.
- Network Layer: Responsible for assigning data pathways for transmission across the network, the network layer incorporates switches, routers, firewalls, and other networking equipment [45]. These components enable proper connectivity and communication among IoT devices.
- Transport Layer: The transport layer provides crucial functions such as packet delivery, multiplexing, congestion avoidance, and data integrity. It ensures that data packets are effectively delivered to their intended destinations and that the transmitted data remains reliable [45].
- Application Layer: Serving as the front end of the IoT architecture, the application layer offers interfaces, platforms, and tools for developers to create various IoT applications, such as smart cities, smart health systems, intelligent transportation, and smart homes [45]. This layer enables data processing, analytics, and the development of innovative IoT services.

2.2.4. Challenges for internet of things

Internet of Things (IoT) systems face several challenges related to data integrity, security, immutability, and privacy by understanding these challenges we can design an efficient and robust blockchain-based solutions for IoT. Let's discuss each of these challenges in more detail:

- Data integrity is crucial in IoT systems to ensure the accuracy and consistency of data. Data corruption, loss during transmission, and unauthorized modifications are key challenges in maintaining data integrity. Techniques such as checksums and digital signatures have been proposed to address these challenges and ensure data integrity [46, 47]. By adding IoT data to a blockchain, each data transaction is recorded as an immutable and timestamped block [48]. The decentralized nature of the blockchain ensures that data cannot be altered or tampered with without detection. Thus, integrating IoT data into a blockchain enhances data integrity by providing a transparent and verifiable record of all data transactions.

- Security is a major concern in IoT due to the interconnected nature of devices and potential vulnerabilities. Unauthorized access, data breaches, and malicious attacks pose significant threats to IoT systems [49, 50]. Integration with Blockchain technology offers inherent security features that can benefit IoT systems. The use of cryptographic algorithms and consensus mechanisms ensures that the data stored in the blockchain is protected from unauthorized access and manipulation [51]. Moreover, the decentralized nature of the blockchain reduces the risk of a single point of failure and enhances overall system security.
- Immutability of IoT data is essential for maintaining its integrity and trustworthiness. Immutable data prevents unauthorized modifications and provides a reliable audit trail. Blockchain technology has been explored as a solution to create tamper-proof and immutable records, adding an additional layer of trust to IoT data [52, 53].this done by creating a chain of blocks, where each block contains a cryptographic hash of the previous block [48]. Any attempt to modify the data in a block would require recalculating the hash of subsequent blocks, which would be computationally infeasible.
- Privacy challenges arise due to the vast amount of personal and sensitive data generated by IoT systems. Protecting user privacy, controlling data collection and sharing, and complying with regulations like the General Data Protection Regulation (GDPR) are critical [54, 55]. Integrating IoT data with blockchain can address privacy concerns by allowing for secure and decentralized data sharing [52]. Blockchain-based smart contracts can enforce data access controls and privacy settings, ensuring that only authorized entities can access specific data. Additionally, privacy-enhancing techniques like zero-knowledge proofs or private transactions can be implemented to protect sensitive information.
- Tamper protection is important to safeguard IoT devices against physical tampering, which can compromise their functionality and security. Unauthorized access, sensor tampering, and data manipulation are potential

risks [56, 57]. Blockchain technology can provide tamper protection by leveraging its decentralized consensus mechanism [51]. Any attempt to tamper with data recorded on the blockchain would require controlling a majority of the network's computing power, making it highly difficult and economically infeasible. This distributed consensus ensures the integrity and security of IoT data, even in the presence of malicious actors.

2.3. Exploring the Impact of Blockchain Technology on IoT

This section investigates the diverse range of applications and use cases where the combination of blockchain and IoT can yield significant benefits.

Supply Chain Management: Blockchain can provide transparency and traceability in supply chain management by securely recording and tracking the movement of goods from the source to the end consumer [58]. It enables real-time visibility, reduces counterfeiting and fraud, and enhances trust among participants in the supply chain ecosystem.

The figure 2.2 shows BIOT Architecture in Supply Chain Management [59].

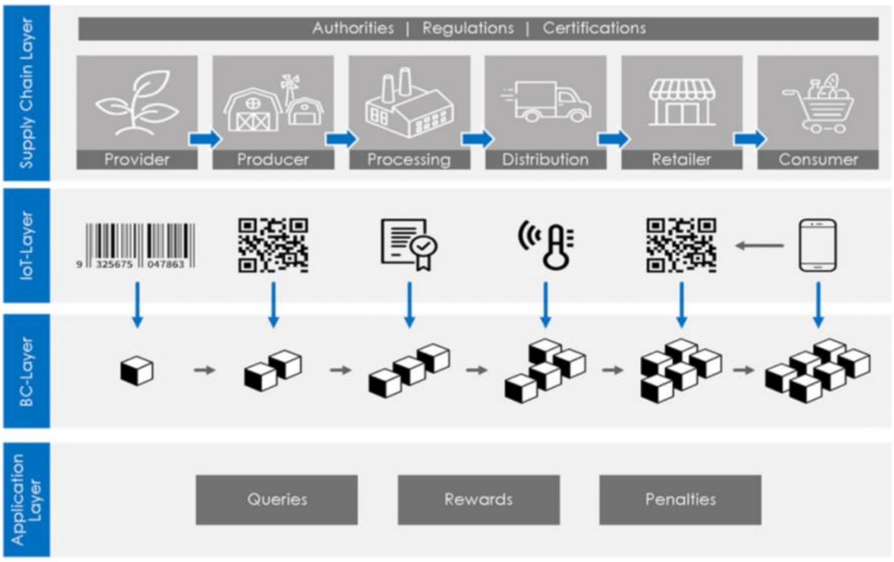


Figure 2.2. BIOT Architecture in Supply Chain Managment [59].

Smart Energy Grids: Blockchain can facilitate peer-to-peer energy transactions and enable the decentralized exchange of energy between producers and consumers in smart grids [60]. It enables secure and transparent energy trading, optimizes energy distribution, and incentivizes the adoption of renewable energy sources.

The figure 2.3 shows BIOT Architecture in Smart Energy grid [61].

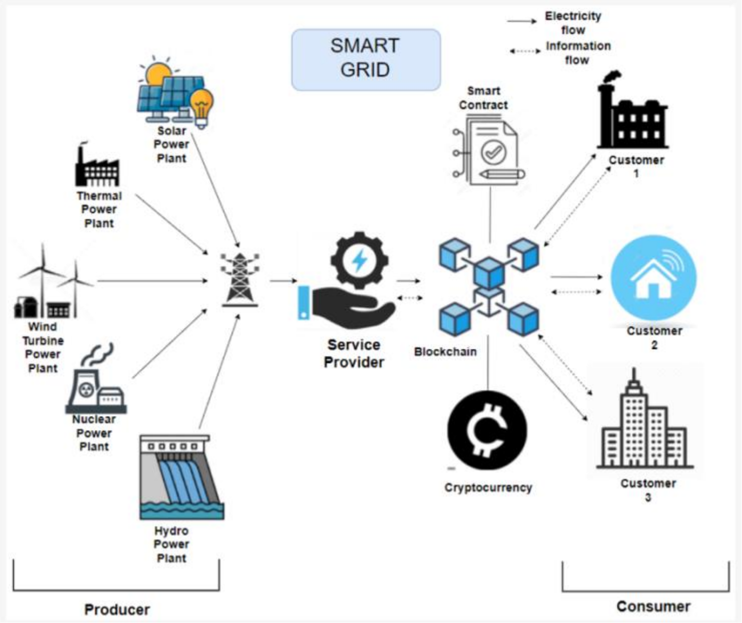


Figure 2.3. BIOT Architecture in Smart Energy grid [61].

Healthcare Data Management: Blockchain can improve the management and sharing of sensitive healthcare data while ensuring privacy and security [62]. It enables patients to have control over their medical records, facilitates secure data sharing between healthcare providers, and enhances interoperability in healthcare systems.

The figure 2.4 shows BIOT Architecture in Healthcare [63].

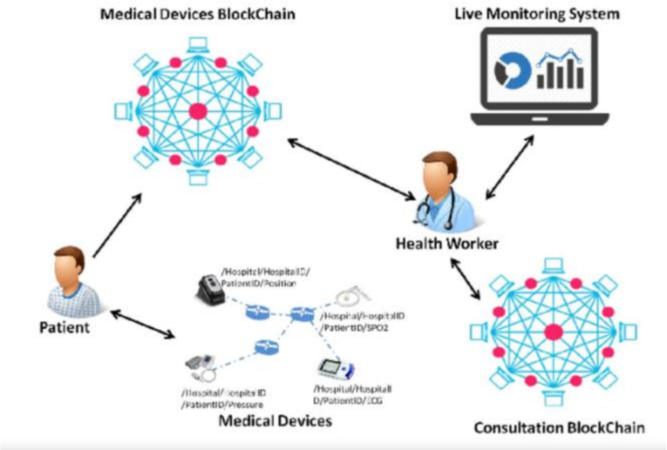

Medical Devices BlockChain
Live Monitoring System
Health Worker
Patient
/Hospitel/HospitalID/ PatientID/Position
/Hospital/HospitalID /PatientID/SPO2
/Hospital/HospitalID /PatientID/Pressure
/Hospital/HospitalID/PatientID/ECG
Medical Devices
Consultation BlockChain

Figure 2.4. BIOT Architecture in Healthcare [63].

Smart Home Automation: Blockchain can enhance security and privacy in smart home automation by providing a decentralized and tamper-resistant platform [64]. It enables secure control and management of IoT devices, protects user data, and facilitates trusted interactions between devices and service providers.

The figure 2.5 shows BIOT Architecture in Smart Home [65].

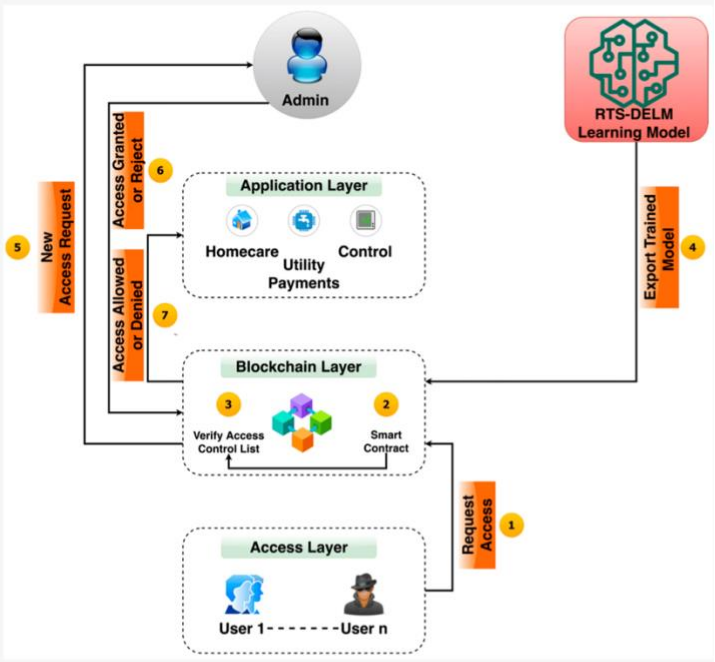


Figure 2.5. BIOT Architecture in Smart Home [65].

Autonomous Vehicles: Blockchain can support the secure and decentralized exchange of data in autonomous vehicle networks [66]. It enables secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, enhances data integrity and trust, and facilitates the development of new mobility and transportation models. The figure 2.6 shows BIOT Architecture in Autonomous Vehicles [67].

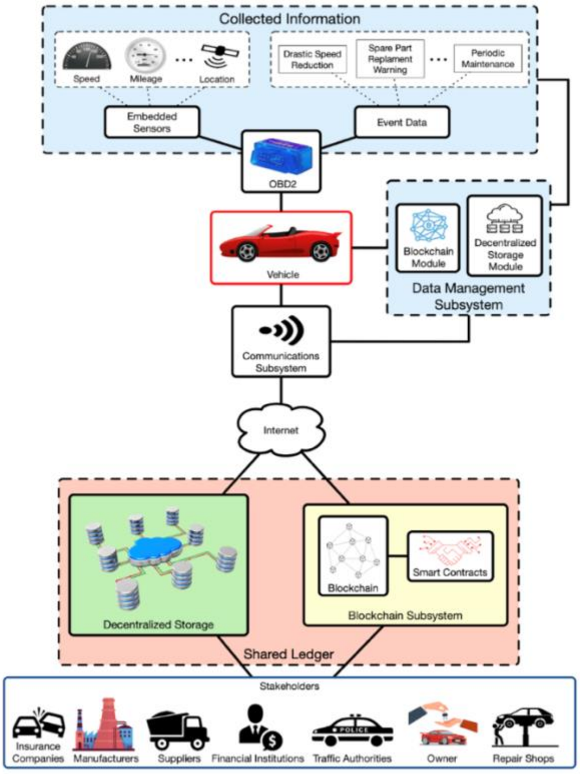


Figure 2.6. BIOT Architecture in Autonomous Vehicles [67].

Agriculture and Food Traceability: Blockchain can improve transparency and traceability in the agricultural and food industry by recording and verifying the origin, quality, and safety of products [68]. It enables consumers to verify the authenticity of food products, reduces food fraud, and promotes sustainable and ethical practices in the supply chain. The figure 2.7 shows BIOT Architecture in Food Traceability [69].

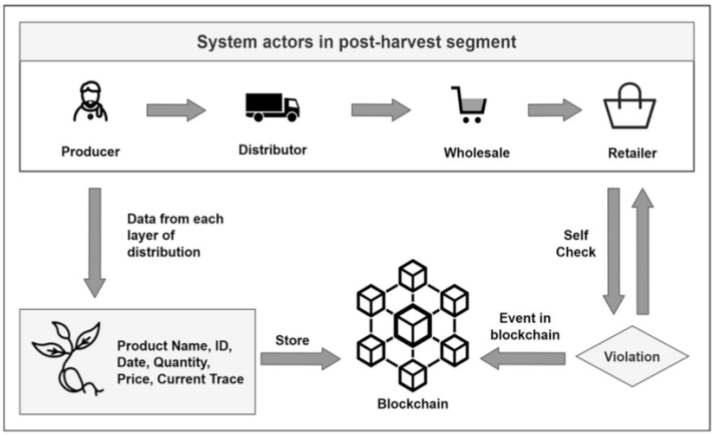

System actors in post-harvest segment
Producer
Distributor
Wholesale
Retailer
Data from each layer of distribution
Self Check
Product Name, ID, Date, Quantity, Price, Current Trace
Store
Blockchain
Event in blockchain
Violation

Figure 2.7. BIOT Architecture in Food Traceability [69].

Smart City Management: Blockchain technology can be leveraged to enhance the management and efficiency of smart cities. By integrating blockchain with IoT devices and systems, cities can create decentralized and secure platforms for data exchange, citizen engagement, and service delivery [70]. Blockchain can enable secure and transparent transactions for services such as transportation, energy management, waste management, and more. It facilitates the development of decentralized identity systems, improves data privacy, and fosters citizen empowerment in shaping the future of their cities. Additionally, blockchain can be utilized for storing sensor data generated by IoT devices in a secure and immutable manner, ensuring data integrity and enabling trusted analysis and decision-making processes. The figure 2.8 shows BIOT Architecture in Smart city [71].

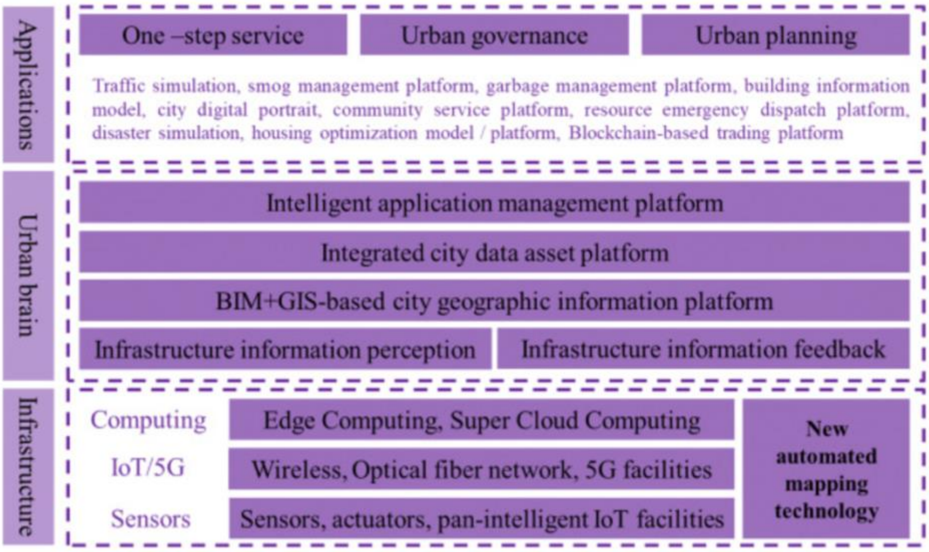

Applications
One –step service
Urban governance
Urban planning
Traffic simulation, smog management platform, garbage management platform, building information model, city digital portrait, community service platform, resource emergency dispatch platform, disaster simulation, housing optimization model / platform, Blockchain-based trading platform
Urban brain
Intelligent application management platform
Integrated city data asset platform
BIM+GIS-based city geographic information platform
Infrastructure information perception
Infrastructure information feedback
Infrastructure
Computing
Edge Computing, Super Cloud Computing
IoT/5G
Wireless, Optical fiber network, 5G facilities
Sensors
Sensors, actuators, pan-intelligent IoT facilities
New automated mapping technology

Figure 2.8. BIOT Architecture in Smart City [71].

Waste Management and Recycling: Blockchain can streamline waste management processes by creating a transparent and auditable system for tracking waste disposal, recycling, and waste-to-energy processes [72]. It enables the verification of waste origins, ensures proper waste treatment, and incentivizes recycling efforts. Blockchain-based platforms can also encourage participation from citizens and businesses by providing rewards for responsible waste management practices. The figure 2.9 shows BIOT Architecture in Waste Management [73].

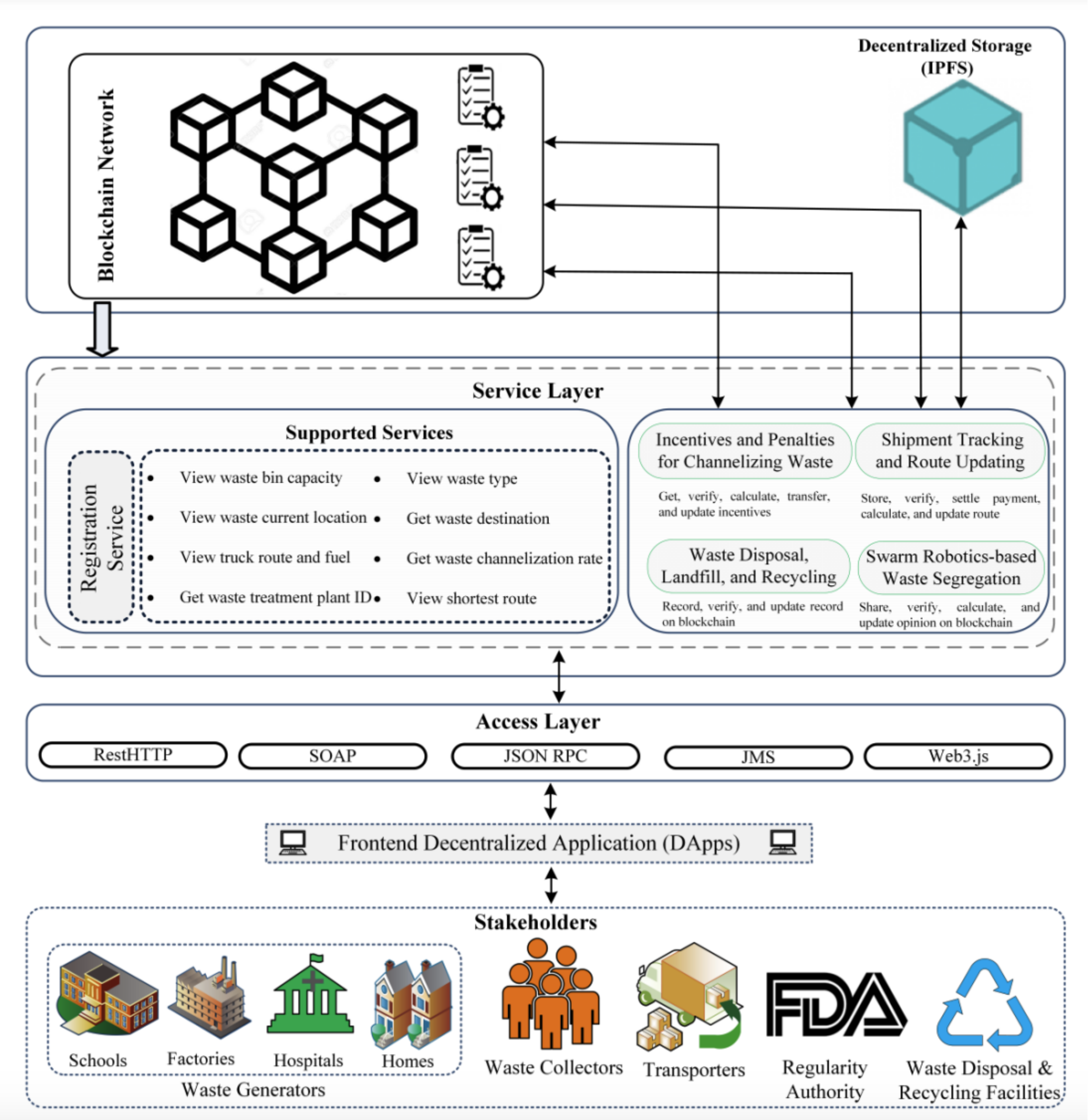

Blockchain Network
Decentralized Storage (IPFS)
Service Layer
Supported Services
Registration Service
View waste bin capacity
View waste type
View waste current location
Get waste destination
View truck route and fuel
Get waste channelization rate
Get waste treatment plant ID
View shortest route
Incentives and Penalties for Channelizing Waste
Get, verify, calculate, transfer, and update incentives
Shipment Tracking and Route Updating
Store, verify, settle payment, calculate, and update route
Waste Disposal, Landfill, and Recycling
Record, verify, and update record on blockchain
Swarm Robotics-based Waste Segregation
Share, verify, calculate, and update opinion on blockchain
Access Layer
RestHTTP
SOAP
JSON RPC
JMS
Web3.js
Frontend Decentralized Application (DApps)
Stakeholders
Schools
Factories
Hospitals
Homes
Waste Generators
Waste Collectors
Transporters
Regularity Authority
Waste Disposal & Recycling Facilities

Figure 2.9. BIOT Architecture in Waste Managment [73].

Citizen Identity and Services: Blockchain technology can offer secure and decentralized identity management systems for citizens in smart cities. By storing citizen identity information on the blockchain, individuals can have control over their personal data and selectively grant access to various services [74]. Blockchain-based identity systems enhance data privacy, reduce identity theft risks, and enable seamless access to smart city services. The figure 2.10 shows BIOT Architecture in Citizen Identity [75].

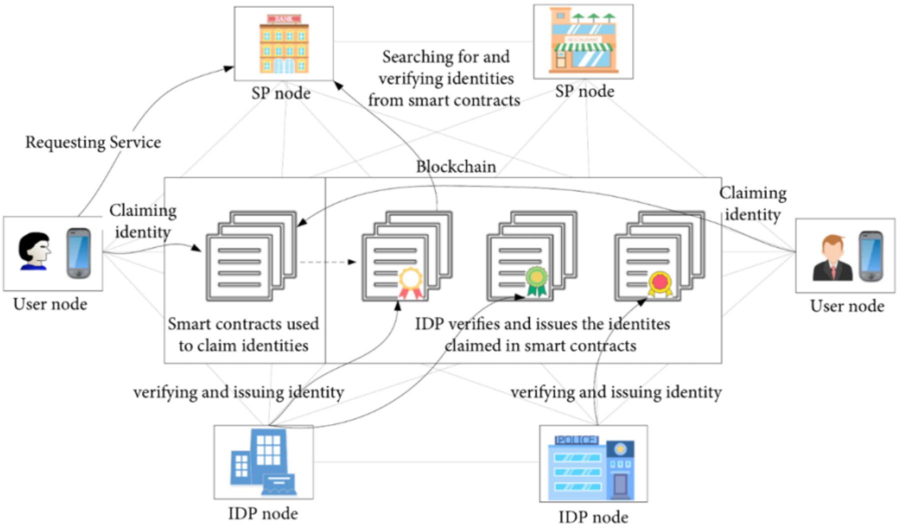

SP node
Searching for and verifying identities from smart contracts
SP node
Requesting Service
Blockchain
Claiming identity
Claiming identity
User node
User node
Smart contracts used to claim identities
IDP verifies and issues the identites claimed in smart contracts
verifying and issuing identity
verifying and issuing identity
IDP node
IDP node

Figure 2.10. BIOT Architecture in Citizen Identity [75].

Urban Planning and Governance: Blockchain can support transparent and participatory urban planning processes by providing immutable records of land ownership, property transactions, and development permits [76]. It facilitates trust and transparency between various stakeholders, including governments, urban planners, developers, and citizens. Blockchain can also enable decentralized governance models, allowing for more inclusive decision-making and accountability in the development and management of smart cities.

3. TOOLS AND LIBRARIES

The setup of a virtual Ethereum network for running smart contracts involves the utilization of various software and libraries to create a simulated environment that mimics the Ethereum blockchain. This chapter focuses on exploring the essential tools and libraries used in this process. By setting up a virtual Ethereum network, developers can test and deploy smart contracts in a controlled and isolated environment, enabling them to experiment, debug, and ensure the stability and functionality of their contracts before deploying them to the live Ethereum network.

3.1. NPM & Node.js

NPM and Node.js play a crucial role in the development and integration of blockchain-related functionalities and applications. They provide the necessary tools, libraries, and frameworks for working with blockchains.

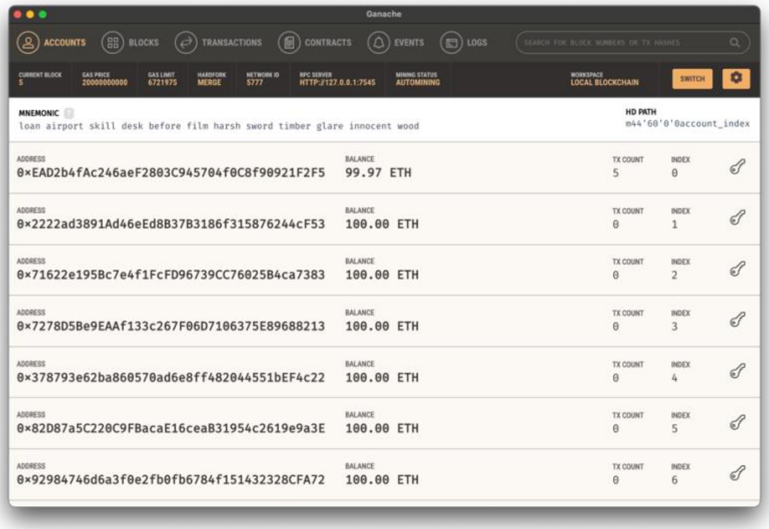
NPM stands for "Node Package Manager." It is a package manager for the JavaScript programming language, primarily used in the Node.js runtime environment. NPM allows developers to easily manage and install reusable code modules, known as packages or libraries, which can be integrated into their Node.js projects. NPM provides a command-line interface that allows developers to search for packages, install them, and manage their dependencies. It also facilitates version control and allows developers to publish their own packages to the NPM registry for others to use.

On the other hand, Node.js is an open-source, server-side JavaScript runtime environment that allows developers to run JavaScript code outside of a web browser. It's built on the V8 JavaScript engine, making it efficient and scalable for building applications like web servers, APIs, and real-time services. Node.js uses an event-driven, non-blocking I/O model, enabling it to handle concurrent connections with low overhead. With its extensive library ecosystem and the ability to share code between server and client-side, Node.js is widely used for building efficient and versatile applications [77, 78].

3.2. Ganache

Ganache is a local development blockchain that allows you to create a personal Ethereum network for testing and development purposes. It provides a user-friendly interface and generates test accounts with pre-funded Ether. Ganache is available as a desktop application and a command-line tool [79].

Main interface : upon creating a workspace, users are provided with server details and a list of accounts (see figure 3.1), each equipped with 100 ethers. This pre-allocated ether in all accounts allows developers to focus on application development without the concern of initial funding. It streamlines the process, enabling seamless testing and deployment of smart contracts within the workspace environment.



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
5	20000000000	6721975	MERGE	5777	HTTP://127.0.0.1:7545	AUTOMINING	LOCAL BLOCKCHAIN

MNEMONIC
loan airport skill desk before film harsh sword timber glare innocent wood

HD PATH
m44'60'0'0account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×EAD2b4fAc246aeF2803C945704f0C8f90921F2F5	99.97 ETH	5	0
0×2222ad3891Ad46eEd8B37B3186f315876244cF53	100.00 ETH	0	1
0×71622e195Bc7e4f1FcFD96739CC76025B4ca7383	100.00 ETH	0	2
0×7278D5Be9EAAf133c267F06D7106375E89688213	100.00 ETH	0	3
0×378793e62ba860570ad6e8ff482044551bEF4c22	100.00 ETH	0	4
0×82D87a5C220C9FBacaE16ceaB31954c2619e9a3E	100.00 ETH	0	5
0×92984746d6a3f0e2fb0fb6784f151432328CFA72	100.00 ETH	0	6

Figure 3.1. Ganache Main Screen.

The figure 3.1 shows six tabs available:

- Accounts shows each account generated with the address and the balance of it.
- Blocks shows each block mined on the blockchain, with the gas used and transactions.
- Transactions shows all transactions run against the blockchain.
- Contracts shows the contracts contained in Truffle projects workspace.
- Events shows all events that have been triggered since this workspace's creation.
- Logs shows the logs for the server, which it uses for debugging.

3.3. Truffle

Truffle is a development framework and tool suite for Ethereum-based smart contract development. It simplifies the process of building, deploying, and testing smart contracts by providing utilities, libraries, and command-line tools. With Truffle, developers can compile and migrate contracts, write automated tests, manage networks, interact with contracts using a JavaScript API, handle asset management, and integrate with other Ethereum tools. It streamlines the development workflow and enhances productivity for decentralized application (dApp) development [80].

3.4. Ethers.js

Ethers.js is a popular JavaScript library that provides a comprehensive set of tools and utilities for interacting with the Ethereum blockchain. It is designed to simplify Ethereum development and decentralized application (dApp) development by providing a high-level and user-friendly interface.

Ethers.js offers a wide range of functionalities, including [81]:

- Web3 Provider Management: Ethers.js allows developers to connect to various Ethereum networks using different providers, such as MetaMask, Infura, or a local node.
- Wallet Management: With Ethers.js, you can generate Ethereum wallets, manage accounts, sign, and send transactions, and interact securely with the blockchain.
- Contract Interactions: Ethers.js facilitates the interaction with Ethereum smart contracts, enabling developers to deploy, read, and write data to smart contracts in a straightforward manner. It abstracts away the complexities of interacting with the low-level Ethereum Virtual Machine (EVM) bytecode.
- Transaction Handling: Ethers.js provides utilities for creating, signing, and broadcasting transactions on the Ethereum network. It offers flexibility in setting gas prices, estimating transaction costs, and handling transaction lifecycle events.
- Event Monitoring: The library allows you to subscribe to and listen for events emitted by Ethereum smart contracts, enabling efficient tracking and processing of blockchain events.

- Ethereum Name Service (ENS) Support: Ethers.js includes built-in support for the Ethereum Name Service (ENS), simplifying the resolution and management of human-readable names for Ethereum addresses.

Ethers.js is widely used in Ethereum development, including dApp development, blockchain integration, and smart contract interactions. It is actively maintained and regularly updated to incorporate the latest features and improvements in the Ethereum ecosystem.

3.5. HTML, CSS & JavaScript

HTML (Hypertext Markup Language) is the standard markup language for creating the structure and content of web pages. It provides a set of tags and elements that define the different parts of a webpage, such as headings, paragraphs, links, images, and more[82].

CSS (Cascading Style Sheets) is a style sheet language that controls the presentation and layout of HTML elements. With CSS, you can define colors, fonts, sizes, margins, and other visual properties to enhance the appearance and aesthetics of the web page [83].

JavaScript is a versatile scripting language that adds interactivity and dynamic behavior to web pages. It allows you to create responsive elements, handle user interactions, manipulate HTML content, make API calls, and implement complex functionality in the web application [84].

By leveraging HTML, CSS, and JavaScript, along with Ethers.js library, we can design an intuitive and functional interface for interacting with smart contracts. This interface empowers users to seamlessly interact with the contract's functionalities, input data, and receive real-time feedback, ultimately enhancing the overall user experience of the smart contract application.

4. IMPLEMENTATION

The implementation of the proposed solution consists of a smart contract written in Solidity (see Figure 4.2) and a web interface developed using HTML, CSS, and JavaScript (see Figure 4.4). The smart contract, named "SensorData," is responsible for storing and managing sensor readings on the blockchain. It utilizes the AccessControl contract from the OpenZeppelin library to manage role-based access control. The implementation step is:

- Setup the blockchain network locally
- Write the smart contract solidity and compile it then deploy it on the local network.
- Design the web interface using HTML/CSS.
- Write the backend function to contact our smart contract using JavaScript.
- Connect the smart contract with our interface using Web3 API.
- Publish the web interface locally using Node.js.

4.1. System Diagram

In the following Figure 4.1, we have a block diagram that represents our solution. we have a smart contract deployed on a local blockchain network and connected to a web interface. In this web interface, we have N virtual IoT sensor that generates reading and sends it, the backend(represented by Web3 API & Javascript) receives this reading and adds them to the smart contract to keep them secure, immutable, and decentralized.

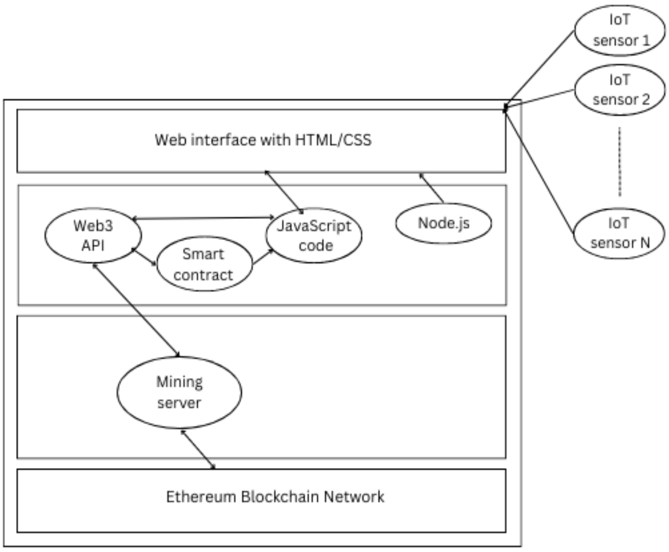
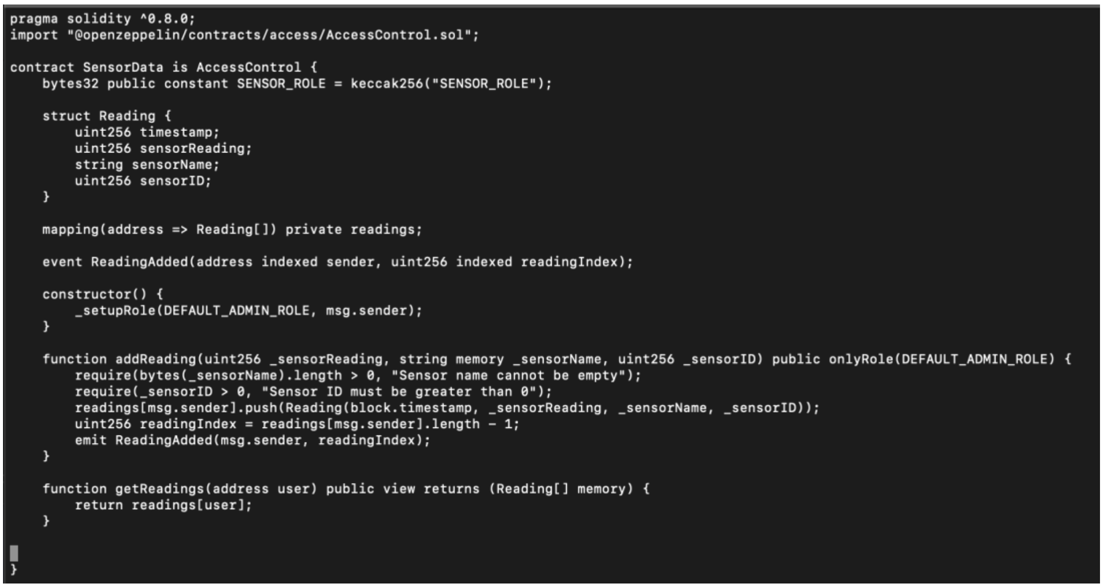


Figure 4.1. System Diagram

4.2. Smart Contract



```
pragma solidity ^0.8.0;
import "@openzeppelin/contracts/access/AccessControl.sol";

contract SensorData is AccessControl {
    bytes32 public constant SENSOR_ROLE = keccak256("SENSOR_ROLE");

    struct Reading {
        uint256 timestamp;
        uint256 sensorReading;
        string sensorName;
        uint256 sensorID;
    }

    mapping(address => Reading[]) private readings;

    event ReadingAdded(address indexed sender, uint256 indexed readingIndex);

    constructor() {
        _setupRole(DEFAULT_ADMIN_ROLE, msg.sender);
    }

    function addReading(uint256 _sensorReading, string memory _sensorName, uint256 _sensorID) public onlyRole(DEFAULT_ADMIN_ROLE) {
        require(bytes(_sensorName).length > 0, "Sensor name cannot be empty");
        require(_sensorID > 0, "Sensor ID must be greater than 0");
        readings[msg.sender].push(Reading(block.timestamp, _sensorReading, _sensorName, _sensorID));
        uint256 readingIndex = readings[msg.sender].length - 1;
        emit ReadingAdded(msg.sender, readingIndex);
    }

    function getReadings(address user) public view returns (Reading[] memory) {
        return readings[user];
    }

}
```

Figure 4.2. Smart Contract Code.

The smart contract implements the following functionalities:

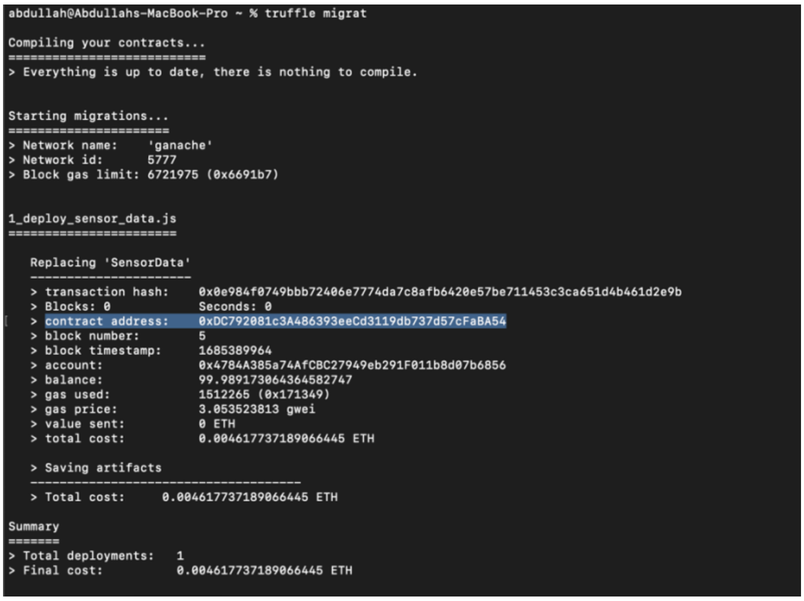
- Access Control: The contract extends the AccessControl contract from the OpenZeppelin library. It defines a constant “SENSOR_ROLE” and grants it to the contract deployer (admin) using the “_setupRole” function in the constructor.

- Reading Struct: The contract defines a struct named “Reading” to represent a sensor reading. It includes the following fields:
    - “timestamp”: The timestamp of the reading.
    - “sensorReading”: The value of the sensor reading.
    - “sensorName”: The name of the sensor.
    - “sensorID”: The unique identifier of the sensor.
- Mapping: The contract includes a private mapping named “readings” that maps an address (sensor) to an array of “Reading” objects. Each sensor can store multiple readings.
- Event: The contract emits the “ReadingAdded” event whenever a new reading is added to the “readings” mapping. The event includes the address of the sender (sensor) and the index of the reading in the array.
- Constructor: The contract's constructor is responsible for setting up the default admin role by calling the “_setupRole” function from the AccessControl contract. The contract deployer (msg.sender) is granted the DEFAULT_ADMIN_ROLE.
- addReading Function: The “addReading” function allows the admin (contract deployer) to add a new sensor reading. It takes three parameters: “_sensorReading”, “_sensorName”, and “_sensorID”. The function checks that the sensor name is not empty, and the sensor ID is greater than zero. If the conditions are met, the function adds the reading to the “readings” mapping for the calling address (sensor). It also emits the “ReadingAdded” event with the sender's address and the index of the added reading.
- getReadings Function: The “getReadings” function allows any user to retrieve the array of readings associated with a specific address (sensor). It takes the “user” parameter and returns an array of “Reading” objects associated with that address.

To compile this smart contract and deploy it locally we need to do the following :

1. Make sure Ganache is running.
2. Save the smart contract to this path “~/contracts” with extension (.sol).
3. Open the terminal and navigate to this path “~/contracts”.

4. Compile the Solidity contract using Truffle by running this command “truffle compile”
5. After the compilation is successful, we need to migrate the contract to the Ganache network using the following command “truffle migrate”
6. After the migrations is done we need the contract address to interact with our contract (see figure 4.3).

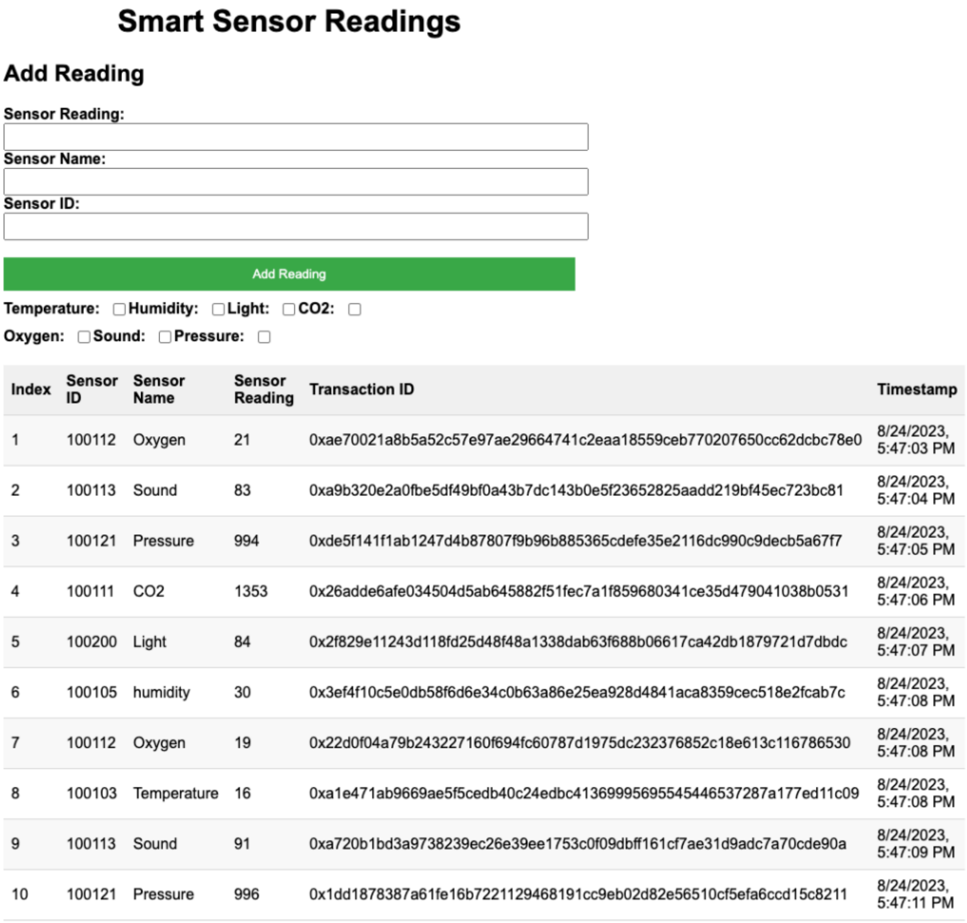


```
abdullah@Abdullahs-MacBook-Pro ~ % truffle migrat

Compiling your contracts...
===========================
> Everything is up to date, there is nothing to compile.


Starting migrations...
======================
> Network name:    'ganache'
> Network id:      5777
> Block gas limit: 6721975 (0x6691b7)


1_deploy_sensor_data.js
=======================

   Replacing 'SensorData'
   ----------------------
   > transaction hash:    0x0e984f0749bbb72406e7774da7c8afb6420e57be711453c3ca651d4b461d2e9b
   > Blocks: 0            Seconds: 0
   > contract address:    0xDC792081c3A486393eeCd3119db737d57cFaBA54
   > block number:        5
   > block timestamp:     1685389964
   > account:             0x4784A385a74AfCBC27949eb291F011b8d07b6856
   > balance:             99.989173064364582747
   > gas used:            1512265 (0x171349)
   > gas price:           3.053523813 gwei
   > value sent:          0 ETH
   > total cost:          0.004617737189066445 ETH

   > Saving artifacts
   -------------------------------------
   > Total cost:     0.004617737189066445 ETH

Summary
=======
> Total deployments:   1
> Final cost:          0.004617737189066445 ETH
```

Figure 4.3. Smart Contract Migrations Result.

4.3. Web Interface

The web interface provides a user-friendly way to interact with the smart contract and display sensor readings. It is built using HTML, CSS, and JavaScript and communicates with the smart contract using ethers.js library.



Smart Sensor Readings

Add Reading

Sensor Reading:

Sensor Name:

Sensor ID:

Temperature: □ Humidity: □ Light: □ CO2: □

Oxygen: □ Sound: □ Pressure: □

Index	Sensor ID	Sensor Name	Sensor Reading	Transaction ID	Timestamp
1	100112	Oxygen	21	0xae70021a8b5a52c57e97ae29664741c2eaa18559ceb770207650cc62dcbc78e0	8/24/2023, 5:47:03 PM
2	100113	Sound	83	0xa9b320e2a0fbe5df49bf0a43b7dc143b0e5f23652825aadd219bf45ec723bc81	8/24/2023, 5:47:04 PM
3	100121	Pressure	994	0xde5f141f1ab1247d4b87807f9b96b885365cdefe35e2116dc990c9decb5a67f7	8/24/2023, 5:47:05 PM
4	100111	CO2	1353	0x26adde6afe034504d5ab645882f51fec7a1f859680341ce35d479041038b0531	8/24/2023, 5:47:06 PM
5	100200	Light	84	0x2f829e11243d118fd25d48f48a1338dab63f688b06617ca42db1879721d7dbdc	8/24/2023, 5:47:07 PM
6	100105	humidity	30	0x3ef4f10c5e0db58f6d6e34c0b63a86e25ea928d4841aca8359cec518e2fcab7c	8/24/2023, 5:47:08 PM
7	100112	Oxygen	19	0x22d0f04a79b243227160f694fc60787d1975dc232376852c18e613c116786530	8/24/2023, 5:47:08 PM
8	100103	Temperature	16	0xa1e471ab9669ae5f5cedb40c24edbc41369995695545446537287a177ed11c09	8/24/2023, 5:47:08 PM
9	100113	Sound	91	0xa720b1bd3a9738239ec26e39ee1753c0f09dbff161cf7ae31d9adc7a70cde90a	8/24/2023, 5:47:09 PM
10	100121	Pressure	996	0x1dd1878387a61fe16b7221129468191cc9eb02d82e56510cf5efa6ccd15c8211	8/24/2023, 5:47:11 PM

Figure 4.4. Smart Contract Web Interface.

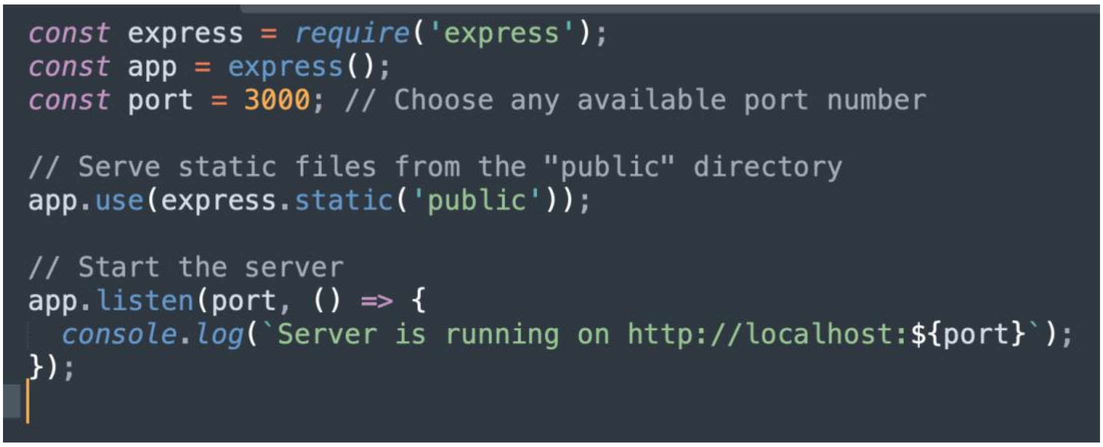
The web interface (see Figure 4.4) consists of the following components:

- 3 text boxes for entering the reading manually.
- 7 checkboxes to act as virtual IoT sensors for sending readings automatically like real IoT sensors.
- Table to show the reading that is stored on the blockchain.

The web interface allows users to perform the following actions:

- Connect to the Ethereum network and select an account for interaction.
- Add a new sensor reading by entering the required information (sensor reading, sensor name, and sensor ID) and invoking the appropriate smart contract function.
- Retrieve and display sensor readings associated with a specific address (sensor) by calling the “getReadings” function and dynamically updating the web interface with the retrieved data.

To run the web interface, we need a web server so the following Figure 4.5 shows a script that will run as a web server :



```
const express = require('express');
const app = express();
const port = 3000; // Choose any available port number

// Serve static files from the "public" directory
app.use(express.static('public'));

// Start the server
app.listen(port, () => {
  console.log(`Server is running on http://localhost:${port}`);
});
```

Figure 4.5. Web Server Script.

After saving the script we need to put the HTML, CSS, JavaScript, and the smart contract abi in the public directory and run the following command “node server.js” Then the web interface will be accessed by this link” http://localhost:3000/ ”.

4.4. JavaScript Functions

JavaScript code provides the necessary functionality to interact with the Sensor Data Interface web application, including adding readings, retrieving readings, generating random readings, and continuously fetching the most recent readings.

The script contains the following function:

- connectToContract() function establishes a connection to the local blockchain network by creating a provider with the specified URL(ganache network URL). It retrieves the user's account address and fetches the ABI (Application Binary Interface) file from the sensorData.json file. It then creates an instance of the contract using the contract address and ABI.
- addReading() function is responsible for adding a new sensor reading to the contract. It retrieves the values from the input fields, connects to the contract, and calls the “addReading()” function of the deployed contract with the provided parameters. After the transaction is successful, it clears the form and retrieves the most recent readings.

- getReadings() function retrieves the readings from the contract by connecting to the contract and calling the “getReadings()” function of the deployed contract. It then calls the “displayReadings()” function to show the readings in the interface.
- displayReadings() function takes an array of readings as input and dynamically generates a table to display the readings in the web interface. If no readings are available, it shows a message indicating so.
- generateReadingTemp(), generateReadingHumidity() generateReadingLight() generateReadingPressure() generateReadingSound() generateReadingCO2() generateReadingOxygen(): these functions generate random sensor readings (as virtual sensors). Then call the “sendReading()” function with the generated values.
- sendReading() function sends a sensor reading to the contract. It connects to the contract and calls the “addReading()” function of the deployed contract with the provided parameters. It also logs the transaction hash to the console.

5. RESULTS AND DISCUSSION

5.1. Results

This chapter presents the results and discussion of implementing the Sensor Data Interface web application with blockchain technology.The integration of blockchain technology in the Sensor Data Interface has yielded significant results in various aspects of sensor data management. The key outcomes achieved include:

1. Data integrity and immutability: By recording sensor readings as transactions on the blockchain, the integrity and immutability of the data are ensured. Each reading becomes tamper-proof, providing a trustworthy and auditable record of the collected data.
2. Transparency and auditable data: Blockchain promote transparency by allowing public visibility of sensor readings. Stakeholders can independently verify the authenticity and accuracy of the data, facilitating collaboration and data analysis processes.
3. Decentralization and reducing single points of failure: The decentralized nature of the blockchain network eliminates the need for a central authority and reduces the risk of a single point of failure. This enhances the system's resilience, reliability, and fault tolerance.
4. Enhanced data security: Blockchain employs robust security mechanisms, including digital signatures and cryptography, to protect the privacy, confidentiality, and integrity of the sensor data. The decentralized nature of the network further mitigates the risk of data breaches.
5. Improved data traceability: Each sensor reading is associated with a timestamp and the identity of the sensor owner, enabling comprehensive traceability. This enhances data quality control, accountability, and reliability.
6. Efficient data exchange and collaboration: Blockchain facilitates secure and efficient data exchange among authorized users, eliminating the need for intermediaries. Real-time collaboration and decision-making are enabled, leading to better utilization of the collected sensor data.

7. Scalability and interoperability: The blockchain framework offer scalability to accommodate an increasing number of sensors and large data volumes. It also promotes interoperability, allowing seamless integration with other systems and applications.

5.2. Discussion

The results of integrating blockchain technology in the Sensor Data Interface provide valuable insights into the enhancements brought by blockchain in the management and utilization of sensor data. These outcomes have implications for various stakeholders and domains, including:

- Research and Development: The use of blockchain ensures the integrity, transparency, and auditable nature of sensor data, enhancing the reliability and trustworthiness of research findings. Researchers can access authentic and unaltered data for analysis, fostering scientific advancements.
- Regulatory Compliance: Blockchain's immutability and traceability features contribute to compliance with data regulations and standards. Regulators can easily verify the authenticity and integrity of sensor data, ensuring compliance and promoting trust.
- Industrial Applications: Blockchain technology provides a secure and transparent platform for industrial applications that rely on accurate and trustworthy sensor data. Industries such as supply chain management, logistics, and environmental monitoring can leverage blockchain to enhance data reliability and streamline processes.
- Collaborative Data Analysis: The transparency and efficient data exchange facilitated by blockchain enable collaborative data analysis efforts. Researchers, organizations, and data analysts can access and share sensor data seamlessly, accelerating insights generation and decision-making.
- Data Monetization: The integration of blockchain enhances the value of sensor data for monetization purposes. The immutable and auditable nature of the data increases its marketability and enables new business models based on data monetization.
- Future Development: The potential for smart contracts and automation opens up possibilities for further advancements in sensor data management. Smart

contracts can automate data validation, trigger actions, and streamline data operations, leading to increased efficiency and reduced manual intervention.

6. CONCLUSION AND RECOMMENDATIONS

6.1. Conclusion

In conclusion, the integration of blockchain technology in the Sensor Data Interface has proven to be a transformative solution for sensor data management. The implementation and evaluation of the system have demonstrated the significant enhancements offered by blockchain in terms of data integrity, security, transparency, and efficiency. Through the utilization of blockchain's inherent features, such as immutability and decentralized consensus, the Sensor Data Interface ensures the authenticity and immutability of sensor data. The transparency provided by the blockchain allows stakeholders to verify the origin, modification history, and integrity of the data, fostering trust and confidence in its accuracy. The decentralized nature of the blockchain eliminates the need for intermediaries or centralized authorities, enabling direct and efficient data exchange among multiple parties. This promotes data interoperability, collaboration, and innovation in sensor-based applications. The integration of smart contracts further enhances the Sensor Data Interface by enabling automation and self-executing agreements. Smart contracts facilitate predefined actions based on predefined conditions, reducing manual intervention, and streamlining data processing workflows. The adoption of blockchain technology in the Sensor Data Interface offers a secure, transparent, and efficient ecosystem for managing sensor data. It empowers stakeholders with greater control and confidence in the accuracy, integrity, and availability of the data they rely on for decision-making.

The findings of this research highlight the significant potential of blockchain technology in transforming sensor data management across various industries. By addressing the challenges of data integrity, security, transparency, and collaboration, blockchain provides a solid foundation for enhancing sensor data management practices.

6.2. Future Work

In the pursuit of further enhancing the Sensor Data Interface, several avenues for future work can be explored. The primary focus will be on deploying the system on a real blockchain network and connecting it to real sensors.

Deploying on a Real Blockchain: One crucial aspect of future work is the deployment of the Sensor Data Interface on a production-ready blockchain network. This involves selecting a suitable blockchain platform and setting up the necessary infrastructure. It is essential to ensure scalability, performance, and cost-effectiveness to handle a significant volume of sensor data and transactions in real-world scenarios.

Connecting to Real IOT Sensors: Integrating the Sensor Data Interface with real sensors is another vital aspect of future work. By connecting the interface to actual sensors, the system can obtain real-time data for analysis and decision-making. This integration can be achieved using oracles, which act as bridges between the blockchain and external data sources. By leveraging oracles, the Sensor Data Interface can provide accurate and up-to-date sensor readings.

Real-World Testing and Validation: Conducting extensive real-world testing and validation is essential to assess the effectiveness and practicality of the Sensor Data Interface. Collaborating with industry partners and stakeholders will provide valuable insights into the system's performance, usability, and limitations. By deploying the system in operational environments and gathering feedback from users, improvements can be made based on real-world experiences and requirements.

REFERENCES

[1] M. Chen, S. Mao, and Y. Liu (2020). "Big data: A survey," Mobile Networks and Applications, vol. 19, no. 2, pp. 171-209.

[2] S. Li, L. D. Xu, and S. Zhao (2019). "Security and privacy in smart city applications: Challenges and solutions," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 759-796.

[3] F. A. Alaba, M. Othman, and A. O. Adetunmbi (2017). "Internet of Things security: A survey," Journal of Network and Computer Applications, vol. 88, pp. 10-28.

[4] S. Li, L. D. Xu, and S. Zhao (2018). "Blockchain-based decentralized trust management in vehicular networks," IEEE Transactions on Vehicular Technology, vol. 67, no. 7, pp. 6064-6076.

[5] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander (2016). "Where is current research on blockchain technology? A systematic review," PloS One, vol. 11, no. 10, e0163477.

[6] T. T. A. Dinh, D. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang (2017). "Untangling blockchain: A data processing view of blockchain systems," IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, pp. 1366-1385.

[7] Antonopoulos, A., & Gillam, L. (2017). "A Survey on Blockchain-Based Solutions for the Internet of Things." IEEE Internet of Things Journal. DOI: 10.1109/JIOT.2017.2745898

[8] Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). "Securing the Internet of Things Using Blockchain Technology." Proceedings of the 17th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM). DOI: 10.1109/WoWMoM.2016.7523549

[9] Panarello, A., Tapas, N., Merlino, G., & Longo, F. (2018). "Blockchain-Enabled Fog Nodes for Secure IoT Applications." IEEE Access. DOI: 10.1109/ACCESS.2018.2798321

[10] Liang, X., Shetty, S., & Toshniwal, D. (2017). "A Blockchain-Based Data Integrity Protection Mechanism for IoT Data." IEEE International Conference on Cloud Computing (CLOUD). DOI: 10.1109/CLOUD.2017.15

[11] Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2018). "Blockchain Solutions for IoT Security: A Review." IEEE Internet of Things Journal. DOI: 10.1109/JIOT.2018.2846062

[12] Christidis, K., & Devetsikiotis, M. (2016). "Blockchains and Smart Contracts for the Internet of Things." IEEE Access. DOI: 10.1109/ACCESS.2016.2566339

[13] Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., ... & Rimba, P. (2018). "A Taxonomy of Blockchain-Based Systems for Architecture Design." IEEE Transactions on Software Engineering. DOI: 10.1109/TSE.2018.2875468

[14] Biswas, K., & Misra, S. (2019). "Blockchain in Internet of Things: Challenges and Solutions." Computers & Electrical Engineering. DOI: 10.1016/j.compeleceng.2018.10.027

[15] Fan, K., Ren, Y., Song, J., & Li, Q. (2018). "Blockchain-based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems in Smart Cities." IEEE Transactions on Intelligent Transportation Systems.

[16] Yuan, Y., Zhang, S., Wen, Y., Wang, X., & Zhang, H. (2018). "Toward Blockchain-Based Intelligent Transportation Systems." IEEE Intelligent Transportation Systems Magazine. DOI: 10.1109/MITS.2018.2876060

[17] Ouaddah, A., Abou Elkalam, A., and Ouahman, A. A. (2018). "Towards a blockchain-based secure and trusted Internet of Things." In Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS), pp. 195-202.

[18] Vasilomanolakis, E., Daubert, J., Böck, H., Hartenstein, H., and Schuba, M. (2017). "Privacy and security in the Internet of Things: Current status and open issues." In Proceedings of the IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1-6.

[19] Dorri, A., Kanhere, S. S., and Jurdak, R. (2017). "Blockchain for IoT security and privacy: The case study of a smart home." In Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 618-623.

[20] Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." White Paper.

[21] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction." Princeton University Press.

[22] Swan, M. (2015). "Blockchain: Blueprint for a New Economy." O'Reilly Media.

[23] Dwork, C., and Naor, M. (1993). "Pricing via processing or combating junk mail." Proceedings of the Annual International Cryptology Conference.

[24] Buterin, V. (2013). "Ethereum: A next-generation smart contract and decentralized application platform." White Paper.

[25] Tapscott, D., & Tapscott, A. (2016). "Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world." PDF Book.

[26] Queiroz, M. M., Rosa, P. F. F., and Ponte, A. M. (2019). "Towards a blockchain-based solution for data sharing and monetization in the IoT." Journal of Parallel and Distributed Computing, vol. 130, pp. 34-45.

[27] Szabo, N. (1994). "Smart contracts: Building blocks for digital markets." Extropy Magazine.

[28] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., and Felten, E. W. (2015). "Research perspectives and challenges for Bitcoin and cryptocurrencies." Proceedings of the IEEE Symposium on Security and Privacy.

[29] Zhang, S., & Lee, J. H. (2020). "A Comparative Study of Consensus Algorithms in Blockchain Networks." In Proceedings of the IEEE International Conference on Blockchain (Blockchain-2020) (pp. 209-216). IEEE.

[30] Wood, G. (2014). "Ethereum: A secure decentralised generalised transaction ledger."

[31] Antonopoulos, A. M. (2018). "Mastering Ethereum: Building smart contracts and DApps." O'Reilly Media.

[32] Atzori, L., Iera, A., & Morabito, G. (2010). "The Internet of Things: A survey." Computer Networks, 54(15), 2787-2805.

[33] Borgia, E. (2014). "The Internet of Things vision: Key features, applications, and open issues." Computer Communications, 54, 1-31.

[34] Chen, M., Ma, Y., Song, J., Yang, L., & Luo, J. (2014). "IoT healthcare: A survey." Mobile Networks and Applications, 19(2), 133-141.

[35] Kanter, T., Chakraborty, D., & Bose, R. P. (2015). "Managing big data for IoT-based large-scale systems: A survey." IEEE Cloud Computing, 2(3), 32-43.

[36] Li, S., Da Xu, L., & Zhao, S. (2017). "The internet of things: A survey." Information Systems Frontiers, 17(2), 243-259.

[37] Liakopoulos, A., Gouvas, P., & Tsoukalas, L. H. (2017). "Internet of Things in agriculture, recent advances and future challenges." Biosystems Engineering, 164, 31-48.

[38] Roman, R., Zhou, J., & Lopez, J. (2013). "On the features and challenges of security and privacy in distributed Internet of Things." Computer Networks, 57(10), 2266-2279.

[39] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). "Edge computing: Vision and challenges." IEEE Internet of Things Journal, 3(5), 637-646.

[40] Yuan, Y., Gao, J., Zhang, Q., & Yang, Z. (2014). "Security and privacy in smart cities: Challenges and solutions." IEEE Communications Magazine, 52(8), 75-81.

[41] Bennis, M., Samarakoon, S., & Taleb, T. (2018). "The road to 5G: A tutorial on 5G and its standardization process." Communications Surveys & Tutorials, 20(3), 1778-1802.

[42] Kassab, W., & Darabkh, K. A. (2020). "A–Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations." Journal of Network and Computer Applications, 163.

[43] Aleksandrovičs, V., Filičevs, E., & Kampars, J. (2016). "Internet of things: Structure, features and management." Information Technology and Management Science, 19, 78-84.

[44] Sethi, P., & Sarangi, S. R. (2017). "Internet of things: Architectures, protocols, and applications." Journal of Electrical and Computer Engineering, 2017, 1-25.

[45] Abdmeziem, M. R., Tandjaoui, D., & Romdhani, I. (2016). "Architecting the internet of things: State of the art." Robots and Sensor Clouds, 55-75.

[46] Zhou, D., Ciuonzo, D. F., & Liu, P. (2018). "IoT data integrity schemes and challenges: A survey." IEEE Communications Surveys & Tutorials, 20(1), 613-630.

[47] Purohit, A., Sharma, A., & Bhardwaj, S. (2020). "Data integrity techniques for internet of things: A systematic literature review." Computers & Electrical Engineering, 86, 106-126.

[48] Zeng, S., Chen, Z., & Li, Y. (2020). "Blockchain-Based Data Integrity Service Framework for IoT Data." Sensors, 20(4), 1174.

[49] Hancke, G., & Chong, T. K. (2017). "Guest editorial: Special issue on security and privacy in the Internet of Things." IEEE Transactions on Dependable and Secure Computing, 14(5), 455-457.

[50] Sun, Y., Wang, S., & Shin, K. G. (2020). "Guest editorial special issue on Internet of Things security and privacy." IEEE Internet of Things Journal, 7(1), 1-3.

[51] Biswas, D., & Misra, R. (2018). "Blockchain Technology in IoT Applications: Challenges and Opportunities." In Proceedings of the 2018 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 1-5.

[52] Dorri, A., Steger, M., Kanhere, S., & Jurdak, R. (2017). "Blockchain for IoT security and privacy: The case study of a smart home." In Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom), pp. 618-623.

[53] Xu, X., He, P., Chen, J., & Luo, X. (2018). "A blockchain-based framework for reliable and efficient data sharing in an IoT environment." IEEE Internet of Things Journal, 5(2), 1184-1195.

[54] Ren, K., Lee, W. C., & Kim, J. (2018). "Secure privacy-preserving data aggregation in mobile IoT." IEEE Transactions on Industrial Informatics, 14(9), 3994-4003.

[55] Dwork, C. (2008). "Differential privacy: A survey of results." In International Conference on Theory and Applications of Models of Computation, pp. 1-19.

[56] Kulkarni, A. A., Thakur, S. J., & Sarode, M. V. (2017). "IoT security: Physical tampering." In Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1141-1145.

[57] Patil, A. P., Jagtap, S. R., & Ghose, M. K. (2019). "A review of secure tamper-proof framework for Internet of Things (IoT) devices." In Proceedings of the 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), pp. 238-243.

[58] Yao, L., Huang, X., Chen, X., & Liu, X. (2019). "Blockchain for the Internet of Things: A systematic literature review." IEEE Access, 7, 66328-66341.

[59] Alrakhami, M., & Al-Mashari, M. (2021). A Blockchain-Based Trust Model for the Internet of Things Supply Chain Management. Sensors, 21(5), 1759. doi: 10.3390/s21051759.

[60] Swan, M. (2015). "Blockchain: Blueprint for a new economy." O'Reilly Media.

[61] Moti, M. M. M. A., Uddin, R. S., Hai, M. A., Saleh, T. B., Alam, M. G. R., Hassan, M. M., & Hassan, M. R. (2022). Blockchain Based Smart-Grid Stackelberg Model for Electricity Trading and Price Forecasting Using Reinforcement Learning. Applied Sciences, 12(10), 5144. doi: 10.3390/app12105144

[62] Ekblaw, A., Azaria, A., Halamka, J. D., & Lippman, A. (2016). "A case study for blockchain in healthcare: 'MedRec' prototype for electronic health records and medical research data." Proceedings of IEEE Open & Big Data Conference, 2016, 25-30.

[63] Attia, O., Khoufi, I., Laouiti, A., & Adjih, C. (2019). An IoT-Blockchain Architecture Based on Hyperledger Framework for Healthcare Monitoring Application. 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 1-5.

[64] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). "Blockchain for IoT security and privacy: The case study of a smart home." Proceedings of IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2017, 618-623.

[65] Farooq, M.S., Khan, S., Rehman, A., Abbas, S., Khan, M.A., & Hwang, S.O. (2022). Blockchain-Based Smart Home Networks Security Empowered with Fused Machine Learning. Sensors, 22, 4522.

[66] Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). "Towards secure vehicular IoT with blockchain." Electronics, 7(11), 286.

[67] Fraga-Lamas, P. & Fernández-Caramés, T. M. (2021). IoT-Connected Vehicle Use. IEEE Smart Cities.

[68] Xu, R., Weber, I., Staples, M., Zhu, L., Bosch, J., & Bass, L. (2017). "A taxonomy of blockchain-based systems for architecture design." Proceedings of IEEE International Conference on Software Architecture (ICSA), 2017, 243-252.

[69] Hasan Pranto, T., All Noman, A., Mahmud, A., & Bahalul Haque, A. K. M. (2021). Blockchain and smart contract for IoT enabled smart agriculture. arXiv e-prints, arXiv-2104.

[70] Li, Q., Xu, X., Liang, X., & Zhao, X. (2018). "Blockchain-enabled smart cities: Framework and applications." IEEE Access, 6, 55178-55186.

[71] Deng, T., Zhang, K., & Shen, Z. J. M. (2021). A systematic review of a digital twin city: A new pattern of urban governance toward smart cities. Journal of Management Science and Engineering, 6(2), 125-134.

[72] Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). "Blockchain-based sharing and traceability of waste management in smart city." IEEE Access, 6, 43843-43853.

[73] Ahmad, R.W., Salah, K., Jayaraman, R., Yaqoob, I., & Omar, M.A. (2021). Blockchain for Waste Management in Smart Cities: A Survey. IEEE Access, 9, 131520-131541.

[74] Jazri, H., Sbita, L., & El Kalam, A. A. (2018). "Blockchain for secure and privacy-preserving data storage and sharing in smart cities." Future Generation Computer Systems, 88, 45-57.

[75] Song, Z., Wang, G., Yu, Y., & Chen, T. (2022). Digital Identity Verification and Management System of Blockchain-Based Verifiable Certificate with the Privacy Protection of Identity and Behavior. Security and Communication Networks, 2022.

[76] Liang, X., Xu, X., Shao, J., Xu, Q., & Zhao, X. (2019). "A blockchain-based framework for trustworthy urban governance in smart cities." IEEE Transactions on Industrial Informatics, 16(6), 4319-4327.

[77] Node.js Foundation. (2022). Node.js Documentation. Retrieved from https://nodejs.org/en/docs/ on [25-05-2023].

[78] npm, Inc. (2021). npm Documentation. Retrieved from https://docs.npmjs.com/ on [25-05-2023].

[79] Truffle Suite. (2021). Ganache Documentation. Retrieved from https://www.trufflesuite.com/docs/ganache on [26-05-2023].

[80] Truffle Suite. (2021). Truffle Documentation. Retrieved from https://www.trufflesuite.com/docs/truffle/overview on [26-05-2023].

[81] Rantanen, R., & Kovanen, A. (2021). Ethers.js Documentation. Retrieved from https://docs.ethers.io/ on [27-05-2023].

[82] World Wide Web Consortium. (2017). HTML5. Retrieved from https://www.w3.org/TR/html52/ on [27-05-2023].

[83] World Wide Web Consortium. (2017). CSS Cascading Style Sheets. Retrieved from https://www.w3.org/Style/CSS/ on [27-05-2023].

[84] Mozilla Developer Network. (n.d.). JavaScript. Retrieved from https://developer.mozilla.org/en-US/docs/Web/JavaScript on [27-05-2023].

CURRICULUM VITAE

Name Surname : Abdullah AL-MOKDAD

EDUCATION:

- **Graduate** : 2023, Sakarya University, Department of Computer and Information Engineering, Computer And Information Engineering.
- **Undergraduate** : 2019, Yarmouk University, Hijjawi Faculty for Engineering Technology, Computer Engineering.

PROFESSIONAL EXPERIENCE AND AWARDS:

- 2021-now web developer freelance.
- 2019-2021 worked as System Engineer at Specialized Technology Grid “STG”, Amman – Jordan.
- 2018-2019 worked as web & android developer at orange yarmouk innovation lab “OYIL”, Irbid – Jordan.

PUBLICATIONS, PRESENTATIONS AND PATENTS ON THE THESIS:

- Abdullah A. , Ünal Ç. (2023) Blockchain Applications and Security Issues Based on the Internet of Things, *Balkan Journal of Electrical and Computer Engineering*.