Arab American University

Faculty of Graduate Studies

Implementing Artificial Intelligence in Blockchain for Ramallah Smart City in Palestine: A Case Study

By

Asad Omar Ahmad Salem

Supervisor

Prof. Labib Arafa

This thesis was submitted in partial fulfillment of the requirements for the Master`s degree in Cybercrime and digital evidence analysis

July /2023

Thesis Approval

Implementing Artificial Intelligence in Blockchain for Ramallah Smart City in Palestine: A Case Study

By

Asad Omar Ahmad Salem

This Thesis was defended successfully on 14/10/2023 and approved by:

Committee Members Signature

1. Prof. Labib Arafa /Supervisor .....

2. Dr. Ahmad Hasasneh/ Internal Examiner: .....

3. Dr. Mohammed Abutaha/ External Examiner: …….....

Mohammed Abutaha

Declaration

I declare that this thesis entitled "Implementing Artificial Intelligence in Blockchain for Ramallah Smart City in Palestine: A Case Study " is my work and has been composed solely by myself, does not contain any work from other researchers, and has not been submitted for any other degree or scientific qualification except the references is made.

Student Name: Asad Omar Ahmad Salem

Signature: …….

Date: ……

Student ID: 201920290

Dedication

To those who sacrificed years of their lives to illuminate my path with their effort and long struggle, to my beloved parents, to my wife and children, without whose sacrifices I wouldn't have reached where I am now, to my brothers who have always stood by my side, strengthening my resolve and supporting me, to my friends and all those who have motivated me to continue this journey, I dedicate this thesis

Abstract

This thesis worked on studying implementation artificial intelligence in blockchain technology, studying smart cities, and studying the smart city of Ramallah, and then linking the two technologies in order to benefit from them optimally. The study presented a proposal to apply blockchain technology in the city of Ramallah in Palestine by proposing a smart parking program in the city of Ramallah. RSP, in order to contribute to transforming the transportation sector from its traditional form into a smart transportation sector that would contribute to alleviating traffic congestion and reducing environmental pollution resulting from fuel combustion in cars, as well as strengthening the security system in the smart city of Ramallah by combating the phenomenon of illegal cars. As well as combating car theft, the study presented a new consensus algorithm in blockchain technology and called it SMO, as this algorithm works in three stages. The first stage begins with creating blocks using the Proof-of-Work consensus algorithm, and in the second stage it is an additional layer of protection called Block Bank: This layer works on early detection of malicious blocks and transactions using ML machine learning algorithms (Anomaly detection (Isolation Forest), Hidden Markov Models, K-means, Random Forests). The algorithm stores the detected malicious blocks in the Distributed Ledger to benefit from them in subsequent operations. In identifying malicious blocks, in the third stage, the Proof-of-Stake consensus algorithm is used to audit the blocks that were not identified in the second stage. If a malicious block is discovered, it is sent to the Distributed Ledger in order to benefit from it in identifying malicious blocks.

The message reached the following recommendations:

- The need to strongly encourage local researchers to address and explore blockchain technology in Palestine.

- It is suggested that it is necessary to study the various basic sectors in the city of Ramallah and contribute to transforming them from their traditional form into smart sectors.
- It is strongly suggested that the current study be applied to the rest of the Palestinian cities and search for ways to transform them into smart cities.
- It is strongly suggested that researchers explore artificial intelligence technology to raise the security level of blockchain technology

Keywords: Blockchain, AI, IoT, Smart-city, Bitcoin, Ethereum, Ramallah-Smart-City, Consensus Algorithm

Table of contents

Table Index

Figure Index

Appendix Index

List of abbreviations

Abbreviation	Definition
RSP	Ramallah Smart Parking
SFpark	San Francisco smart parking system
SMO	A new hybrid consensus algorithm is proposed in this study
ML	Machine Learning
GC	Gaza currency
IoT	Internet of Things
InfluxDB	Database to manage IoT devices
PoW	Proof-of-Work
PoS	Proof-of-Stake
PoA	Proof-of-Activity
ICT	Information and Communication Technologies
PBFT	Practical Byzantine Fault Tolerance
HMMs	Hidden Markov Models
AI	Artificial Intelligence
P2P	peer-to-peer
PoI	Proof of Importance
DPoS	Delegated Proof-of-Stake
PoB	Proof of Burn
PoET	Proof of Elapsed Time
BFT	Byzantine Fault Tolerance
PBFT	Practical Byzantine Fault Tolerance
TCP	Transmission Control Protocol
DApps	Decentralized Applications
APIs	application programming interfaces
HD wallets	Hierarchical deterministic wallets
PIN codes	Postal Index Number
Intel SGX	Intel Software Guard Extensions
QR code	quick-response code
DoS attacks	Denial of Service attacks
RPCA	Ripple Protocol Consensus Algorithm
SCP	Stellar Consensus Protocol
CFT	Crash Fault Tolerance consensus algorithms
PoW weight	Proof of Weight
PoC	Proof of Capacity
FTS	The Follow-the-Satoshi algorithm
Sp8de (SPX)	A digital asset that operates on the Ethereum platform.
(Tx/s)	The number of transactions processed per second
CoA	Chains-of-Activity
DEWA	Dubai Electricity and Water Authority
5G	The 5th generation mobile network
RTA	Roads and Transport Authority

1 Chapter one: General frame of study

1.1 Introduction

Blockchain technology has gained a wide popularity due to the complex process based on it in building contracts in a decentralized manner, through which transparency, integrity and security are achieved at a high level. As Blockchain technology can be described simply as a decentralized and distributed database of encrypted records secured in a cryptographic way. The principle of its work is to link a group of blocks sequentially in a time-stamped order that the blocks keep on all transactions that were created in the past and secured in a cryptographic way. Furthermore, it allows the review and verification process all information stored in a ledger without allowing it to be modified under any circumstances. This made it the subject of interest for many companies to exploit it in concluding contracts and transactions for it, and then expanded its use and became applied in many countries and government institutions around the world. As an example, the government of Estonia has used Blockchain technology since 2008 to secure health records for its citizens and documents, Legal and other important data (Kshetri, Nir. 2018). Singapore government has also adopted blockchain technology to improve its public services and enhance the security and efficiency of its financial system (Heng Teo. 2018). In addition, Dubai government has launched the Dubai Blockchain strategy, which aims to make Dubai the first government in the world powered by blockchain technology by 2020 (Benslimane & Benamar, 2018). Moreover, the Chinese government is investing heavily in blockchain technology and has launched several initiatives to explore its use in various industries, including finance and supply chain management (Xu et al., 2017). The Swiss government has also been a supporter of blockchain technology for several years and has launched several initiatives to support the development of blockchain-based

startups and applications (OECD, 2019). Finally, several states in the United States, including Arizona, Vermont, and Illinois, have passed laws recognizing the legal validity of blockchain-based smart contracts (Arizona State Legislature, 2017).

Despite the advantages provided by Blockchain technology, However, after research we found that there are limited initiatives in Palestine in exploring and using this technology, for example what the Governor of the Palestinian Monetary Authority announced in one of his statements that the Palestinian leadership is in the process of studying issuing a digital currency similar to Bitcoin (Jones, M. , 2017).Another example is what he (Abusamra, E. H. 2020) did by creating a Gaza wallet using Blockchain technology, which aims to facilitate to the citizens of Gaza to conduct financial transactions in a currency they called the Gaza currency (GC).

Blockchain technology has gained significant attention due to its cryptographic features, making it suitable for strong security solutions. A blockchain-based e-voting system can limit cybercrimes, providing a cost-effective, fast, and convenient service with high-security standards (Drescher. 2017). Blockchain is a distributed, immutable, and public ledger consisting of interconnected nodes, with no single authority controlling the network. Each node has a copy of the ledger that includes a summary of all processed transactions in the network. A transaction is accepted only when it obtains the majority agreement of the nodes (Drescher, 2017). Three main traits distinguish blockchain technology. Firstly, immutability refers, which refers to the creation of new blocks that must be referenced with the previous ones to create an immutable chain, preventing tampering with the integrity of the previous blocks. Secondly, verifiability is ensured through decentralization, distribution, and replication of the ledger among multiple nodes, providing high availability and eliminating a single point of failure. Thirdly, distributed consensus determines who can append the next new transaction to the ledger, and a

majority of the network nodes must reach consensus before any new proposed block of entries becomes a permanent part of the ledger. These three traits are achieved through advanced cryptography, providing a greater security level than previously known record-keeping systems (Alcaraz, et all. 2018).

A smart city is a city that uses technology and data to improve the quality of life of its citizens, optimize resource management, and enhance urban services' efficiency. Smart cities enable citizens to participate in decision-making processes and promote sustainable growth. The benefits of smart cities include reduced traffic congestion, energy efficiency, enhanced public safety, improved waste management, and increased citizen engagement in urban governance (Caragliu, Del Bo, & Nijkamp, 2011). Blockchain technology has the potential to transform smart cities by improving transparency, security, and trust in transactions. The decentralized nature of blockchain technology allows for secure data sharing among different stakeholders while protecting personal data privacy (Zhang, Xu, & Xu, 2018). Moreover, blockchain technology enables smart cities to build secure and efficient digital infrastructure, such as smart contracts, IoT-enabled devices, and energy management systems. Examples of smart cities that use blockchain technology include Dubai, which launched the Dubai Blockchain Strategy aiming to become the first blockchain-powered city by 2020 (Smart Dubai, n.d.), and Amsterdam, which is experimenting with blockchain technology to develop a platform for peer-to-peer energy trading (Kshetri, Nir. 2018).

1.2 The Importance of the study

During the 2014 Expotech conference with the theme "Smart Cities for a Creative Society," the then-Mayor of Ramallah, Mr. Musa Hadid, launched the Ramallah Smart City project in partnership with the Palestinian Telecommunications Company. The

project aimed to provide electronic services to citizens, offer Wi-Fi wireless internet to residents and visitors, and connect Ramallah municipality's buildings and facilities to its headquarters using Optics Fiber technology. This would allow visitors and residents of the city to use the Wi-Fi service free of charge. Local newspapers covered the news extensively (Ma'an News Agency, n.d.).

In 2022, the Palestinian Minister of Communications declared in an interview with Al-Hadath newspaper that the optical fiber network would be extended to cover all Palestinian cities, villages, and camps, as depicted in (Al Hadath News, n.d.). This study aims to shed light on the main features that can be utilized in the use of Blockchain technology in the smart city of Ramallah, as a smart Parking system (Ramallah Smart Parking - RSP) based on Blockchain was proposed with the aim of contributing to solving the problem of traffic congestion of vehicles in the city and contributing to raising the level of security in it, by combating illegal and expired vehicles and contributing to reducing vehicle theft crimes.

The study also presents a new consensus algorithm called SMO, which contains an additional layer of protection for the blockchain network, with the aim of adapting the blockchain to the resources and needs of the smart city of Ramallah.

1.3 Problem Statement

The city of Ramallah in Palestine targets key sectors in the transition to a smart city: technological infrastructure, smart governance, smart education, smart economy, smart mobility, and smart environment.

Despite this, these sectors are still witnessing many challenges, including the transportation sector, which faces multiple challenges in terms of transportation

management and mobility, most notably the increasing traffic congestion and carbon pollution resulting from fuel combustion emissions in vehicles, the use of illegal vehicles, and vehicle theft crimes.

Where this study proposes an applied solution to transform the transportation sector into smart transportation with the aim of promoting sustainable practices in the smart city of Ramallah and responding to the challenges faced by the transportation sector by taking advantage of the basic advantages of Blockchain technology and integrating it with Ramallah smart city and studying the opportunities and challenges in this. In addition to studying Blockchain applications in smart cities around the world and benefiting from them in presenting the Ramallah Smart Parking Proposal (RSP). To represent an effective response from Ramallah smart city to reduce the challenges faced by the transportation sector.

In addition, the study presented a new consensus algorithm SMO that works on early detection of malicious blocks that were nominated to be added to the blockchain network. Thus, the algorithm proposed in this study was able to reduce energy consumption in the blockchain network, raise the level of security, and ensure speed and effectiveness.

1.4 Research questions

This research will answer the following questions:

1. What are the fundamental principles and mechanisms of blockchain technology that make it a potential solution for enhancing the infrastructure and services of a smart city like Ramallah in Palestine?

2. What are the key characteristics and components of a smart city, and how can blockchain technology be effectively integrated into the existing smart city framework of Ramallah?
3. What are the specific challenges and opportunities associated with implementing blockchain technology in the context of Ramallah Smart City, considering factors such as governance, transportation, energy efficiency, and data security?
4. How can the proposed Ramallah Smart Parking (RSP) system, based on blockchain technology, address the traffic crisis, improve security, and promote sustainable practices within the city?
5. What are the potential applications of blockchain technology in smart cities globally, and how do these insights inform the development and optimization of blockchain solutions for Ramallah Smart City?
6. What are the key findings, lessons learned, and recommendations derived from the case study of Ramallah Smart City that can guide future research and practical implementations of blockchain technology in smart city projects, both within Palestine and on a global scale?

1.5 Hypothesis

Hypothesis 1: Effectively implementing the core principles and mechanisms of blockchain technology significantly enhances the infrastructure and services of a smart city like Ramallah in Palestine.

Hypothesis 2: The application of the Smart Parking System (RSP) based on blockchain technology in Ramallah addresses traffic congestion, improves security, and promotes sustainable practices within the city.

Hypothesis 3: Applying insights derived from potential blockchain technology applications in smart cities globally to the Smart City of Ramallah leads to meeting its unique needs.

1.6 Methodology

In this research, an applied research approach will be used. One of the smart city applications, which is the smart Ramallah parking, has been implemented so that the system is built on the basis of Blockchain technology to be used as an example for the response of the smart city of Ramallah in transforming the transportation sector into a smart transportation in order to reduce the challenges facing this sector, most notably traffic congestion, carbon pollution resulting from Vehicle fuel combustion, illegal vehicle use, vehicle theft crimes.

Where drivers are able to search for and reserve parking spaces without the need to search for them and cause a state of traffic congestion, thus reducing the amount of fuel that is burned, which leads to a decrease in pollution resulting from carbon emissions, in addition to the capabilities of the proposed system to detect illegal vehicles and notify the competent authorities of that. As well as detecting theft of vehicles and informing the competent authorities immediately.

Also, experiments were conducted in the protection layer (Block Bank) in the SMO consensus algorithm proposed by the study, to verify the advantages it provides and its compatibility with the resources and needs of the smart city of Ramallah.

1.7 Research Contribution

The contribution of this study is to present a new consensus algorithm SMO that is commensurate with the resources and needs of the smart city of Ramallah and adds a

higher level of security to the blockchain technology and reduces the consumption of energy and computing resources when verifying the candidate blocks to be added to the blockchain network through early detection of malicious blocks, as well the study evaluates the feasibility of integrating Blockchain technology into the infrastructure of Ramallah Smart City. And exploiting Blockchain technology to overcome many challenges facing the smart city of Ramallah by developing the transportation sector and contributing to its transformation into smart mobility to overcome challenges facing the city such as traffic congestion and pollution, as well as the use of illegal means of transportation, and vehicle theft crimes. This study proposed RSP smart car parking system in Ramallah based on the integration of various types of Blockchain technology and IoT as well as InfluxDB database to manage IoT devices, in order to make the most of the advantages of Blockchain technology such as decentralization, transparency, security, stability, efficiency, speed and scalability. To achieve this, the study will examine best practices from other smart cities that have successfully implemented Blockchain technology. The ultimate goal of the study is to actively contribute to transforming the city of Ramallah into a smart city by introducing the RSP system to contribute to transforming the transportation sector into a smart mobility by taking advantage of the main advantages of Blockchain technology.

1.8 Scope and limitation

Scope:

Geographical scope: The study focuses specifically on the application of blockchain technology in the context of the city of Ramallah in Palestine, as a case study for contributing to the development of a smart city.

Focus on Technology: The research explores the potential of implementing artificial intelligence in technology blockchain technology and its applications within the framework of smart cities, with a special focus on its implementation in the context of the smart city of Ramallah. The study presented a proposed system based on the integration of Public Blockchain, Private Blockchain, Consortium Blockchain, Internet of Things InfluxDB database, and in addition, the study proposes a hybrid consensus algorithm called SMO, which combines the Proof-of-Work consensus algorithm and the Proof-of-Stake consensus algorithm, in addition to creating an additional layer of protection from Distributed Ledger, especially in malicious blocks that are discovered, and machine learning algorithms for early detection of malicious blocks to be used in the Ramallah Smart Parking system (RSP)

Case study methodology: The thesis adopts a case study methodology, focusing mainly on the Ramallah smart city project and the application of blockchain technology in the Ramallah smart parking system (RSP) and comparing it with parking systems in smart cities around the world and measuring the effectiveness of the proposed RSP system by comparing it with other systems that have been studied.

Interdisciplinary perspective: The study takes an interdisciplinary approach, drawing on knowledge and theories from areas such as blockchain technology, smart cities, studying some smart city applications around the world and taking advantage of the strengths they possess and avoiding the weaknesses of the Ramallah Smart Parking System - RSP.

Limitations:

1. Generalizability: The results and recommendations of the study may be limited to generalization outside the specific context of the city of Ramallah and some other

Palestinian cities that are similar to the city of Ramallah in the infrastructure of technology and communications.

2. Time constraints: Due to the time constraints inherent in the master's thesis, the research may not cover the full scope of blockchain applications in smart cities, but rather focus on specific aspects, with a primary focus on the smart parking system in Ramallah.
3. Data Availability: The availability of accurate and comprehensive data related to the implementation and performance of blockchain technology in the Ramallah Smart City project may constitute a limitation of the study as there is a dearth of research related to Blockchain in Palestine or in the city of Ramallah.
4. Stakeholder Perspectives: The study may not capture the views and experiences of the stakeholders involved in the Ramallah Smart City project or the implementation of blockchain in smart cities due to the need for high-level coordination between the Ramallah Municipality, the Palestinian Ministry of Transportation, and the Palestinian Police, so the research was adopted in the first place. on the available literature.
5. Financial costs: The implementation of the proposed project for the study needs to be approved by the responsible authorities, as it needs financial funding to provide the basic requirements for its implementation, such as Internet of Things sensors, as well as building private Blockchain networks for the parties to the system such as the Palestinian police and the Palestinian Ministry of Transport, in addition to that the WIFI network of the smart city of Ramallah does not It covers all areas of the city, in addition to the high costs of using the third generation network.

6. Confidence in Blockchain Technology: Due to the scarcity of research related to Blockchain technology in Palestine and the lack of applications that depend on this technology in Palestine, this may lead to insufficient knowledge by the public in the smart city of Ramallah about the benefits and advantages achieved by Blockchain technology, and this requires spreading knowledge awareness Tell the audience about the importance of using applications based on this technology.

1.9 Thesis Organization

This study titled " Implementing Artificial Intelligence in Blockchain for Ramallah Smart City in Palestine: A Case Study" is organized into several chapters to provide a structured and comprehensive exploration of the topic. The following outlines the organization of the thesis:

In the first chapter of this study, which is titled "Introduction", an overview of the research topic was provided, the rationale for conducting the study was presented, and the objectives and research questions were set. In addition, the importance of blockchain technology in the context of smart cities was highlighted, with a special focus on the city of Ramallah in Palestine.

In the second chapter, which is titled "Literature Review", an introduction to the study, research questions and objectives are reviewed, then an overview of blockchain technology, then applications of blockchain in smart cities, an overview of the smart city of Ramallah, and then a case study (Ramallah Smart Parking - RSP) is presented. And then review research, developments and future directions.

In the third chapter of this study, which is titled " Blockchain and Smart City Technology ", the basic concepts and principles of Blockchain Technology are explored, the

decentralized nature of this technology is discussed, and its components and consensus mechanisms used by the Blockchain are discussed. Also included "Blockchain Consensus Algorithms", the concept of Consensus Algorithms was introduced, the classifications of consensus algorithms were also dealt with and the conditions that must be met in the consensus algorithm that will be used in Ramallah Smart Parking system (RSP) to be compatible with the needs of Ramallah Smart City were dealt with, then comparisons were made of the most prominent consensus algorithms widely used in blockchain technology, and then the consensus algorithm was studied. Proof-of-Work (PoW), Proof-of-Stake (PoS) algorithm, Proof-of-Activity (PoA) algorithm extensively, and then propose a new hybrid algorithm called SMO, which has been reviewed and studied. Also included "Smart Cities", the concept of smart cities was introduced and the main components and features of smart cities and the most prominent technologies used in them were explored. Also included "Ramallah Smart City", the Ramallah Smart City project in Palestine was reviewed, its infrastructure for technology and communications was explored, the challenges facing the smart city of Ramallah were studied, and the opportunities for applying Blockchain technology in Ramallah Smart City were studied. Also included "Blockchain Applications in Smart Cities", an overview of blockchain applications in smart cities was given, then a case study of blockchain in some smart city projects around the world, and then a comparison was made between blockchain solutions in smart city projects. Also included "Ramallah Smart Parking - RSP", an application system for blockchain technology was proposed in the smart city of Ramallah, which bears the name Ramallah Smart Parking System - RSP, which aims to contribute to transforming the transport sector into a smart transport to contribute to reducing traffic congestion. In the streets of the city and reducing carbon emissions resulting from vehicle

exhausts as well as contributing to raising the security level of the city by combating illegal and expired vehicles as well as combating vehicle theft crimes with full use of the advantages of blockchain technology, as multiple technologies have been integrated into the system, including Public Blockchain and Private Blockchain, Consortium Blockchain, and InfluxDB.

In the fourth chapter, "SMO algorithm Experimental work", practical experiments were carried out on the machine learning algorithms used in the proposed SMO algorithm, which are Random Forests ML Algorithm, K-means algorithm ML algorithm, Hidden Markov Models (HMMs) ML algorithm, Anomaly detection ML algorithm, and then Work on analyzing the results and verifying the level of performance and the efficiency and effectiveness achieved by the proposed hybrid consensus algorithm SMO.

In the Fifth chapter, "Conclusion", a summary of the results, the contribution of the study, the practical results, the limitations and challenges it encountered, and recommendations for future research were reviewed.

2 Chapter 2: Literature Review

2.1 Introduction

Blockchain technology is a distributed ledger that performs secure, transparent, and tamper-proof transactions and has the potential to revolutionize many sectors, including the smart city sector.

A smart city is a city that relies on the use of information and communication technologies (ICT) to improve the quality of life for its citizens and respond quickly to the needs and requirements of the city. ICT can be used to improve smart city infrastructure, increase and upgrade services, and overall efficiency. Smart cities seek to enhance and raise the level of efficiency and response to many sectors, most notably the education, health, transportation, energy, economy and other sectors through Blockchain technology. Examples of this are securely store and manage data, Track the provenance of goods and services, facilitate payments, automate transactions and Improve transparency and accountability.

This study will explore the potential of blockchain technology to be applied to the smart city sector. It will focus on a case study of Ramallah smart city, a city in Palestine.

The study will begin with an overview of blockchain technology and its mechanism of action, the study also deals with the consensus algorithms used in the blockchain, studying the algorithms that are widely used, working on analyzing them, and proposing a new hybrid consensus algorithm called SMO that is compatible with the capabilities of the city of Ramallah to be used in the system proposed by the study, RSP. then an overview of smart cities, then an overview of Ramallah Smart City, and then deal with Blockchain Applications in Smart Cities. The study then addresses a proposal for smart parking based on blockchain technology named (Ramallah Smart Parking) abbreviated as RSP, then the

study reviews the results, and in conclusion the study discusses the challenges and limitations of using blockchain technology in smart cities. It will also make recommendations for future research.

2.2 Blockchain and Smart City Technology

Blockchain technology uses a distributed ledger to securely store and transfer digital assets or information in a decentralized, transparent manner. Blockchain, at its heart, is a digital, distributed, and decentralized ledger that keeps track of transactions across numerous computers, or nodes (Nakamoto, 2008). By fostering participant consensus and preserving openness and integrity, this distributed ledger eliminates the need for a centralized authority (Swan, 2015). The state of the ledger is validated and agreed upon using consensus procedures, such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) (Buterin, 2013). These safeguards guard against fraud, duplication of transactions, and data manipulation (Popov, 2005). Additionally, blockchain technology incorporates smart contracts, which are self-executing agreements that automatically enforce predefined conditions. Smart contracts operate within the blockchain and eliminate the need for intermediaries, enhancing efficiency and reducing costs (Swan, 2015).

2.3 Blockchain Consensus Algorithms

Presented a review of the most important consensus algorithms and worked on analyzing the most common algorithms and then making comparisons and identifying the strengths and weaknesses of each of them, and then a new hybrid consensus algorithm called SMO was proposed that works with the same principle as the PoA consensus algorithm, but it introduced an additional protection layer called Block Bank It contains a Distributed

ledger consisting of malicious blocks that were detected earlier, as well as machine learning algorithms Random Forests Algorithm, K-means algorithm, Hidden Markov Models (HMMs) and Anomaly detection algorithm, which works on early detection of malicious blocks and achieves a high level of security from Security threats to blockchain technology, as well as prevent wastage of computer resources to verify the validity of blocks, and contribute to the reduction in energy consumption required for this.

2.4 Blockchain Applications in Smart Cities

Smart cities are urban environments that leverage advanced technologies to improve the quality of life for residents and optimize resource management. These cities encompass various components, including smart infrastructure, IoT devices, data analytics, and interconnected systems (Caragliu, Del Bo, & Nijkamp, 2011). Integrating blockchain technology into smart cities offers several advantages. Firstly, blockchain enhances data security and privacy by providing a transparent yet tamper-resistant platform for storing and sharing sensitive information (Zhang, Wen, & Huang, 2018). Secondly, blockchain enables efficient and reliable transactions by reducing the need for intermediaries and facilitating peer-to-peer interactions (Yli-Huumo et al., 2016). Numerous case studies have demonstrated the application of blockchain in smart cities globally. For example, Dubai has implemented blockchain for land registration and real estate transactions, enhancing transparency and reducing fraud (Dubai Future Foundation, 2020). Similarly, the city of Austin, Texas, utilizes blockchain for identity management and voting systems, increasing trust and security (IBM, n.d.). However, there are challenges and limitations to implementing blockchain in smart cities. These include scalability issues, high energy consumption, regulatory complexities, and the need for interoperability between different blockchain platforms (Zhang et al., 2018; Yli-Huumo et al., 2016).

2.5 Ramallah Smart City

Ramallah Smart City is a project aimed at creating a sustainable and competitive environment by partnering with the private and government sectors. It focuses on six axes, including technological infrastructure, smart governance, smart education, smart economy, smart mobility, and smart environment. The project aims to improve communication, service delivery, and community engagement through data gathering tools, mapping cultural assets, and a social platform. Challenges such as occupation, limited energy supply, restricted water access, waste management, and population density present opportunities for implementing smart solutions. Blockchain adoption in Ramallah Smart City can enhance data security, transparency, and accountability while promoting decentralized applications, digital identity management, and peer-to-peer energy trading for sustainability and economic opportunities (Ramallah Municipality, n.d.; Resilient Ramallah 2050; Crosby et al., 2016 (Kshetri, Nir. 2018); Liang et al., 2018; Scott et al., 2018; Swan, 2015).

2.6 Case Study: Ramallah Smart Parking – RSP:

A study of the application of the Ramallah Smart Parking System (RSP) based on Blockchain technology aims to contribute to alleviating the traffic crisis in the streets of Ramallah city by reducing the time for drivers to search for parking for their vehicles, which leads to reduced fuel consumption and lower transportation costs as well as leads To reduce pollution of carbon emissions resulting from fuel combustion, in addition to contributing to raising the level of security in the smart city of Ramallah by combating illegal cars and cars with expired licenses, as well as combating car theft and contributing to locating people wanted by the executive body (police) or vehicles required to be kept it or follow it.

The RSP system consists of several ACTORS, including users, smart parking, Ramallah Municipality, the Ministry of Transportation, and the Palestinian Police.

2.6.1 Users:

As the system can be accessed through websites or mobile applications and it is based on the Blockchain, where the users in the system are divided into two types, the first is the regular users (drivers) and the second is the private Administrator in the smart municipality of Ramallah, where each user of the regular users (drivers) to create a rare and single account on the system after entering and attaching all the required data from it, which is stored on blockchain, the system enables users to search for empty parking lots in the place near the user, or it can search for parking in a specific area that the user wants Going to it, after the user chooses the parking lot he wants to reserve, a smart contract is created on the Blockchain network stating that the parking lot has been reserved and the status of the parking on the network is changed that it has become unavailable (reserved). After completion, the user pays through the system, and the payment system was used in visa cards and not in currencies Digital, as it is prohibited from circulation in Palestine, and based on the above, we can contribute to alleviating the traffic crisis in the streets of the city of Ramallah by reducing the time required for drivers to search for parking spaces and reduce their fuel consumption, as well as reducing carbon emissions that cause pollution and resulting from fuel combustion. The second type of users (Administrator) is private in the smart municipality of Ramallah, where he is able to add and delete the parking lot, interact with the notifications received from the system about occupying an unreserved parking lot or occupying a parking lot by a person other than the person who made the reservation.

2.6.2 Smart parking:

The parking lot contains cameras and sensors that operate on the IOT network, where it compares the number of the vehicle that reserves the parking lot with the records of the traffic department to verify that the vehicle is included in the vehicle register and that its license is valid, as well as compares the vehicle number with the Palestinian police records to verify that the vehicle is not required to be kept. Or that its ownership does not belong to a person who is wanted to be arrested. In the event that the vehicle is illegal, the license has expired, or it is wanted by the police, or it is owned by a person who is wanted to be arrested, and he is the one who reserved the parking lot, the system immediately informs the police of the parking location, number, vehicle data, and photos of the vehicle. And for the driver so that they can take legal action.

In the event that the parking lot has been reserved and the car has been moved without completing the payment process, the system immediately communicates with the user and asks him if he is the one who moved the vehicle or if it was moved with his knowledge. Data, details, and photos of the vehicle and the last driver of the vehicle.

2.6.3 RSP Techniques:

The proposed Ramallah Smart Parking (RSP) system utilizes a Consortium Blockchain for enhanced privacy, security, scalability, and governance (Khan, Salah, & Javed, 2019). Consortium blockchains allow trusted entities like the user, Ramallah municipality, Ministry of Transport, police, and Internet of Things (IoT) to control data visibility and protect sensitive information. The integration of InfluxDB as the IoT database offers advantages such as efficient storage and retrieval of time series data, scalability, and real-time analytics capabilities (Deng et al., 2020). InfluxDB's specialized features for time

series data enable seamless ingestion, analysis, and storage of data from various IoT devices in smart city applications. Linking the consortium blockchain with InfluxDB provides a robust solution for secure and decentralized data management. The consortium blockchain ensures data authentication, access control, and auditability, while InfluxDB optimizes time series data storage and retrieval (Chatterjee et al., 2018; Dorri et al., 2019; Zheng et al., 2020).

The proposed hybrid algorithm SMO guarantees the realization of the needs of the city of Ramallah in blockchain applications, which have been developed for use in the Public Blockchain network in RSP andits terms of high security availability, scalability, efficiency, decentralization, and minimizing energy use.

2.7 Current Research and Developments:

Recent studies and research have highlighted the potential of blockchain technology in transforming smart cities. The researchers explored various aspects of blockchain implementation, including data management, governance models, and security frameworks. For example, Li et al. (2020) A study on the integration of blockchain and edge computing for efficient data sharing and processing in smart cities. They proposed a decentralized framework that improves data integrity and reduces latency. Another area of research focuses on emerging innovations and trends in blockchain technology for smart cities. The scientists investigated novel applications such as blockchain-based energy trading systems, decentralized supply chain management, and blockchain-enabled mobility solutions. These innovations aim to promote efficiency, transparency, and sustainability in urban environments (Li et al., 2020; Zanella et al., 2019). Furthermore, comparative analyzes of blockchain applications in smart cities were conducted to assess successes, challenges, and lessons learned from global implementations. Case studies

from different regions, such as Dubai, Singapore, and Estonia, contribute to identifying best practices, assessing scalability, and analyzing the impact of blockchain on citizen engagement, governance, and service delivery (Cho, Lee, & Nam, 2021; Yan Wen and Rana, 2019). This comparative analyzes contribute to a deeper understanding of the diverse approaches and outcomes of applying blockchain in smart cities.

2.8 Artificial Intelligence in Blockchain Integration

Artificial intelligence (AI) is the broad concept of machines carrying out tasks in a way that we would consider "smart" if done by humans. Machine learning is a subset of AI that involves training machines to learn from data, enabling them to make predictions, decisions, or perform tasks without being explicitly programmed. Essentially, machine learning is a crucial technique within the broader field of artificial intelligence, providing the ability for machines to learn and improve from experience, making AI applications more adaptable and intelligent over time. As one of the most prominent benefits obtained when using artificial intelligence is work on Enhances efficiency, automates tasks, and aids in decision-making (Russell, S. J. and Norvig, P. 2009).

In this study, artificial intelligence is applied in blockchain technology through the utilization of machine learning algorithms. The aim is to leverage the advantages provided by AI and harness them within blockchain technology. Machine learning algorithms (Random Forests, K-means, Hidden Markov Models, and the Isolation Forest anomaly detection) were employed within the proposed SMO consensus algorithm.

2.9 SMO algorithm Experimental work

In this chapter resented many experiments to measure the effectiveness and efficiency of the proposed hybrid consensus algorithm SMO in early detection of malicious blocks, as

the experiments that were conducted in the additional protection layer Block Bank in the proposed algorithm SMO proved the effectiveness of the hybrid consensus algorithm SMO, where it was able within one minute to analyze And classifying 227250 blocks and identifying malicious blocks from them without the need to consume computer resources, as is the case in other consensus algorithms, as well as finding the strengths of the SMO algorithm, including that the more malicious blocks the system detects, the higher the speed in detecting blocks In the future, the SMO consensus algorithm increased the decentralization of the system, as the early detection of malicious blocks is done before they reach the audit stage in the next step by means of the PoS algorithm. The SMO algorithm was also able to raise the level of security of the blockchain by adding the additional security layer Block Bank to detect malicious blocks before Subject to auditing and that it provides 5 stages to verify the block and not as is the case in other consensus algorithms in relying only on the result of the audit stage only, the SMO consensus algorithm constituted an incentive for auditors to participate in audits as they are nominated for blocks that were not recognized by the Block Bank security layer and thus The exploitation of their computer resources in the blocks with a high probability that they are correct blocks, and therefore their chances of achieving gains from the audit process are higher than in other consensus algorithms. The proposed consensus algorithm SMO achieved an ideal solution for Sybil Attack Resistance and DoS Attack attacks. SMO from short-term attacks Because the work on examining and discovering the block is not only done by auditors, but also preceded by machine learning algorithms, the hybrid consensus algorithm SMO also prevents the chances of success of long-term attacks.

2.10 Conclusion and Future Directions

In conclusion, this literature review has highlighted the potential of blockchain technology in the smart city sector, with a specific focus on the case study of Ramallah Smart City in Palestine. Blockchain technology offers benefits such as enhanced data security, transparency, and efficient transactions, which are crucial for the development of smart cities. Key insights and contributions to this review include a comprehensive overview of blockchain technology and its applications in smart cities and analysis of the Ramallah Smart City project. The study also presented a case study of the Ramallah Smart Parking System Proposal (RSP), which demonstrated how blockchain technology can address traffic congestion and improve security in a smart city. However, there are still challenges and limitations to implementing blockchain in smart cities, including issues Scalability, energy consumption and regulatory complexities.

For future research, there is a need to further explore the integration of blockchain with emerging technologies such as edge computing, the Internet of Things, and artificial intelligence to enhance data sharing, processing, and analytics in smart cities. Comparative analyzes of blockchain applications in different smart city projects can provide valuable insights into best practices and lessons learned. Further research should also focus on addressing the challenges and limitations of blockchain implementation, such as scalability, energy efficiency, and interoperability. Practical implementations of blockchain in smart cities should consider the specific needs and contexts of each city, and collaborative efforts between government, private sectors, and research institutions are essential for successful implementation. Overall, the potential of blockchain technology in the smart city sector is promising, and further research and practical implementations will contribute to its continued development and optimization. In

addition to the above, there is a need to conduct more research on smart cities, blockchain applications, and the Internet of things in Palestine, since the trend to transform the city of Ramallah into a smart city may be the first step towards transforming the rest of the Palestinian cities into smart cities, which requires more research and suggestions that contribute to the development.

In addition to the above, the study also presented a proposal for a new hybrid consensus algorithm called SMO, where this algorithm was built by combining the PoW algorithm and the PoS algorithm, in addition to an additional protection layer called Block Bank consisting of Distributed Ledger for malicious blocks and machine learning (ML) algorithms. Such as Random Forests Algorithm, K-means algorithm, Hidden Markov Models (HMMs) and Anomaly detection in order to work on early detection of malicious blocks, protect the system from different types of attacks faced by the blockchain, and ensure that the blockchain is compatible with the capabilities of Ramallah city.

3 Chapter 3: Blockchain and Smart City Technology

3.1 Blockchain Overview

The interest in Blockchain surged in 2008 when Nakamoto introduced Bitcoin, a digital currency utilizing a peer-to-peer network. This coincided with the global financial crisis, leading many to attribute the crisis to central administration. Blockchain technology emerged as a solution, offering smart contracts based on consensus algorithms that foster transparency and trust among contract parties. Whereas, the Blockchain can be defined as a distributed ledger, which is an environment for storing and processing data by a group of nodes that operates on the principle of complete mistrust between them (Dinh et al. (2018)), and according to (Saghiri, 2020) Blockchain is divided into three types: Public Blockchains, Private Blockchains, and Consortium Blockchains. Public Blockchains allow anyone to join or leave the network with some incentives for participants, for example Bitcoin.Private Blockchain provides permissions in writing for a particular institution or entity, but reading the data can be for everyone or is restricted. Consortium Blockchains is a mixture of Public Blockchains and Private Blockchains.As the Blockchain system operates on a peer-to-peer (P2P) network. According to (Hakak et al., 2020), Blockchain was able to attract the attention of researchers and investors due to its many characteristics, which are summarized in Robust, Incorruptible and Secure, Consensus algorithms, Transparency and Validation of Information. As the decentralized nature of Blockchain and its reliance on a distributed ledger and storing data in a chain of blocks was able to achieve the Robust feature, and it achieves the Incorruptible and Secure feature by distributing data and information over the entire network and thus any fraud process that requires high computational resources, in addition to that as a result of data distribution On the entire chain, it also achieved the advantage of Transparency and

Validation of Information, as users can verify the validity of the data and ensure its integrity and that it has not been tampered or modified. Blockchain also uses consensus algorithms that work within a set of protocols and whose main work is to ensure the legitimacy of transactions, The most prominent consensus algorithms in Blockchain are Proof of Work (PoW) and Proof of Stake (PoS), Proof of Importance (PoI), Delegated PoS (DPoS), Tangle, Proof of Burn (PoB), Proof of Elapsed Time (PoET), Byzantine Fault Tolerance (BFT), Practical Byzantine Fault Tolerance (PBFT).

3.2 Blockchain Architecture

According to Feng et al. (2019) the basic Blockchain architecture consists of three main layers. The Peer-to-peer network forms the first layer. While, databases (Global ledger) form the second layer, the applications layer forms the third layer. In the first layer, the P2P network was relied on in order to provide decentralization. The P2P network provides free communication between the various Blockchain nodes in terms of implementing communication and query among them, and that all nodes are equal in terms of application without the need for a central server. The nodes are consuming and providing information through the exchange of requests and the answers to them among themselves and synchronize data blocks. The responsibility of the global ledger layer is to provide a complete trust between different accounts by reliably transmitting messages between them and providing alias addresses for accounts consisting of a unique digital address that is generated through the use of a public encryption key by the user. The communication between two or more addresses is carried out through a transaction where A transaction is defined here as a record containing the address of the sender and the recipient, messages, timestamps, and signatures of the relevant participants. Blockchain provides flexibility for exchanging messages between participants through the smart contract. The

smart contract has been defined by many definitions, the most prominent of which was in Bitcoin as the process of executing a text during the confirmation of the cryptocurrency. Where the smart contract and the messages it contains are recorded in the global ledger in a list of blocks that increases continuously so that each block points to the previous block and the subsequent block except for the configuration block refers to the subsequent block being the first block created in the chain and the blocks are arranged on the basis of their chronological sequence so that it starts The blocks are interconnected from the configuration block to the most recent timestamp generated block where smart contracts are organized in the form of a Merkle Hash tree, where transactions are broadcast over the entire P2p network using one of the agreed consensus mechanisms. The private application layer of the Blockchain provides application interfaces for users to interact with each other, see figure no. (1):

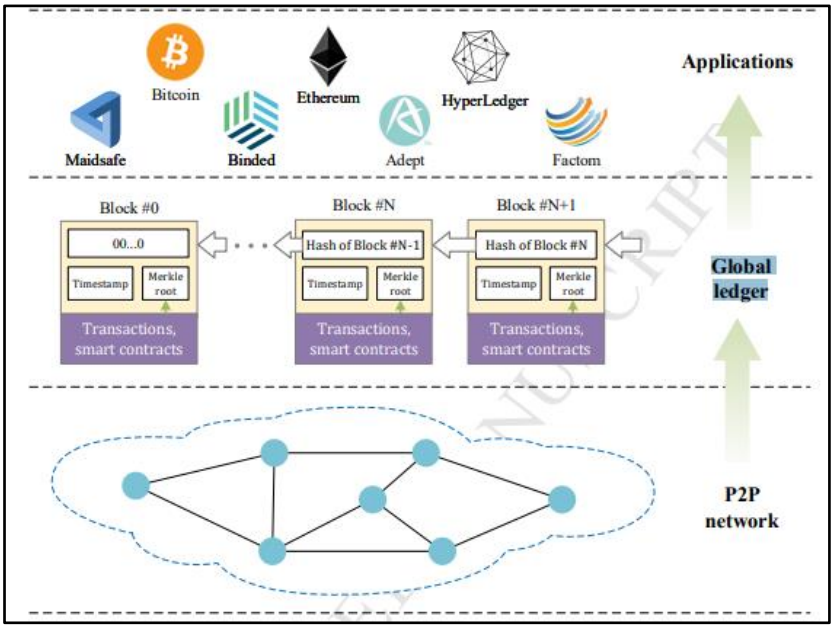

Figure 1:Blockchain Architecture (Feng et al., 2019).

(Yao et al. 2021). Introduced the Blockchain architecture in a broader way, as it consists of four main layers, namely infrastructure layer, network layer, data layer, consensus layer, and application layer. See Figure 2.

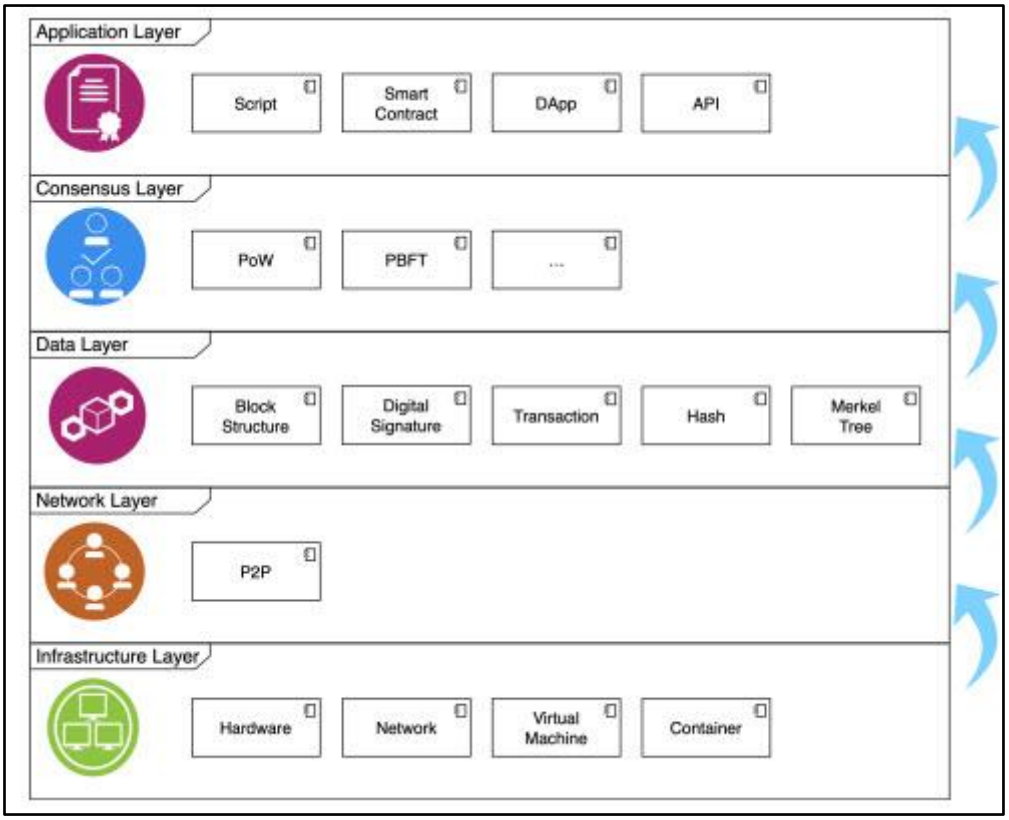

Figure 2: Blockchain Architecture (Yao et al. 2021)

- **Infrastructure Layer** included Hardware, network architectural tools, and deployment environments for blockchain systems such virtual machines and Docker containers.
- **Network Layer** verification mechanisms for transactions and blocks are implemented. The peer-to-peer (P2P) networks used by the blockchain network, whose nodes display equality, dispersion, and autonomy, operate the network. A new node joins the network and uses the Transmission Control Protocol (TCP) three-way handshake to connect to other nodes. The node can act as a fully functional node for submitting and validating transactions and synchronizes block information with connected nodes. Newly created blocks are broadcasted for validation and added to the blockchain if they are valid. As long as there are functioning nodes in the network, the distributed structure of the blockchain ensures data availability even if some nodes are unavailable.

- **Data Layer** Data is captured and saved using the blockchain structure at the data layer of a blockchain system, offering traceability and tamper-proof properties. Each data block in Bitcoin is made up of a block header and a block body. System data, previous block hash values, difficulty targets, random numbers, Merkel tree roots, and timestamps are all included in each block's header. The block body has a complete Merkel tree made up of these validated transactions. Data integrity is maintained through the Merkel tree, which makes sure that any update to the data propagates from the leaf nodes to the root. The Merkel tree generates a unique root that is recorded in the block header, and the data in the block body is the bulk of the blockchain ledger. To determine the block's hash value, the block header is hashed.
- **Consensus Layer** is at the heart of the blockchain's consensus process where extremely decentralized nodes decide whether or not a block of data is genuine. Blockchain technology's capacity to scale is largely dependent on key consensus techniques including Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT). Nodes are encouraged to participate in the blockchain's security verification job by using incentive models, which are particularly effective in processes like PoW.
- **Application Layer** included Decentralized Applications (DApps), smart contracts, script codes, and application programming interfaces (APIs).

3.3 Block Structure

Each Block in Blockchain consists of two main parts, Block Header and Block Body. The first section includes Block Version, Parent Block Hash, Timestamp, Nonce, nBits and

Merkle Tree Root Hash while Block Body includes Transaction Counter, Hash and Transaction (Chandel et al., 2019). See Figure 3.

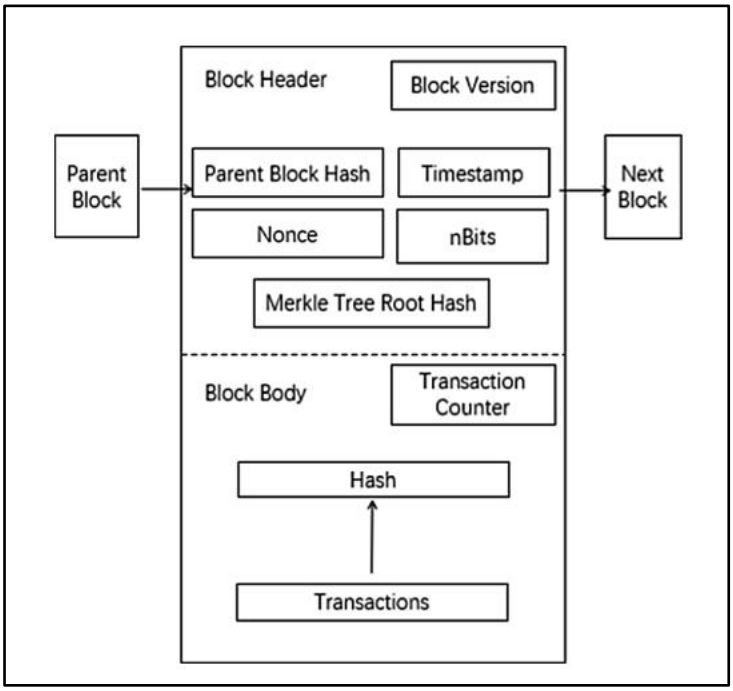

Figure 3: The structure of a block in a Blockchain (Chandel et al., 2019).

3.4 Blockchain Types

1. Public Blockchain: This type of Blockchain crystallizes a concept of digital trust, whereby anyone can send, read and share transactions. Examples include Etherum and Hyperleger (AbuSamra et al., 2020).
2. Private Blockchain: This type of Blockchain is managed by network administrators so that it is joined by their consent, where one or more entities are in control of the network with reliance on a third party to perform transactions, where the participating entity is aware of the transaction known to it while preventing access to others for the transaction (Dinh et al., 2017).
3. Consortium Blockchain: This type of Blockchain consists of a semi-decentralized network so that it does not give members to a single entity and gives them to a group of nodes. It provides higher network security than Public Blockchain and it

provides a large degree of control and faster processing while ensuring security and efficiency. However, this type has fewer nodes than Public Blockchain and is less transparent than it, and some researchers consider it a hybrid system of Public Blockchain and Private Blockchain (Gai et al., 2019).

3.5 Blockchain Wallet

Blockchain wallets are digital wallets that store cryptocurrencies, and they are used to send, receive, and manage these digital assets. There are various types of blockchain wallets, including non-deterministic wallets, deterministic wallets, hierarchical deterministic wallets, brain wallets, paper wallets, hardware wallets, online wallets, mobile wallets, multi-signature wallets, full node wallets, light node wallets, web-based wallets, desktop wallets, cold storage wallets, hot storage wallets, custom wallets, and non-custodial wallets. Each type of wallet has its own definition, advantages, disadvantages, and uses.

3.5.1 Types of Blockchain Wallets:

- **Non-deterministic wallets:** A type of Blockchain wallet that generates a new private key for each transaction to increase anonymity and avoid the reuse of the same address. They are more vulnerable to brute force assaults as a result, which makes them less secure than other wallet kinds and more difficult to backup. These wallets are appropriate for users who prioritize privacy over security and do not regularly engage in transactions. Non-deterministic wallets promote anonymity, but because of the randomness of the production of their private keys, they are inappropriate for users that value security and usability over anonymity. Users that want to safeguard their

identities and maintain the secrecy of their transactions should choose for non-deterministic wallets (Bitcoin.org, n.d.).

- **Deterministic wallets:** a type of blockchain wallet that creates a series of private keys from a single seed value. Since the seed value may be used to generate all the related private keys, backing up and restoring the wallet is made simple. Since the seed values used in deterministic wallets are lengthy and complicated, making them difficult to crack through brute force attacks, they are thought to be more secure than non-deterministic ones. They are particularly appropriate for users that often interact in cryptocurrencies and place a higher importance on security than privacy (Bitcoin.org, n.d.). The main benefit of deterministic wallets is their simple backup and ease of use. Users can access all of their private keys by just remembering the seed value, which makes them a desirable choice for frequent bitcoin transactions. Deterministic wallets, however, can compromise users' privacy because all related private keys can be generated from the seed value. Deterministic wallets could also be more susceptible to certain attacks, including side-channel attacks (Bitcoin.org, n.d.). Users that often deal in cryptocurrencies and value security above privacy are best suited for deterministic wallets. They are frequently used since they support several cryptocurrencies and are accessible in both hardware and software formats (Bitcoin.org, n.d.).
- **Hierarchical deterministic wallets (HD wallets):** a type of Blockchain Wallet that improves on deterministic wallets by incorporating a hierarchical structure to the seed value, allowing for the creation of several unique key pairs. This enhances the versatility and management of transactions of HD wallets. HD wallets provide the convenience of easy backup and restoration of the wallet, with the seed value being

used to regenerate all private keys. HD wallets are more secure than non-deterministic wallets, as they utilize long and complex seed values that are resistant to brute force attacks (Bitcoin.org, n.d.). HD wallets are beneficial due to their versatile organization capabilities, as they can produce numerous distinct key pairs that allow for the efficient management of transactions. Additionally, HD wallets offer enhanced security by using long and complex seed values, making them more resistant to brute force attacks. However, HD wallets may compromise privacy, as the hierarchical structure of the seed value could potentially link transactions back to a single wallet (Bitcoin.org, n.d.). HD wallets are best suited for individuals and businesses that require frequent cryptocurrency transactions and prioritize both security and organization. These wallets are widely used and can be found in both software and hardware forms, and are compatible with various cryptocurrencies (Bitcoin.org, n.d.).

- **Brain wallets:** a type of Blockchain Wallet that allow users to create private keys from a passphrase or set of words, rather than a randomly generated seed value. This means that users can create a private key that is easy to remember but still secure. One advantage of brain wallets is that they are easy to use and can be accessed from anywhere, as they do not require users to store a physical key. However, brain wallets are less secure than deterministic wallets, as passphrases can be vulnerable to dictionary attacks or other types of guessing attacks (Bitcoin.org, n.d.). Brain wallets are best suited for users who prioritize convenience over security and do not store large amounts of cryptocurrency. They are useful for users who frequently need to access their wallets from different devices or locations and do not want to carry a physical key. However, brain wallets should not be used to store large amounts of cryptocurrency, as they are less secure than deterministic wallets (Bitcoin.org, n.d.).

brain wallets are a convenient and accessible option for users who prioritize ease of use and accessibility. However, they are less secure than deterministic wallets and should not be used to store large amounts of cryptocurrency. Brain wallets are widely available and can be used with various cryptocurrencies (Bitcoin.org, n.d.).

- **Paper wallets:** a type of Blockchain Wallet that involve printing out the public and private keys on a physical piece of paper, which can be used to access and manage cryptocurrency. One advantage of paper wallets is their high level of security, as they are not connected to the internet and therefore less vulnerable to cyberattacks. Additionally, paper wallets offer a high degree of privacy, as the user can generate a new wallet for each transaction, making it difficult for others to trace their transactions (Bitcoin.org, n.d.). However, paper wallets are not user-friendly, as they require technical expertise to set up and manage. Moreover, paper wallets are susceptible to physical damage, such as fire or water damage, which can render the wallet unusable. Finally, paper wallets may not be practical for frequent transactions, as the user needs to manually enter the private key each time, they want to access the wallet (Antonopoulos, 2014). Paper wallets are best suited for users who prioritize security and privacy over convenience and frequently store their cryptocurrency for long periods of time. Paper wallets are particularly useful for storing large amounts of cryptocurrency that will not be accessed frequently, such as long-term investments (Bitcoin.org, n.d.). Moreover, paper wallets are a popular option for those who are concerned about the security of online wallets and exchanges. However, it is important to note that paper wallets should be generated using a secure, offline device to ensure maximum security (Antonopoulos, 2014).

- **Hardware wallets:** a type of blockchain wallet that provide enhanced security by storing private keys offline, often in the form of a physical device. This makes them less vulnerable to hacking and malware attacks, as the private keys are not connected to the internet except when needed for a transaction. Hardware wallets also often include features such as PIN codes and two-factor authentication to further enhance security. The downside of hardware wallets is that they can be costly and may not be as convenient as software wallets for frequent transactions (Dinh et al., 2018). One major advantage of hardware wallets is their enhanced security through offline storage of private keys and additional security features such as PIN codes and two-factor authentication. This makes them an ideal choice for users who prioritize security over convenience and frequently store large amounts of cryptocurrency. However, hardware wallets can be expensive and may not be suitable for users who need to make frequent transactions or who have smaller amounts of cryptocurrency to store (Bitcoin.org, n.d.). Hardware wallets are best suited for users who prioritize security and store large amounts of cryptocurrency. They are particularly useful for long-term storage of cryptocurrency, as they offer a high level of protection against hacking and malware attacks. Hardware wallets are available from various manufacturers and support a range of cryptocurrencies (Bitcoin.org, n.d.).
- **Online wallets:** also called web wallets, are a kind of blockchain wallet that stores private keys on a web server, making them accessible through any internet-connected device. The main benefit of online wallets is their convenience, as users can easily access their wallets from anywhere with an internet connection without the need for downloads or installations. However, online wallets have some drawbacks, including the fact that they are less secure than other wallet types and vulnerable to hacks and

phishing attacks. Additionally, online wallets rely on third-party providers, which can pose a risk of service disruption or loss of funds. Online wallets are best suited for users who prioritize convenience over security and are not dealing with significant amounts of cryptocurrency. However, for users who hold substantial amounts of cryptocurrency, offline storage solutions such as hardware wallets may be more appropriate (Bitcoin.org, n.d.).

- **Mobile wallets:** a type of blockchain wallet that allow users to access their cryptocurrency funds through a mobile device, such as a smartphone or tablet. One of the main advantages of mobile wallets is their convenience, as users can easily manage their funds on the go and make quick transactions. Mobile wallets also offer enhanced security features such as biometric authentication, PIN codes, and encryption. However, mobile wallets are vulnerable to risks such as device loss, theft, or malware attacks, which can compromise the security of the funds stored in the wallet. Additionally, some mobile wallets may not support all cryptocurrencies or may have limited features compared to other types of wallets. Mobile wallets are best suited for users who frequently transact in cryptocurrencies and prioritize convenience and accessibility over security. However, for users who hold significant amounts of cryptocurrency, offline storage solutions such as hardware wallets may be more appropriate (Bitcoin.org, n.d.).
- **Multi-signature wallets:** it's a type of blockchain wallet that require multiple private keys to authorize transactions, also known as multisig wallets. This added layer of security makes multisig wallets less vulnerable to theft or hacks than single-signature wallets. Depending on the required level of security, multisig wallets can be established with various signature combinations, such as 2-of-3 or 3-of-5. One

advantage of multisig wallets is that they allow for shared control over funds, making them useful for businesses or joint accounts. Additionally, multisig wallets can be used to create backup systems, where one key is held by the user and the other is held by a trusted third party. However, multisig wallets can also have some disadvantages, such as the complexity of setting up and using multiple keys, and the possibility of losing access to funds if one or more key holders are unavailable. Multisig wallets are best suited for users who prioritize security and want to share control over funds or create backup systems (Bitcoin.org, n.d.).

- **Full node wallets:** a type of blockchain wallet that downloads and verifies the entire blockchain ledger, providing users with full control over their transactions and privacy. One advantage of full node wallets is their security, as users can verify transactions themselves without relying on third-party providers. Additionally, full node wallets offer enhanced privacy, as they allow users to mask their IP addresses and avoid the risk of de anonymization. However, full node wallets also have some drawbacks, including their high storage and computational requirements, which may make them less accessible for some users. Furthermore, full node wallets may require significant time and resources to set up and maintain. Full node wallets are best suited for advanced users who prioritize security and privacy over convenience and are willing to dedicate the necessary resources to ensure the smooth functioning of the wallet (Bitcoin.org, n.d.).
- **Light node wallets:** also known as thin wallets, are a type of blockchain wallet that do not store a full copy of the blockchain but instead rely on a trusted full node to provide blockchain data. One advantage of light node wallets is their low storage requirements and fast synchronization times. They are also more accessible and user-

friendly than full node wallets. However, light node wallets are less secure than full node wallets because they rely on a trusted third party for blockchain data. Additionally, light node wallets may not support all blockchain features and may not provide the same level of privacy as full node wallets. Light node wallets are best suited for users who prioritize convenience over security and do not require advanced blockchain features. However, for users who prioritize security and privacy, full node wallets may be more appropriate (Bitcoin.org, n.d.).

- **Web-based wallets:** also known as browser-based wallets, are a type of blockchain wallet that can be accessed through a web browser. These wallets rely on a third-party service provider to manage the user's private keys and cryptocurrency. One of the advantages of web-based wallets is their accessibility, as they can be accessed from any device with an internet connection and a browser. Another advantage is the ease of use, as web-based wallets often have a user-friendly interface that makes it simple to send and receive cryptocurrency. However, web-based wallets also have some disadvantages. They can be less secure than other types of wallets, as they rely on the security of the service provider's servers. Additionally, users of web-based wallets have less control over their private keys, which can be a concern for those who prioritize security. Web-based wallets are best suited for users who prioritize convenience and ease of use over security, and who do not hold significant amounts of cryptocurrency (Tschorsch & Scheuermann, 2016).
- **Desktop wallets:** a type of blockchain wallet that store private keys on a user's desktop computer. One advantage of desktop wallets is that they provide users with complete control over their private keys and funds, without relying on third-party providers. Additionally, desktop wallets often offer advanced security features such

as two-factor authentication and multi-signature support. However, desktop wallets also have some drawbacks, including the fact that they are only accessible from the computer on which they are installed. This can limit their convenience and accessibility for users who frequently switch between devices. Desktop wallets are best suited for users who prioritize security and control over convenience, and who primarily use a single desktop computer for their cryptocurrency transactions (Bitcoin.org, n.d.).

- **Cold storage wallets:** a type of blockchain wallet that stores private keys offline, typically on a hardware device or paper. This approach ensures that the private keys are not vulnerable to online attacks, making cold storage wallets one of the most secure types of wallets. Cold storage wallets are commonly used by institutional investors, exchanges, and individuals who hold large amounts of cryptocurrency for an extended period. While cold storage wallets provide superior security, they also come with some drawbacks. For example, they can be more difficult to use than other types of wallets and may require additional setup and maintenance. Additionally, if the hardware device or paper is lost or damaged, there is a risk of losing access to the cryptocurrency. Cold storage wallets are best suited for users who prioritize security over convenience and do not need frequent access to their cryptocurrency holdings (Bitcoin.org, n.d.).
- **Hot storage wallets:** also known as online wallets, are a type of blockchain wallet that store private keys on a device that is connected to the internet, such as a computer or smartphone. One advantage of hot wallets is their ease of use and accessibility, as users can easily access their funds from anywhere with an internet connection. Additionally, hot wallets can be used for everyday transactions and are often

integrated with exchanges and other services, making it easy to buy, sell, and exchange cryptocurrencies. However, hot wallets are considered less secure than cold storage wallets because they are vulnerable to hacks and cyber-attacks. Furthermore, because hot wallets rely on a third-party provider, they may be subject to service disruptions and other technical issues. Hot wallets are best suited for users who need frequent access to their funds and are not dealing with large amounts of cryptocurrency. However, for users who hold significant amounts of cryptocurrency, cold storage solutions such as hardware wallets may be more appropriate (Bitcoin.org, n.d.).

- **Custodial wallets:** a type of blockchain wallet in which a third party, usually an exchange or a service provider, holds the private keys on behalf of the user. This means that the user does not have full control over their cryptocurrency and must trust the custodian to manage their funds securely. One of the main advantages of custodial wallets is their ease of use, as they often offer a user-friendly interface and 24/7 customer support. Additionally, custodial wallets may offer insurance to protect against theft or loss of funds. However, custodial wallets also have some drawbacks, including the fact that they are not as secure as non-custodial wallets since the user does not have full control over their private keys. Moreover, custodial wallets may not support all cryptocurrencies, and their fees may be higher than non-custodial wallets. Custodial wallets are best suited for users who prioritize ease of use and convenience over full control of their cryptocurrency and are willing to trust a third party to manage their funds securely (Grigg, 2019).
- **Non-custodial wallets:** are a type of blockchain wallet that gives users complete control over their private keys and funds. They are also known as self-custody wallets

as they allow users to be their own custodians of their digital assets. Non-custodial wallets offer several benefits, including enhanced security and privacy, as users don't have to rely on a third party to secure their funds. They also enable users to transact directly on the blockchain without intermediaries. However, non-custodial wallets have some drawbacks, such as the sole responsibility of users to secure their private keys and the risk of losing access to funds if the keys are lost. These wallets are ideal for users who prioritize security and control over their digital assets and are willing to take on the responsibility of managing and securing their private keys. (Antonopoulos, 2014).

Table 3.1 provides a concise summary of the advantages, disadvantages, and uses of each type of blockchain wallet:

Table 3.1: advantages, disadvantages, and uses of blockchain wallets.

#	Blockchain Wallet Type	Advantages	Disadvantages	Uses
1.	Non-deterministic wallets	Simple to use	Prone to key loss, low security	Small transactions, quick access to funds
2.	Deterministic wallets	Easy to backup, secure	May have long backup seed phrases	Long-term storage, high-value transactions
3.	Hierarchical deterministic wallets	Same as deterministic wallets, plus additional address generation	May have long backup seed phrases	Long-term storage, high-value transactions
4.	Brain wallets	No need for external storage, can be memorized	Prone to hacking attempts	Small transactions, experimental use
5.	Paper wallets	Highly secure, no need for internet connection	Prone to physical damage, loss or theft	Long-term storage, high-value transactions
6.	Hardware wallets	Highly secure, easy to use, offline storage	Can be expensive, may require software updates	Long-term storage, high-value transactions

#	Blockchain Wallet Type	Advantages	Disadvantages	Uses
7.	Online wallets	Convenient, easy to use, accessible from anywhere	Prone to hacking attempts, third-party control over funds	Small transactions, frequent use
8.	Mobile wallets	Convenient, accessible from anywhere	Prone to hacking attempts, loss or theft of device	Small transactions, frequent use
9.	Multi-signature wallets	High security, requires multiple approvals for transactions	Can be complicated to use, may require additional security measures	Long-term storage, high-value transactions
10.	Full node wallets	Full control over blockchain data, highly secure	Requires significant storage and computing resources	Advanced users, developers, and node operators
11.	Light node wallets	Easy to use, less storage and computing resources required	Less secure, relies on third-party nodes	Novice users, simple transactions
12.	Web-based wallets	Easy to use, accessible from anywhere	Prone to hacking attempts, third-party control over funds	Small transactions, frequent use
13.	Desktop wallets	Highly secure, accessible offline, full control over funds	Requires installation, potential for malware attacks	Long-term storage, high-value transactions
14.	Cold storage wallets	Highly secure, offline storage	Not easily accessible, may require more time and effort for transactions	Long-term storage, high-value transactions
15.	Hot storage wallets	Convenient, easily accessible	Less secure, prone to hacking attempts	Small transactions, frequent use
16.	Custom wallets	Tailored to specific needs	May require technical expertise to develop and use	Advanced users, developers, and businesses
17.	Non-custodial wallets	Full control over funds, no third-party control	User responsible for security, potential for key loss	Long-term storage, high-value transactions

3.6 Peer-to-peer Network (P2P):

The Peer-to-peer Network (P2P) was addressed because Blockchain technology is built on this type of network, and according to (Asghari & Navimipour, 2018) a P2P network is considered as a group of computing nodes that share information and data within the

group consisting of a large group of peers instead of the presence of a central server where the nodes store data and answer queries from other nodes. P2P is composed of dynamic variables G = (P, E), where P represents a non-empty peer set in the network and E indicates the edge set, such as e = {pi, pj} ∈ E represents a peer advantage between pi and pj. See figure 4 as sample of P2P networks with all possible connections.

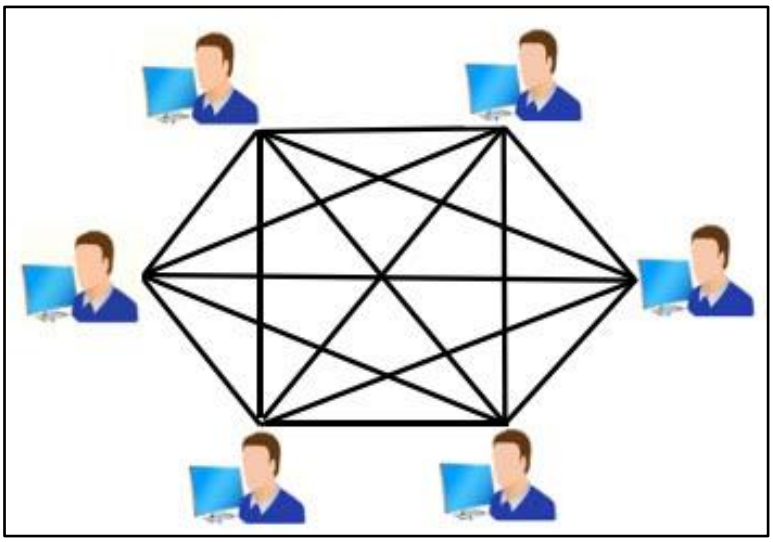

Figure 4: Sample of P2P networks with all possible connections (Asghari & Navimipour, 2018).

3.7 Consensus algorithm

Concern for the security and development of any technology is the main focus of the work sought by researchers and developers in order to gain the trust of users and provide them with a secure digital environment capable of achieving integrity, confidentiality and availability (CIA triangle). This gives them quick access to their data and information and protects it from attackers. This is the focus of consensus mechanisms in Blockchain technology, in this section we will discuss common consensus algorithms (Proof of Work (PoW), Proof of Stake (PoS), Proof of Importance (PoI), Delegated PoS (DPoS), Tangle, Proof of Elapsed Time (PoET), Byzantine Fault Tolerance (BFT) and Practical Byzantine

Fault Tolerance (PBFT)), how they work, and their role in building trust and security in Blockchain.

3.7.1 Proof of Work (PoW):

Proof of Work (PoW) is a widely used consensus mechanism in Blockchain, notably for cryptocurrencies like bitcoin and Ethereum. This mechanism safeguards against malicious activities and potential attacks by requiring network nodes to demonstrate their computational work to validate and add new transactions to the Blockchain. Where the nodes that will add the next block in the Blockchain are set in proportion to the computing power they own, and this would create competition between the nodes in the use of their computing power, as the miners in the Blockchain network solve a complex mathematical problem in order to create the blocks and this is known as the challenge Proof of work. In order to decentralize the verification process across the entire network, the difficulty of the challenge is adjusted for each block by maintaining a 10-minute interval between mining two blocks by the same miner, knowing that miners can enter and exit the network freely, as the proof-of-work mechanism requires Miners have to consume a lot of energy and bear a large amount of cost in electrical devices in order to perform complex calculations, as through the protocol, automatic adjustment is made to increase or decrease the target relocation according to the number of miners. A time delay in accepting a block may cause a problem known as a short-term fork where a miner finds another miner who has made the same block in the Blockchain. The two blocks are valid because they contain a larger share of the proof of work and therefore the other block is disposed of, which is what is called the orphan block. Another problem may arise when a hacker who has enough computational power to control the network reverses some transactions or tries to double the spending of a certain currency. They are performed at

the same time in order to spend a certain currency and both processes enter into an uncertain set of procedures. Once one of the transactions is entered and verified by the other miners, the second transaction will not be entered and it is considered as an invalid transaction and then withdrawn from the network. If the two transactions are taken in at the same time by miners, blocks containing both transactions are added to the Blockchain and a fork is created. As Blockchain technology is decentralized, this fraudulent split becomes ineffective over time because the miner has a low probability of winning consistently by mining the next block. Because PoW makes it difficult to monopolize computing power by a user or group of users, because retail production requires expensive electrical resources and devices and consumes a large amount of electricity (Kaur et al., 2021). (See Figure 5).

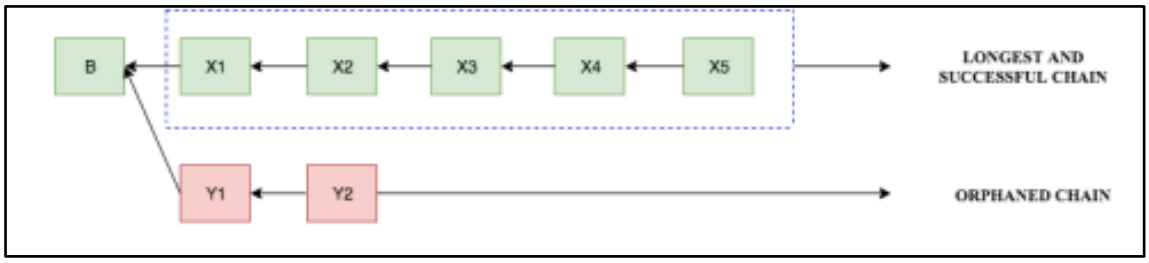

Figure 5: Blockchain Forking (Esposito et al., 2021).

3.7.2 Proof of Stake (PoS):

Proof of stake is a consensus mechanism for processing transactions and creating new blocks on the blockchain. Proof-of-Stake keeps the blockchain secure by reducing the computational effort required to validate blocks and transactions, thereby keeping cryptocurrencies safe. Proof-of-stake is changing the way blocks are verified using coin-holder machines. Owners provide their coins as collateral for the ability to validate blocks. Token holders who hold tokens become "validators". POS aims to reduce energy

consumption by considering that each party has a certain interest in the blockchain. Each block has a process of choosing a random leader; the party elected may enact the following block. The more participation a party has, the more likely it is to be elected leader. Similar to POW, the block version is a reward (Siem, 2017).

3.7.3 Proof of Importance (PoI):

Proof of Importance (POI) is a mechanism used to determine the eligibility of users to add new blocks to a blockchain and receive rewards. It assigns priority to miners based on the number of transactions they perform using the corresponding cryptocurrency. The more transactions a user conducts with their cryptocurrency wallet, the higher their chances of being selected for mining tasks. Proof of Importance systems aim to incentivize active cryptocurrency transactors by giving priority to miners based on the volume and frequency of transactions from their wallets. These systems may also consider other factors, such as the wallets involved in the transactions. It is also possible to combine Proof of Importance with Proof of Stake and Proof of Work algorithms, where additional factors like the amount of cryptocurrency held may be taken into account when prioritizing mining. (Sharma & Jain, 2019).

3.7.4 Delegated PoS (DPoS):

Similar to proof of stake (PoS), delegated proof of stake uses a voting and delegation mechanism to encourage users to protect the network using their staked collateral. In order to take part in the PoS and DPoS consensus mechanisms, users must stake their coins. However, in order to produce a successful block, network users must pick witnesses, also known as delegates, because only voters and elected delegates may approve transactions. The chosen delegates are frequently referred to as witnesses or

block producers. By combining all of your coins into one central staking pool and then linking those coins to a particular delegate, it is feasible to vote on delegates when delegated proof of stake is employed. It's crucial to realize that when we link to a delegate, your funds don't actually move from one wallet to another. After being chosen, delegates must be able to agree on which transactions should be accepted and which should be denied. (Wagner, Keller, & Seiler, 2019) The node operator must persuade a sufficient number of users to vote, which is typically based on how much cryptocurrency they own as each cryptocurrency unit typically counts as one vote. Where nodes split the remaining rewards among their "components" and retain a portion of the block reward as payment for their services. Due to this motivation, a number of potential validators are standing by to take any open positions should an existing node lose trust and subsequently its delegate votes. The remaining nodes examine the validity of both the validation procedure and the inline transactions while choosing one node to validate each block. The remaining nodes may flag suspicious activity and work together to divide the chain and/or notify users of such events if any discrepancies are found or if the delegate continually fails to validate the blocks, allowing for a re-vote. However, supporters insist that adequate decentralization is provided by the two-tiered approach, in which all shareholders can vote for delegates, and in the nature of delegates being publicly known individuals or entities that have a symbiotic relationship with the network and can be voted out of office at any time. Critics of the DPoS consensus algorithm argue that the delegate concept results in a less decentralized network. The interests of stakeholders are thus taken into consideration thanks to this direct democratic method. Another issue brought up is the lack of an immediate monetary fine for suspicious behavior on the part of the verification node. In some ways, this is comparable to the "nothing at stake" introduced by traditional

PoS, but in this instance, the social aspect of requiring user votes to remain an active node incentivizes proper behavior, especially given that the remaining nodes have the option to fork the blockchain and thereby rollback any malicious transactions if necessary.

3.7.5 Tangle:

By burning the cryptocurrency coins, the miners in this process come to an agreement. It's a system where cryptocurrency is entirely cut off from normal circulation. In these circumstances, the process for burning currency is employed to confirm transactions. Due to this, a miner's chances of adding a block to the network are increased by burning more cryptocurrency. PoB lowers power usage when evaluating the (PoW). Additionally, unlike (PoS), PoB does not require miners to stake coins in order to add a new block to the network. Blockchain uses several different Proof of Burn iterations, with Iain Stewart's method receiving the most attention. The concept of "burning the coins" by using local funds to purchase virtual mining equipment (Aggarwal & Kumar, 2021).

Proof of Elapsed Time (PoET):

Proof of Elapsed Time (PoET) is a consensus mechanism used in blockchain networks to achieve resource and energy efficiency while maintaining process effectiveness. It employs a fair lottery system where participants are randomly selected based on a generated amount of time. PoET ensures transparency by allowing verification of lottery results through a trusted code executed in a secure environment. The consensus process of the PoET algorithm guarantees two important aspects. Firstly, it ensures that participants select a time interval randomly rather than choosing a shorter time to increase their chances of winning. Secondly, it verifies that the winner has completed the required waiting period. The PoET mechanism aims to distribute the probability of winning across

a larger number of network participants, resembling a fair lottery system where each node has an equal opportunity of being chosen. In the PoET network, each participating node waits for a specified duration, and the node that successfully completes the waiting period first is declared the winner of the new block. The winning node then broadcasts the necessary information to the peer network and adds the new block to the blockchain. Subsequent block discoveries follow the same process (Chen et al., 2017).

3.7.6 Byzantine Fault Tolerance (BFT):

A consensus technique called Byzantine Fault Tolerance (BFT) attempts to solve the Byzantine Generals' dilemma in a decentralized network. The Byzantine Generals' dilemma is a logic conundrum. Its foundation is the possibility that communication issues could arise between generals of the same side commanding various armies when deciding on the next course of action. A consensus technique called Byzantine Fault Tolerance (BFT) opposes a system that tries to solve the dilemma of the Byzantine Generals. The system should continue to function even if one of the nodes (or the entire system) fails. BFT also tries to lessen the impact on the network of malicious byzantine nodes (or general). According to (Malkhi, Nayak, & Ren, 2019). In BFT, a protocol designer or service administrator first selects a set of assumptions (such as the percentage of Byzantine faults and specific timing assumptions) and then creates (or selects) a protocol that is appropriate for that specific environment. Every replica maintaining the service and every client using the service (also known as the "learner" role) are subject to the assumptions made by the protocol designer. A protocol of this nature breaks down when used in conditions other than those for which it was intended. In particular, if the percentage of Byzantine faults surpasses 1/3, optimal-resilience partially synchronous solutions. Similar to this, synchronous solutions with optimal resilience fail to provide

safety or liveness when the percentage of Byzantine faults is greater than half or when the synchrony bound is broken.

3.7.7 Practical Byzantine Fault Tolerance (PBFT):

Practical Byzantine Fault Tolerance (PBFT) is a consensus algorithm specifically designed to operate efficiently in asynchronous systems where there is no fixed upper bound on the time it takes to receive a response. It aims to minimize overhead time and address various challenges associated with existing Byzantine Fault Tolerance solutions. PBFT finds applications in distributed computing and blockchain technology. According to Xu et al. (2021), PBFT is considered one of the most effective approaches to achieving consensus in distributed systems. It tackles the challenge of reaching an agreement among multiple nodes in a distributed system. However, as the number of peers in the supply chain increases, the consensus efficiency of PBFT may become uncertain. To overcome this limitation, concurrent PBFT has been employed to achieve high consensus efficiency, meeting the requirements of low transaction latency and high throughput introduced by the Transactions on Internet Technology (Xu et al., 2021).

3.8 Comparison between Blockchain consensus algorithms

Blockchain consensus algorithms play a crucial role in the security and efficiency of the blockchain network. There are several consensus algorithms in the blockchain, including Proof of Work (PoW), Proof of Stake (PoS), Proof of Importance (PoI), Delegated PoS (DPoS), Tangle, Proof of Elapsed Time (PoET), Byzantine Fault Tolerance (BFT), and Practical Byzantine Fault Tolerance (PBFT) (Zohar, 2015). Each consensus algorithm possesses unique strengths and weaknesses, rendering them suitable for specific use cases. PoW is the most commonly used algorithm in blockchain networks, but it has the

drawback of high energy consumption and slow transaction speeds (Nakamoto, 2008). On the other hand, PoS is energy-efficient and faster than PoW, but it is susceptible to the "nothing-at-stake" problem (King & Nadal, 2012). PoI aims to solve the problems of PoW and PoS by incorporating the importance of nodes in the network, but it is still in the experimental phase (Chen, Li & Yang, 2017). DPoS is a variation of PoS that introduces a delegate system to achieve faster transaction processing (Larimer, 2014). Tangle is a DAG-based algorithm that claims to offer scalability and zero transaction fees, but it is still relatively new and untested (Popov, 2017). PoET is a consensus algorithm that uses a random wait time to minimize energy consumption and improve network scalability (Eyal & Sirer, 2013). BFT and PBFT are fault-tolerant algorithms that aim to ensure the consistency of the blockchain network in the presence of malicious nodes (Castro & Liskov, 1999). Therefore, understanding the strengths and weaknesses of each consensus algorithm is crucial for choosing the most appropriate one for a particular use case. see table 3.2:

Table 3.2: Comparison between Blockchain consensus algorithms

#	Consensus Algorithm	Key Features	Advantages	Disadvantages	Use Cases
1.	Proof of Work (PoW)	Nodes compete to solve a cryptographic puzzle to add blocks to the chain.	Proven to be secure, widely adopted, incentivizes miners to participate.	High energy consumption, slow transaction speeds, centralization risk due to mining pool concentration.	Bitcoin, Ethereum (for now).
2.	Proof of Stake (PoS)	Nodes are chosen to add blocks to the chain based on the amount of cryptocurrency they hold and "stake" as collateral.	Energy-efficient, faster than PoW, less centralization risk, discourages concentration of mining power.	Susceptible to "nothing-at-stake" problem, initial stake required to participate, may create oligarchy of wealthy validators.	Cardano, Cosmos, Ethereum 2.0.

#	Consensus Algorithm	Key Features	Advantages	Disadvantages	Use Cases
3.	Proof of Importance (PoI)	Incorporates node importance based on transaction history, balance, and other factors.	Tries to address the problems of PoW and PoS, encourages participation and activity.	Experimental, complex to implement, may lead to centralization.	NEM
4.	Delegated PoS (DPoS)	Similar to PoS, but uses a delegate system where nodes are elected to validate transactions and create blocks.	Fast transaction processing, less energy consumption than PoW, less centralization risk.	Delegates can become corrupt or collude, may lead to centralization.	BitShares, EOS, Lisk.
5.	Tangle	Uses a directed acyclic graph (DAG) instead of a traditional blockchain, with each transaction confirming two previous transactions.	Claims to offer scalability, zero transaction fees, and fast processing.	Relatively new and untested, may have security vulnerabilities.	IOTA
6.	Proof of Elapsed Time (PoET)	Nodes wait a random amount of time before adding a block to the chain, with the shortest wait time winning.	Energy-efficient, promotes fairness and participation.	Limited adoption, requires hardware support for randomness generation.	Hyperledger Sawtooth.
7.	Byzantine Fault Tolerance (BFT)	Nodes agree on the state of the network through multiple rounds of voting.	Fast processing, fault-tolerant in the presence of malicious nodes.	Requires a predetermined number of nodes, not suitable for large networks, vulnerable to Sybil attacks.	Hyperledger Fabric, Ripple.
8.	Practical Byzantine Fault	Similar to BFT, but more efficient in larger networks.	Fault-tolerant, fast processing, works well in larger networks.	Requires a predetermined number of nodes, vulnerable to Sybil attacks.	Stellar

#	Consensus Algorithm	Key Features	Advantages	Disadvantages	Use Cases
	Tolerance (PBFT)				

3.9 Blockchain transactions

Blockchain transactions are the core building blocks of Blockchain technology, where the information is recorded in a decentralized, immutable, and transparent manner through a network of nodes. Transactions in a Blockchain network are initiated by users and validated by nodes using complex algorithms and consensus mechanisms (Antonopoulos, 2014). Each transaction contains a unique digital signature and cryptographic hash that ensures its authenticity and security (Nakamoto, 2008).

In a typical Blockchain transaction, a user creates a transaction by entering the recipient's address and the amount to be transferred. The transaction is then broadcasted to the network, where it is verified and validated by nodes using a consensus mechanism (Tapscott & Tapscott, 2016). Once the transaction is confirmed by the nodes, it is added to a block and added to the Blockchain through a process called mining (Swan, 2015).

The process of mining involves the use of powerful computers that solve complex mathematical problems to validate and add new blocks to the Blockchain. Miners are incentivized through the issuance of new cryptocurrencies as a reward for their efforts in maintaining the network (Zheng et al., 2018). This process ensures the security and integrity of the Blockchain by preventing malicious actors from altering the records.

Blockchain transactions are immutable and irreversible, which means that once a transaction is added to the Blockchain, it cannot be altered or deleted. This feature ensures the transparency and accountability of transactions in the network (Werbach, 2018).

Furthermore, the use of smart contracts allows for the automation and execution of predefined conditions, making transactions faster, cheaper, and more efficient (Buterin, 2014).

Blockchain transactions are the fundamental components of Blockchain technology, which enables secure and transparent record-keeping without the need for intermediaries. Transactions are initiated and validated by nodes using complex algorithms and consensus mechanisms. The use of cryptography, mining, and smart contracts ensures the integrity, security, and efficiency of Blockchain transactions (Crosby et al., 2016 & Li et al., 2018 & Swan, 2017 & Mougayar, 2016).

3.9.1 Transaction pools:

In the context of Blockchain technology, a transaction pool is a collection of unconfirmed transactions that have been broadcasted to the network and are awaiting validation by a miner or a validator node (Bitcoin Wiki, 2021). These transactions are temporarily stored in the memory of participating nodes until they are added to the next block of the Blockchain. As the number of unconfirmed transactions grows, the size of the transaction pool increases, which may cause longer transaction processing times and higher transaction fees (Antonopoulos, 2014).

Transaction pools are an essential component of Blockchain networks, as they enable the efficient processing and validation of transactions without the need for centralized intermediaries (Crosby, Pattanayak, Verma, & Kalyanaraman, 2016). In contrast to traditional payment systems, where a centralized authority processes and verifies transactions, Blockchain transactions are validated by a decentralized network of nodes through a consensus mechanism, such as proof-of-work (PoW) or proof-of-stake (PoS)

(Nakamoto, 2008). This distributed validation process allows for greater transparency, security, and immutability of transactions (Swan, 2015).

To ensure that transactions in the pool are valid and comply with the network's rules, participating nodes may perform some preliminary checks before accepting a transaction (Buterin, 2014). These checks may include verifying the transaction's digital signature, checking that the transaction inputs have not been spent before, and verifying that the transaction meets the network's minimum transaction fee requirements. Once a transaction is accepted by a node, it is added to its local transaction pool, and it is propagated to other nodes in the network.

Transaction pools play a crucial role in the efficient and decentralized processing of transactions in Blockchain networks. The size of the transaction pool affects the time and cost required for transaction processing, making it a critical factor in the performance of a Blockchain network. To ensure the validity and security of transactions, participating nodes perform preliminary checks before accepting transactions into their local transaction pools (Zohar, 2015).

3.9.2 Transaction verification:

Blockchain transactions verification is an essential process in ensuring the security and integrity of the blockchain network. Transactions are validated through a consensus mechanism to prevent double-spending and other malicious activities (Nakamoto, 2008). When a transaction is broadcasted to the network, it is added to the transaction pool where it waits to be verified by the nodes in the network. The process of verification involves validating the transaction against predefined rules to ensure that it meets the required conditions for execution (Antonopoulos, 2014).

Blockchain networks employ various verification methods, including Proof of Work (PoW) and Proof of Stake (PoS) (Buterin, 2014). In the PoW consensus mechanism, nodes compete to solve complex mathematical equations to validate transactions and add them to the blockchain network. The first node to solve the equation is rewarded with newly minted cryptocurrency (Popov, 2016). In contrast, PoS uses a different approach where nodes are selected to verify transactions based on the amount of cryptocurrency they hold (Kiayias, Russell, David, & Oliynykov, 2018).

To validate a transaction, the node must ensure that it has a valid digital signature, confirming that the transaction was initiated by the owner of the cryptocurrency (Tapscott & Tapscott, 2016). The node then verifies that the cryptocurrency used in the transaction is available and has not been previously spent. The node also confirms that the transaction meets the predefined criteria for execution (Zohar, 2015).

Once the transaction is verified, it is added to the blockchain network as a new block. The newly created block is then broadcasted to all the nodes in the network for verification and approval. If the majority of the nodes in the network approve the block, it is added to the blockchain, and the transaction is considered complete (Narayanan et al., 2016).

transaction verification is a crucial process in maintaining the security and integrity of the blockchain network. Various consensus mechanisms such as PoW and PoS are used to validate transactions and add them to the blockchain network. The verification process involves validating the digital signature, confirming the availability of cryptocurrency, and ensuring that the transaction meets the predefined criteria for execution. Once the transaction is verified, it is added to the blockchain network as a new block and broadcasted to the nodes in the network for verification and approval.

3.10 Blockchain Challenge's

Blockchain technology faces, like any technology, needs and challenges that evolve with the development of the concept of its use, and some research has focused on some challenges such as security, which was addressed in the mechanisms of consensus and addressing response time, and that increased productivity with reduced response time causes us a problem called Bottleneck and Scalability problem for Blockchain technology. Some suggested solutions to the mentioned problems, which are as follows:

- (Zamani, Movahedi, & Raykova, 2018) suggested to use Rapid Chain protocol and they defined it as the first public protocol in the blockchain and its working principle is based on sharing as well as providing flexibility for Byzantine errors to up to 1/3 part of the participants, working on the complete anatomy of computation, storage and communication on top of the processing processes without assuming any reliable setup. Rapid Chain relies on the use of a perfect consensus algorithm that achieves high productivity, as well as the use of a novel gossiping protocol for large blocks in order to ensure durability. The Rapid chain protocol avoids gossiping transactions to the entire network. Knowing that the evaluations made by researchers for this protocol that it is capable of processing and confirming more than 7300 tx/sec and that the delay is approximately 8.7 seconds in a network consisting of 4000 nodes. With a remarkable time-to-failure exceeding 4,500 years.
- Regarding the scalability has been suggested by (Allen et al., 2020) To become a node consisting of more than one machine and not just from one machine so that one machine is replaced by many linked servers that act as a single node and thus become a high node performance as well as they can maintain the security

characteristics of the original protocol and allow expansion in proportion to the available resources.

- (Dang et al., 2019) turned to blockchain scaling by working on the application of hashing to Blockchain systems. With the aim of broadly improving transaction throughput, it challenges the fundamental difference in failure models between Blockchain and databases. By working to improve Byzantine consensus protocols, work on improving individual shards' throughput and then work on designing an effective protocol for forming shards and assigning nodes securely. In which. They have relied on reliable hardware, Intel SGX, in order to achieve high performance of consensus protocols and hard formation protocol. Then they worked on the design of a globally distributed transaction protocol in order to ensure the safety of vitality even if users were malicious. After conducting a comprehensive assessment on Google Cloud Platform and on a local cluster, the results were according to the research that the consensus and shard formation protocols out per form state-of-the-art solutions at scale that they reached high productivity capable of handling workloads at the Visa level.

3.11 Smart Contract

Simply, the smart contracts are blockchain-based algorithms that execute when certain criteria are met. They are often used to automate the implementation of an agreement so that all parties can be certain of the conclusion right away, without the need for an intermediary or additional delay. They can also automate a workflow such that when circumstances are met, the following action is executed. Smart contracts operate by implementing simple "if/when...then" phrases in code, which are then deployed and stored on a blockchain. A network of computers will perform the activities if certain

conditions have been verified to have been met. These can entail paying out money to the right people, registering a car, sending out notices, or writing a ticket. Once a transaction is completed, the blockchain is updated, ensuring that the transaction becomes immutable and cannot be modified. Furthermore, the outcome of the transaction is only visible to authorized parties who have been granted permission. Smart contracts can include an extensive range of conditions to provide reassurance to participants regarding the successful execution of an activity. To establish the terms for transactions governed by smart contracts, participants must collectively agree on the "if/when...then" rules and consider any possible exceptions. They also need to design a framework for resolving disputes that may arise. Participants must also choose how transactions and the data they are associated with will be displayed on the blockchain. While developers can construct smart contracts from scratch, an increasing number of businesses are opting for pre-designed templates, web interfaces, and online tools to simplify the process of creating smart contracts.

Given the security concerns of smart contracts, which could undermine users' confidence in the event of possible errors and security failures, researchers (Tsankov et al., 2018) has proposed to the use of a secure security tool for Ethereum contracts called Securify tool, it is a fully automated tool that verifies the security of contracts by analyzing their behavior and checking for specific properties. It uses a contract dependency graph to extract semantic information from the code. Additionally, it employs a pattern-based approach to identify conditions that prove ownership. The effectiveness of Securify has been demonstrated through its successful application to real-world Ethereum contracts. (See Figure 6):

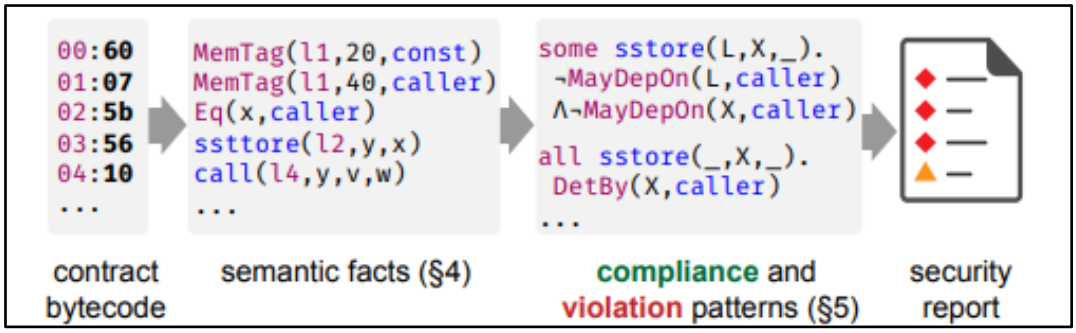

Figure 6: Securify is based on the automatic inference of semantic program facts, which is then checked for compliance and security violations over these facts (Tsankov et al., 2018).

3.12 Taxonomy Blockchain applications

Many researchers classified Blockchain applications into financial applications and non-financial applications, due to the connection of Blockchain technology in cryptocurrencies. For example, (Casino, Dasaklis, & Patsakis, 2019) proposed multiple classifications based on the use of strict statistical methodologies so these ratings are proportional to the evolution of the Blockchain. The researchers suggested the following categories of Blockchain applications, including: Financial applications, Integrity Verification, Governance (Citizenship and User Services, Public sector, Voting), Internet of Things, Healthcare management, Privacy and Security, Business and industrial applications (Supply chain management, Energy sector). Education, Data Management, and Miscellaneous applications. (See Figure 7):

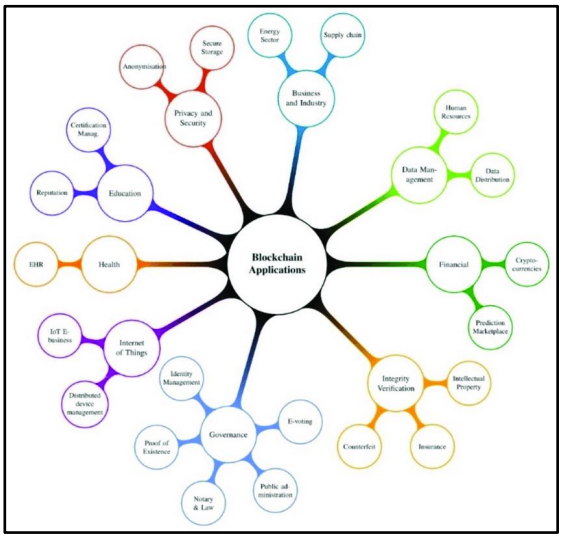

Figure 7: Classification Blockchain applications (Casino, Dasaklis, & Patsakis, 2019).

3.13 Blockchain in Palestine

Up to my best knowledge, the use of Blockchain technology in Palestine has rare publications as it is a technology that is still new to our Palestinian society. The various articles that address Blockchain in Palestine include:

3.13.1 Gaza Wallet:

(AbuSamra, Elbatsh, & Hassan, 2020) establishment of a financial system to be applied in the Gaza Strip, which is a digital wallet that allows users to store their encrypted currencies and manage their balances through a digital wallet programmed in the Python language based on Blockchain technology, where users are provided with wallet keys and are unique numbers, where access to the wallet is through the authorization To the Blockchain website or through a mobile application, where you will show them their balance of the currency that they created and called the Gaza coin, which is expressed with the symbol CG. The user can also send a request to another user to perform the conversion process, and accordingly the system creates a unique address that can be converted into a QR code. See figure 8 it explains the process of Gaza Wallet Application in Android.

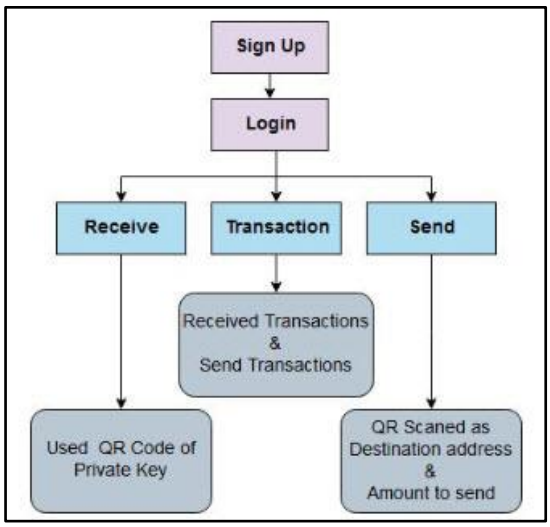

Figure 8: the process of Gaza Wallet Android Application (AbuSamra, Elbatsh, & Hassan, 2020)

3.13.2 Blockchain application in the Palestine Exchange:

The researchers reviewed the results of the research that they prepared on the use of Blockchain technology in the stock market for third world countries, with a focus on the case of the stock exchange in Palestine (Aburidi, 2022), where it was summarized that the application of the Blockchain is suitable for third world countries as it does not require high costs such as constructing buildings. In addition, the study concluded that it will be The Palestine Exchange can accelerate its liquidity cycle at the lowest costs while ensuring transparency and expanding its activity by absorbing new products and attracting new investors. As the researchers considered that the application of Blockchain in the Palestine Exchange works to bridge the gap and contribute to reshaping the Palestine Exchange.

3.14 Blockchain Security

Consensus algorithms are a core component of Blockchain technology that enables participants to agree on the validity and order of transactions. Because the proposed Ramallah Smart Parking System (RSP) is based on the use of three types of Blockchain, which are public blockchains, private blockchains and Consortium blockchains An in-depth research will be done on the most prominent consensus algorithms used in these types of Blockchain to verify that they achieve effective results in forging a secure Blockchain environment. Since there is no global agreement on a consensus algorithm that is the best for all types of blockchain, so many researchers have made comparisons between these algorithms and evaluated them based on many factors, including decentralization, security, efficiency, and scalability.

(Yadav and Singh, 2020) presented a comparative study between consensus algorithms (Proof-of-Work (PoW), Proof-of-Stake (PoS), Proof-of-Activity (PoA), Proof-of-Elapsed-Time (PoET), Practical Byzantine Fault Tolerance (PBFT) and Delegated Proof-of-Stake (DPoS)). The result was summarized as following Table 3.3:

Table 3.3: Comparison between Blockchain consensus algorithms (Yadav and Singh, 2020).

Consensus Algorithm	Decentralization	Security	Efficiency	Scalability	Power Usage
Proof-of-Work (PoW)	High	High	Low	Low	High
Proof-of-Stake (PoS)	High	High	High	High	Low
Proof-of-Activity (PoA)	Moderate to High	High	High	High	Variable
Proof-of-Elapsed-Time (PoET)	Moderate to High	High	High	High	Variable
Practical Byzantine Fault Tolerance (PBFT)	Moderate to High	High	Medium	Medium to High	Variable
Delegated Proof-of-Stake (DPoS)	Moderate to High	High	High	High	Variable

Also, Qianwen Wang et al. (2020) they worked on the study of consensus algorithms (PoW, PoS, DPoS and PBFT), and the results of the study are summarized in the following table 3.4:

Table 3.4: Comparison between Blockchain consensus algorithms (Qianwen Wang et al. 2020).

Consensus Algorithm	Decentralization	Security	Efficiency	Scalability	Power Usage
Proof of Work (PoW)	High	High	Low	Low	High
Proof of Stake (PoS)	Low	Medium	High	Medium	Low
Delegated PoS (DPoS)	Medium	Medium	High	High	Low
Practical BFT (PBFT)	Low	High	Medium	Low	Low

In addition to the above, (Bamakan et al. 2020) conducted a survey of consensus algorithms, as the result of the study is presented in the following table 3.5:

Table 3.5: Comparison between Blockchain consensus algorithms (Bamakan et al. 2020).

Consensus Algorithm	Decentralization	Security	Efficiency	Scalability	Power Usage
Proof of Work (PoW)	High	High	Low	Medium	High
Proof of Stake (PoS)	Medium	Medium	High	High	Low
Delegated Proof of Stake	Low	High	High	High	Low
Proof of Elapsed Time	Low	High	Medium	High	Medium
Practical Byzantine Fault Tolerance	Medium	High	High	Medium	Low
Delegated Byzantine Fault Tolerance	Low	High	High	Medium	Low
Proof of Weight (PoWeight)	Medium	High	High	Medium	Medium
Proof of Burn (PoB)	High	Medium	High	Medium	Medium
Proof of Capacity (PoC)	Medium	Medium	Medium	Medium	Low

3.14.1 Security Concerns Impacting Blockchain:

There are many ways and methods that attackers use in the blockchain, and we summarize the most prominent of them as follows:

1. Denial of Service (DoS) attacks: These attacks aim to overwhelm the network's resources, through flood the nodes by attackers causing congestion and degradation of performance, making it difficult or impossible for legitimate users to access or use the blockchain. (Hasanova et al. 2019).
2. Sybil Attacks: the attackers create a rogue node that may continue fraudulent transactions, and hence disrupt the blockchain. (Nair and Dorai, 2021).

3. SelfishMining Attacks: When mining, the attacker only discloses the blocks that they have already extracted, wasting the time of other miners of equal skill who must still mine the more blocks. This uses up the computing power of the miners. (Nair and Dorai, 2021).
4. Short range Attacks: Short-range attacks in blockchain, such as stakeholder bribing, refer to attacks that exploit the trust or influence of specific stakeholders within the network. Stakeholder bribing involves attempting to manipulate the consensus process or gain control over the blockchain by offering incentives or rewards to influential stakeholders in exchange for their cooperation in carrying out malicious activities. In stakeholder bribing attacks, the attacker aims to convince key stakeholders, such as validators or block producers, to act in their favor by offering financial or other benefits. This can include bribing stakeholders to approve fraudulent transactions, manipulate the consensus algorithm, or withhold/block legitimate transactions. (Hasanova et al. 2019).
5. Long range attacks: also known as history revision attacks, involve the attacker starting from the genesis block or some of the earliest blocks and creating new blocks to form a longer blockchain than the existing legitimate blockchain (Hasanova et al., 2019).
6. Coin age accumulation: attack refers to a scenario where an attacker accumulates a significant number of coins in a blockchain system over a long period of time. By holding these coins, the attacker gains a higher chance of being selected as a validator or for other privileges in the consensus mechanism, such as proof of stake. This allows the attacker to exert greater control over the system and potentially carry out fraudulent activities (Hasanova et al., 2019).

7. A pre-computing attack: also known as a rainbow table attack, involves the attacker having access to a database containing a list of pre-computed password hashes. With this information, the attacker can easily match the password hashes stored in the blockchain's blocks and gain unauthorized access to the corresponding blocks. This type of attack exploits the weakness of weak or poorly protected password storage mechanisms in the blockchain system. It highlights the importance of using strong cryptographic hashing algorithms and secure password storage techniques to mitigate the risk of such attacks (Hasanova et al., 2019).

3.15 Blockchain Consensus Algorithms

Blockchain is a distributed ledger a continuously block each block linked for the previous block each block uses a cryptographic hash, timestamp, and transaction data. Consensus algorithm isa main layer in blockchain architecture. Unti l now, there has not been a consensus on a single consensus algorithm to be used in blockchain purification, but the choice is made based on the nature of use, its specific function, and the desired advantages such as Decentralization, Security, efficiency, scalability, and power usage.

Assuring the integrity and consistency of the shared ledger in a decentralized manner, consensus algorithms in blockchain networks seek to achieve agreement among distributed nodes by utilizing cryptographic techniques and incentive mechanisms to validate and agree on the order and content of transactions. To handle problems like Byzantine faults, reach consensus, and maintain the security and reliability of the blockchain system, these algorithms use a variety of techniques including Proof of Work, Proof of Stake, or other processes.

In this chapter, we seek to shed more light on the most prominent consensus algorithms used, and then choose the consensus algorithm that is ideally suited to the proposed Ramallah Smart Parking - RSP system, and then work on analyzing it, analyzing its operation mechanism, and checking if it is compatible with the RSP system.

3.15.1 Classification of consensus algorithms in blockchain:

Many researchers, such as (Pahlajani, Kshirsagar, and Pachghare.2019), have classified consensus algorithms in Privet blockchain into two main categories. The first category is the voting-based consensus, and this type of consensus algorithm requires that nodes in the network announce their findings from mining the new block or transaction, before adding a new block or transaction to the blockchain. The second class is the proof-based consensus which requires a mathematical puzzle be solved by new nodes joining the blockchain network in order to prove that they are better qualified than the rest to perform appending or mining activity.

Also, (Yao et al. 2021) classified consensus algorithms in two ways, the first method according to the final decision-making approach to reach a consensus, and divided it into two parts, the first is proof-based consensus algorithms (PoW, PoS, PoA, PoET, and PoSpace) and the second section is voting-based (Paxos, Raft, PBFT, RFBT, RPCA, SCP, Tendermint, HotStuff, HoneyBadger, BFT-smart). The second method is to classify consensus algorithms through the design principle of tolerance with the error.

3.16 Classification of consensus algorithms in blockchain as decision-making

3.16.1 Proof-based consensus algorithms:

The Voting-based consensus algorithms needs to solve the encryption problem in order for the block to join the network, the most prominent consensus algorithms that fall under this type of classification are as mentioned, which are summarized according to the following table 3.6:

Table 3.6: Proof-based consensus algorithms) Pahlajani, Kshirsagar, and Pachghare.2019)

No	consensus algorithms	Description
1.	Proof of Work	solving an mathematical puzzle
2.	Proof of Stake	having more stake in blockchain
3.	Proof of Elapsed time	some timeout is set with scheduling.
4.	Proof of Luck	random selection
5.	Proof of Space	bigger size hard-disk is required
6.	Proof of authority	Validators are chosen based on their identity and reputation rather than computational power or stake

3.16.2 Voting consensus algorithms

The Vote-based consensus calls for the results to be exchanged throughout the network prior to adding the block to the blockchain. A check must be done to ensure that at least x (x is the threshold set) peers agree on it before a peer can add a block to its chain. If there are f failed nodes, then f plus 1 should be operative for a decision. Therefore, see table 7 vote consensus is generally categorized as follows as mentioned by (Pahlajani, Kshirsagar, and Pachghare.2019):

Table 3.7: Voting consensus algorithms

No	consensus algorithms	Description
1.	Byzantine (Hyperledger, Corda, Iroha with Sumeragi, Ripple, Stellar)	Nodes are crashed and unsettled
2.	Crash (Raft, Chain with Federated,	Nodes are crashed
3.	Paxos	

No	consensus algorithms	Description
4.	PBFT	
5.	RPCA	
6.	SCP	
7.	Tendermint	
8.	HotStuff	
9.	HoneyBadger	
10.	BFT-smart	

3.17 Classification of consensus algorithms in blockchain as design principle of tolerance

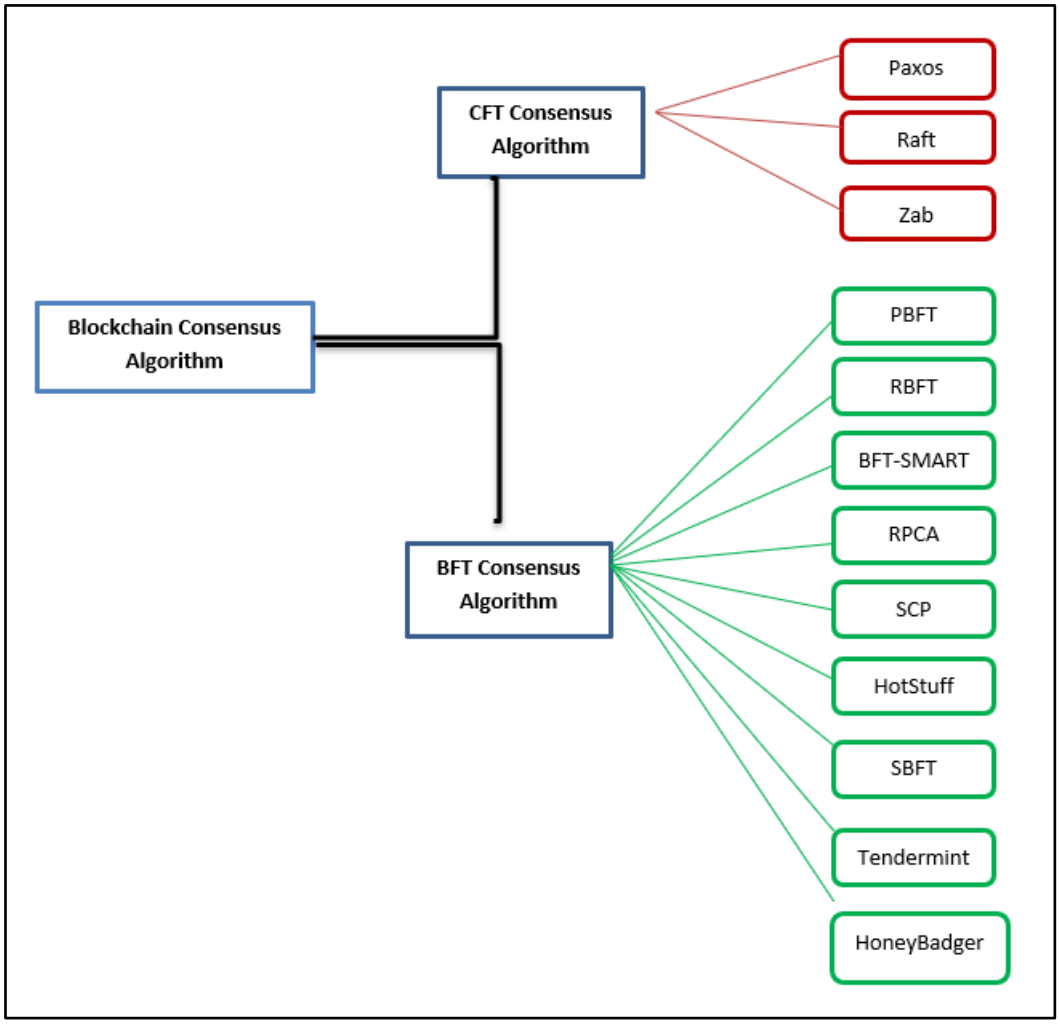

Figure 9: Classification of Blockchain Consensus Algorithm by Fault Tolerance (Yao et al. 2021)

Figure 9 illustrates the categorization of Blockchain Consensus Algorithms based on their Fault Tolerance. Crash Fault Tolerance consensus algorithms (CFT) provide a strong guarantee of reliability and resiliency for blockchain networks, particularly in the face of

node failures. Node failures, also known as non-Byzantine faults, can be brought on by faulty hardware, crashing processes, a downed network, or programming flaws. Byzantine mistakes, or situations involving malicious behavior, cannot be addressed by CFT. A CFT algorithm cannot ensure system dependability when nodes in a blockchain willfully and maliciously break consensus principles, for as by altering with data. CFT consensus algorithms are predominantly employed in closed contexts, such as enterprise blockchains. The Paxos algorithm and Raft are two popular CFT consensus techniques today. Raft is derivative of the former and is a streamlined version of Paxos that is intended to be more practical for industry application.

Byzantine Fault Tolerance (BFT) A consensus technique opposes a system that tries to solve the dilemma of the Byzantine Generals. The system should continue to function even if one of the nodes (or the entire system) fails. BFT also tries to lessen the impact on the network of malicious byzantine nodes (or generally).

3.18 Ramallah Smart City Parking RSP Blockchain consensus algorithms

So far, there is no specific consensus on one of the consensus algorithms to be applied in the different types of Blockchain technology. In this chapter, we will seek to choose one of the algorithms that are suitable for use in the proposed system for the Ramallah smart city situation, so that it achieves maximum benefit in terms of the following factors:

1. Security: The fact that Ramallah Smart City did not use Blockchain technology in the services it provides to the public, therefore, security is very necessary, as it contributes to achieving public satisfaction and gaining its trust.

2. Scalability: because the city of Ramallah seeks to become a smart city, therefore, the expansion feature must be taken into account in order to expand in other sectors.
3. Power: It is necessary that the consensus algorithm be low in energy consumption, because according to the document (Resilience of Ramallah 2050), among the problems that the city suffers from is that it does not produce electric energy, but rather it buys 95% from the Israeli Electricity Company and 5% from Jordan.
4. Efficiency: Effectiveness is achieved in the speed of response and implementation of the required operations in order to achieve high efficiency in performance
5. Decentralization: It requires greater availability in the RSP system in the public blockchain and in the Consortium network.

3.19 Comparisons of Blockchain consensus algorithms

Consensus algorithms are a core component of Blockchain technology that enables participants to agree on the validity and order of transactions. Because the proposed Ramallah Smart Parking System (RSP) is based on the use of three types of Blockchain, which are public blockchains, private blockchains and Consortium blockchains in depth research will be done on the most prominent consensus algorithms used in these types of Blockchain to verify that they achieve effective results in forging a secure Blockchain environment. Since there is no global agreement on a consensus algorithm that is the best for all types of blockchain, so many researchers have made comparisons between these algorithms and evaluated them based on many factors, including decentralization, security, efficiency, and scalability.

(Yadav and Singh, 2020) presented a comparative study between consensus algorithms (Proof-of-Work (PoW), Proof-of-Stake (PoS), Proof-of-Activity (PoA), Proof-of-

Elapsed-Time (PoET), Practical Byzantine Fault Tolerance (PBFT) and Delegated Proof-of-Stake (DPoS)). The result was summarized as following Table 3.8:

Table 3.8: A Comparison between Blockchain consensus algorithms according to (Yadav and Singh, 2020).

Consensus Algorithm	Decentralization	Security	Efficiency	Scalability	Power Usage
Proof-of-Work (PoW)	High	High	Low	Low	High
Proof-of-Stake (PoS)	High	High	High	High	Low
Proof-of-Activity (PoA)	Moderate to High	High	High	High	Variable
Proof-of-Elapsed-Time (PoET)	Moderate to High	High	High	High	Variable
Practical Byzantine Fault Tolerance (PBFT)	Moderate to High	High	Medium	Medium to High	Variable
Delegated Proof-of-Stake (DPoS)	Moderate to High	High	High	High	Variable

Also, Qianwen Wang et al. (2020) they worked on the study of consensus algorithms (PoW, PoS, DPoS and PBFT), and the results of the study are summarized in the following table 3.9:

Table 3.9: A Comparison between Blockchain consensus algorithms according to (Qianwen Wang et al. 2020).

Consensus Algorithm	Decentralization	Security	Efficiency	Scalability	Power Usage
Proof of Work (PoW)	High	High	Low	Low	High
Proof of Stake (PoS)	Low	Medium	High	Medium	Low
Delegated PoS (DPoS)	Medium	Medium	High	High	Low
Practical BFT (PBFT)	Low	High	Medium	Low	Low

In addition to the above, (Bamakan et al. 2020) conducted a survey of consensus algorithms, as the result of the study is presented in the following table 3.10:

Table 3.10: A Comparison between Blockchain consensus algorithms according to (Bamakan et al. 2020).

Consensus Algorithm	Decentralization	Security	Efficiency	Scalability	Power Usage
Proof of Work (PoW)	High	High	Low	Medium	High
Proof of Stake (PoS)	Medium	Medium	High	High	Low
Delegated Proof of Stake	Low	High	High	High	Low
Proof of Elapsed Time	Low	High	Medium	High	Medium
Practical Byzantine Fault Tolerance	Medium	High	High	Medium	Low
Delegated Byzantine Fault Tolerance	Low	High	High	Medium	Low
Proof of Weight (PoW eight)	Medium	High	High	Medium	Medium
Proof of Burn (PoB)	High	Medium	High	Medium	Medium
Proof of Capacity (PoC)	Medium	Medium	Medium	Medium	Low

Based on the previous results of comparisons of consensus algorithms, none of them achieved the ideal for Decentralization, Security, Efficiency, Scalability, and Power Usage at one time, this is because each algorithm strengths and weaknesses, and sometimes the strengths and weaknesses differ according to the nature of the use of the consensus algorithm. In the blockchain research, some researchers have worked on using hybrid consensus algorithms to take advantage of the strengths of more than one algorithm. One of these algorithms is the Proof-of-Activity (PoA) consensus algorithm, this is the result of the combining of the Proof of Work and Proof of Stake algorithms. As they thus bypassed the risks present in the PoW algorithm from the possibility of an attacker taking over the network if he owns at least 51% of the mining computing power of the network, as well as the possibility of the attacker taking over the network in PoS if he owns no less than 51% of the cryptocurrency On the network, and thus the attacker's acquisition of these two characteristics would be very difficult, and thus the success rate

of the attack to acquire the network decreased from 51% to 0%. However, this is accompanied by some weaknesses, such as the relatively high consumption of energy and the need for powerful devices, since PoW uses high computational power, as well as the problem of double signing by auditors. (Crypto Robin, n.d.)

In this section we will propose a new hybrid algorithm similar to the Proof-of-Activity (PoA) algorithm, but we will use Machine Learning in order to perform comparison operations with Malicious Block's discovered on the network earlier in order to obtain a safe algorithm with consumption Less energy and meet the required requirements in the consensus algorithm that will be used in the Ramallah Smart Parking System - RSP so that it achieves Decentralization, Security, Efficiency, Scalability, and low Power Usage together at the same time, and we will call the proposed hybrid algorithm SMO.

In the following sections of this chapter, we will discuss a detailed analysis of the PoW proof-of-work algorithm, the PoS algorithm, and then the Proof of Activity (PoA) algorithm, and then present the proposed SMO algorithm.

3.19.1 Proof-of-Work (PoW) consensus algorithm:

Proof-of-Work (PoW) consensus algorithm is commonly used in blockchain networks to create widespread consensus and protect the blockchain from fraudulent activity. For the PoW process to validate transactions and add new blocks to the blockchain, users, referred to as miners, must solve computationally challenging puzzles. It takes a lot of processing effort and energy to obtain a hash value that satisfies a set of requirements, which is why miners compete to find it. Newly created cryptocurrency tokens or transaction fees are awarded to the first miner to find a valid solution. (Nakamoto, 2008).

3.19.2 Proof-of-Work (PoW) Mechanism:

According to (Nakamoto, 2008), In the PoW system, miners compete to find a nonce value that, when hashed with a specific algorithm (such as SHA-256), produces a hash with a certain number of leading zero bits. The difficulty of finding the nonce is adjusted dynamically to maintain a target average block generation time. By requiring miners to expend computational effort, PoW ensures that adding a new block to the blockchain is resource-intensive and time-consuming. Once a valid solution is found, it is easy for other participants to verify the work by performing a single hash operation. This work represents a "proof" that the miner has invested a significant amount of computational power. The PoW algorithm also addresses the problem of majority decision-making. Instead of relying on a one-IP-address-one-vote system that can be easily manipulated, PoW implements a one-CPU-one-vote approach. The decision on the valid blockchain is based on the longest chain, which represents the greatest cumulative proof-of-work effort. if the majority of CPU power is in the hands of honest nodes, the honest chain will have the fastest growth and become the dominant chain. See figure 10.

The security of PoW lies in the fact that modifying a past block would require redoing the proof-of-work for that block and all subsequent blocks, while also surpassing the cumulative work of the honest nodes. As more blocks are added to the chain, the probability of a slower attacker catching up diminishes exponentially. To adapt to changes in hardware speed and network participation, the difficulty of the PoW puzzle is adjusted over time. A moving average targeting a specific average block generation rate is used to maintain a balance between block production and computational resources.

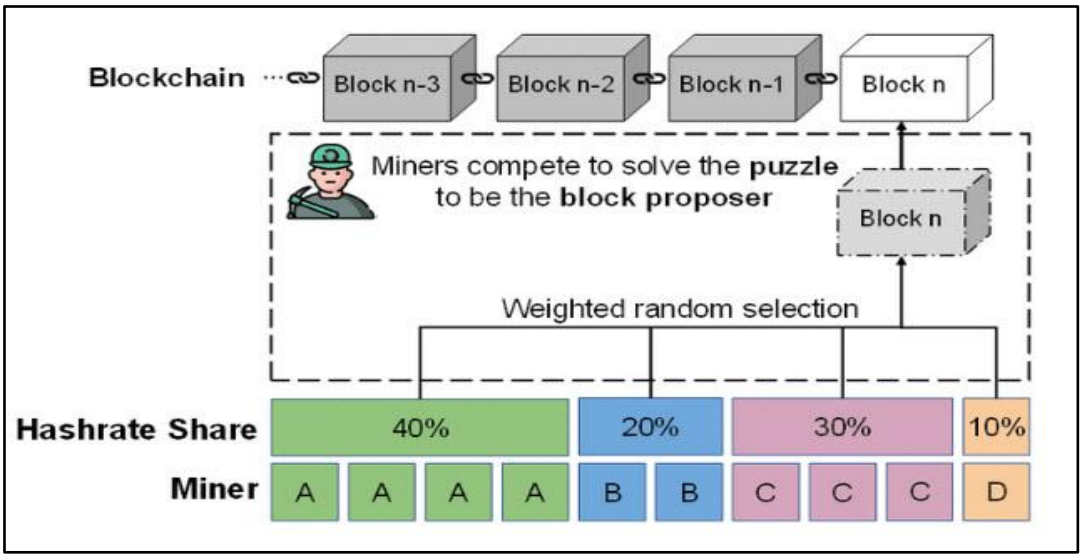

Figure 10: Proof-of-Work Consensus Mechanism (Shi et al., 2023).

- **Hashes:** After closing a block in the blockchain, the hash of the block needs to be verified before proceeding to the next block. This verification process is called as proof of work. The hash is a 64-digit encrypted hexadecimal number that can be generated quickly with modern technology. However, miners intentionally spend a significant amount of time trying to guess the correct hash, which is computationally intensive.
- **Nonce:** The nonce (number used once) is a number used in the process of mining in blockchain. Miners generate hashes using a nonce starting from zero.
- **Solving the Hash:** A miner will successfully solve a hash by generating a value lower than the network target. The network target is a hexadecimal number derived from a mathematical formula and determines the mining difficulty. Miners continuously adjust the nonce value and generate new hashes to meet the target. The reward for solving the hash on the Bitcoin blockchain is given to the miner who successfully completes the task. If the hash generated by a miner is greater than the target value, the miner increments the nonce by 1 and generates a new hash. This process continues until a hash is found that meets the target

criteria. This approach is employed by the entire network of miners, who compete to solve the hash in this manner. (Lantz and Cawrey, 2020, Chapter 8).

3.19.3 Proof-of-Work (PoW) performance:

According to (Nair and Dorai, 2021) The PoW algorithm tool was evaluated according to Energy Consumption, Fairness, and Reliability of the System as follows:

- **Energy Consumption:** Proof of Work (PoW) consensus algorithms in blockchain systems are known to have high energy consumption levels that remain consistent.
- **Fairness:** In terms of fairness, pure Proof of Work (PoW) models demonstrate the highest level of fairness, ensuring that coins are distributed equally among all nodes participating in mining. The distribution of coin age is also relatively even in pure PoW systems.
- **Reliability of the System:** Pure Proof of Work (PoW) systems exhibit excellent reliability in terms of performance and coin mining. These systems are highly reliable in solving the required equations for accurate block generation. The reliability remains consistent and does not vary significantly throughout the operation.

3.19.4 Proof-of-Work Security concerns:

According to (Nair and Dorai, 2021), the security vulnerabilities in the blockchain when using the proof-of-work algorithm are summarized in the following table 3.13:

Table 3.11: vulnerabilities of Pow. (Nair and Dorai, 2021).

No.	Attack	Is Proof of Work Vulnerable?
1.	DoS	✓
4	Selfish Mining	✓
5	Short-Range Attack	X
6	Long-Range Attack	X

No.	Attack	Is Proof of Work Vulnerable?
7	Coin-Age accumulation Attack	X
8	Pre-Computation Attack	X
9	Sybil Attack	✓

3.20 Proof-of-Stake (PoS) consensus algorithm

Proof-of-Stake (PoS) is a consensus algorithm used in blockchain networks to achieve consensus and validate transactions. Unlike Proof-of-Work (PoW), which relies on computational power and energy consumption, PoS selects block validators based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. PoS was developed with the aim to reduce the computational requirements and energy-saving alternatives to PoW (Nguyen, et all. 2019).

3.20.1 Proof-of-Stake (PoS) Mechanism:

Proof-of-Stake (PoS) is a consensus mechanism used in blockchain networks to achieve agreement on the state of the blockchain. PoS (Proof of Stake) relies on the selection of validators who are responsible for creating new blocks and validating transactions. The selection process is based on the amount of cryptocurrency held by the validators and their willingness to "stake" it as collateral. The PoS mechanism operates on the principle that validators with a larger stake in the network are more likely to act honestly and in the best interest of the blockchain. Instead of relying on computational power and solving complex mathematical puzzles like in Proof-of-Work (PoW), PoS selects validators based on their stake in the network. Validators are chosen to create new blocks in a deterministic manner, often based on factors such as the amount of cryptocurrency they hold and the duration of their stake. The selection process varies among different PoS implementations, but the general idea is to give higher probabilities of selection to validators with larger stakes. Once selected, validators propose and validate new blocks

by placing their stake as collateral. If a validator is found to have acted maliciously or tried to manipulate the network, they may lose a portion or the entirety of their stake as a form of punishment. PoS offers several advantages over PoW, including reduced energy consumption, as it doesn't require extensive computational power. It also encourages more participation and decentralization since validators can be selected based on their stake rather than specialized hardware. (Hasanova, at all. 2019).

According to (Nguyen, et all. 2019), The Follow-the-Satoshi (FTS) algorithm has found widespread adoption in various Proof of Stake (PoS) based blockchains, including Cardano, Sp8de, and Tezos. These networks utilize an indexing system where all tokens are assigned a unique identifier. The FTS algorithm is a hash function that operates on a seed, which can be the previous block's header or a random string generated by selected nodes. It produces a token index, which is used to locate the current owner of the token by searching the transaction history. This selected owner becomes the leader based on the FTS algorithm's output. The probability to choose the pi that node i is selected to be the leader in a network of N participants is:

$$P_i = \frac{S_i}{\sum_{j=1}^{N} S_j}$$

Si is the probability of a node being selected as the leader is proportional to its stake. Hence, nodes with higher stakes have a greater likelihood of being chosen as the leader.

In addition to the energy efficiency advantage, Proof-of-Stake (PoS) mechanisms offer faster transaction confirmation speeds compared to Proof-of-Work (PoW) mechanisms. In a blockchain network, transaction confirmation relies on two key factors: transaction throughput and block confirmation time. Transaction throughput refers to the number of transactions processed per second (Tx/s) by the network, which is crucial for network

performance, particularly when there is a high volume of pending transactions. The calculation of Tx/s involves, can be calculated by:

$$\mathrm{Tx/s} = \frac{\mathrm{Block_{size}}}{\mathrm{Tx_{size}} \times \mathrm{Block_{time}}}$$

See figure 11 Comparison between PoW & PoS:

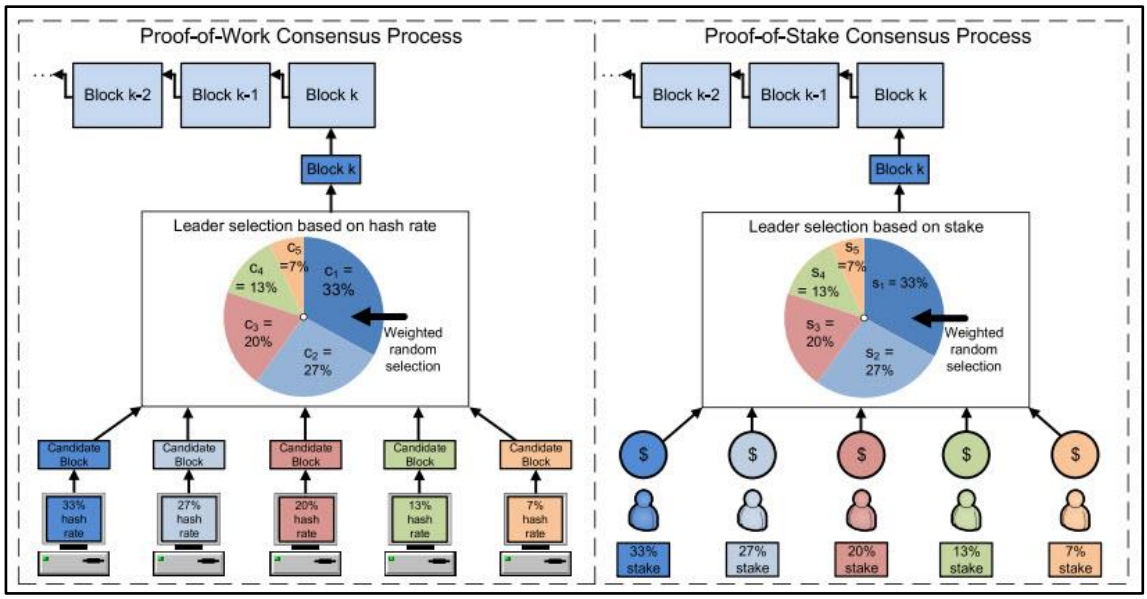

Figure 11: Comparison between PoW& PoS (Nguyen, et all. 2019).

3.20.2 Proof-of-Stake Security concerns:

According to (Nair and Dorai, 2021), the security vulnerabilities in proof-of-Stoke algorithm are summarized in the following table12:

Table 3.12: Vulnerabilities of PoS. (Nair and Dorai, 2021).

No.	Attack	Is Proof of Stake Vulnerable?
1.	DoS	✓
4	Selfish Mining	X
5	Short-Range Attack	✓
6	Long-Range Attack	✓
7	Coin-Age accumulation Attack	✓
8	Pre-Computation Attack	✓
9	Sybil Attack	✓

3.20.3 Security of Proof-of-Stake (PoS):

The security of Proof-of-Stake (PoS) protocols is influenced by several factors. One crucial factor is network synchrony, which plays a significant role in the security of many PoS protocols. In these protocols, leader selection processes are simulated through voting rounds, where participants send their votes to others. However, due to network delays and connection complexities, it is not guaranteed that all messages will be successfully transmitted. Therefore, considering network synchrony is essential for assessing the security of the protocol. Some PoS protocols are proven to be secure under partially synchronous network conditions, where messages reach their destinations within a specified time frame, or even under asynchronous conditions where messages may not reach their destinations at all (Nguyen, et all. 2019).

In addition to network synchrony, the incentive mechanism is crucial for the security of a PoS consensus mechanism. The reward scheme must provide incentives for consensus participation by rewarding block creators and validators. Simultaneously, it must also discourage malicious behaviors and prevent various attacks specifically targeting PoS, such as those involving the creation of a large number of blocks, which is comparatively easier in PoS. This section will delve into a range of emerging protocols based on the Proof of Stake (PoS) consensus algorithm that have gained significant traction. These protocols, namely Ouroboros, Chains-of-Activity, Casper, Algorand, and Tendermint, have been widely implemented and are known for their unique approaches to achieving consensus in PoS-based blockchain networks. Through their innovative designs and mechanisms, these protocols aim to address various challenges associated with traditional

consensus algorithms, offering enhanced security, scalability, and decentralization. See Figure 12.

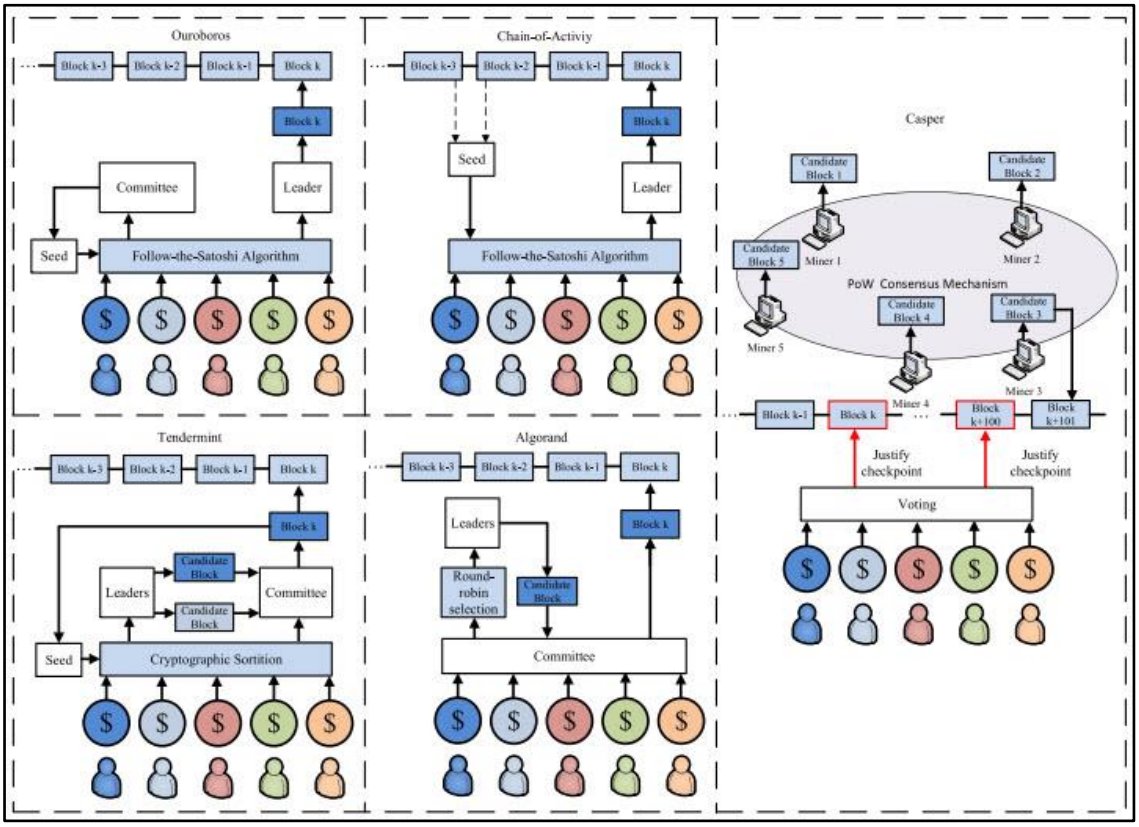

Figure 12: Illustrations of several PoS consensus processes

- **OUROBOROS:** is a Proof-of-Stake (PoS) protocol that utilizes a dynamic committee selection process based on stake distribution. The protocol divides time into epochs, and during each epoch, committee members participate in a 3-phased coin tossing protocol to generate seeds for the FTS algorithm. The FTS algorithm then outputs coin indices, and the current owners of these coins are chosen as leaders and become committee members in the next epoch. Unlike Proof-of-Work (PoW) protocols, Ouroboros leaders only create empty blocks, while input endorsers confirm and add transactions to the blocks. Block rewards are shared among committee members, leaders, and input endorsers to incentivize participation. Ouroboros incorporates a stake delegation mechanism, allowing stakeholders to delegate their participation

rights in the committee, encouraging smaller stakeholders to contribute to the consensus process. The protocol assumes a partial synchrony network and is proven to be secure when the adversary controls less than 51% of the total stake. However, Ouroboros considers asynchronous nodes as part of the adversary nodes due to practical limitations in guaranteeing network synchrony. The dynamic stake distribution and creation process in Ouroboros mitigate biased behavior and grinding attacks, where block proposers attempt to influence leader selection rounds by trying different block hashes. The protocol also addresses attacks involving secret alternative forks, such as the nothing-at-stake attack and long-range attack, by designating only one leader in each round. However, Ouroboros is still vulnerable to 51% attacks. Ouroboros offers advantages such as low transaction confirmation time (around 2 minutes), high transaction throughput (around 257 Tx/s), and minimal energy consumption compared to PoW-based networks. It also stands out for its formal definitions and strong theoretical foundation supporting security and incentive compatibility. As a result, Ouroboros has been adopted by several cryptocurrencies (Nguyen, et all. 2019).

- **CHAINS-OF-ACTIVITY:** Chains-of-Activity (CoA) is another Proof-of-Stake (PoS) protocol similar to Ouroboros. In CoA, the leader selection process is based on the FTS algorithm, but the seed for the algorithm is determined differently. The chain is divided into groups of blocks, and the hash of each block within an epoch is used to seed the FTS algorithm for selecting the next epoch's leaders. CoA introduces checkpoint blocks that solidify the chain and prevent long adversarial forks from taking over. The protocol also requires leaders to make a deposit before creating a block, and the block reward is claimed if the block is created properly. This deposit

scheme helps prevent double-spending attacks and bribe attacks. The CoA protocol mitigates grinding attacks by seeding the FTS algorithm with hashes from the previous group of blocks. It also addresses nothing-at-stake and long-range attacks by designating only one leader per round. Long-range attacks, where stakeholders sell their stakes after realizing they will be leaders in the next epoch, are mitigated by the checkpoint blocks mechanism. CoA has low energy consumption as only one block is created per round. It also offers a low transaction confirmation time of around 6 minutes and a high transaction throughput of 40 Tx/s. The cryptocurrency Tezos is partially designed based on the CoA protocol (Nguyen, et all. 2019).

- **CASPER:** The Casper protocol was introduced by the Ethereum network to facilitate the transition from a Proof-of-Work (PoW) protocol to a pure Proof-of-Stake (PoS) protocol. Unlike other PoS protocols, Casper does not interfere with the leader selection process. Instead, it utilizes a dynamic committee that employs a Byzantine-Fault Tolerance (BFT) protocol to vote on and justify checkpoint blocks at regular intervals, such as every 100 blocks. Blocks up to the second latest justified checkpoint are considered finalized. To join the committee, validators must make a deposit proportional to their desired voting power. The deposit can be slashed for engaging in malicious behavior. Casper is proven to be secure if at least 2/3 of the voting power is controlled by honest validators in a partially synchronous network. By incorporating a withdrawal delay, the protocol can address dynamic stake distribution and mitigate long-range attacks. One notable advantage of Casper is its compatibility with existing PoW protocols, providing additional security to the underlying chain. However, Casper's performance is contingent on the performance of the underlying

PoW mechanism. Ethereum has been actively developing Casper and is expected to implement it in future PoW-based blockchain protocols (Nguyen, et all. 2019).

- **ALGORAND:** The Algorand protocol, similar to Ouroboros, operates with a committee but uses a cryptographic sortition mechanism instead of the FTS algorithm for leader and committee member selection based on stake distribution. The cryptographic sortition employs a Verifiable Random Function (VRF) to assign nodes a range of hash values proportional to their stake, and the selection is revealed only when the node submits a proof. The initial seed is generated using a distributed random number generator and updated through the VRF for subsequent rounds. Unlike other protocols, Algorand does not rely solely on leader selection for security. The committee votes to finalize blocks in each round, eliminating forks and mitigating attacks such as double spending, long-range attacks, nothing-at-stake attacks, and bribe attacks. Grinding attacks are mitigated by distributing private keys in advance of the seed. Energy consumption in Algorand is low as participants don't compete in hash rate, and transaction throughput can reach up to 875 Tx/s. The protocol offers immediate finality, resulting in faster transaction confirmation times (around 20 seconds) compared to protocols based on the longest chain rule. Algorand has been adopted by various cryptocurrencies, including Algorand and Arcblock (Nguyen, et all. 2019).
- **TENDERMINT:** The Tendermint protocol utilizes a Byzantine Fault Tolerance (BFT) voting mechanism for block confirmation. Validators gain voting rights through a deposit and a proposer is selected from the validators to propose a block in each round. Validators vote to confirm proposed blocks, ensuring immediate finality of blocks and transactions. Block rewards are distributed among validators while

deposits are confiscated for malicious behavior. Under the assumption of a partially synchronous network, Tendermint is secure as long as 2/3 of the voting power is controlled by honest participants. Fork-related attacks are mitigated since there are no forks in Tendermint. Tendermint has low energy consumption as only one block is created per round. It offers high transaction throughput (up to 800 Tx/s) and fast transaction confirmation times (around 1 second on average) due to immediate block finality. However, formal definitions and theoretical analysis are lacking, and the incentive mechanism is not thoroughly examined. Tendermint is currently applied in practical use cases like BigchainDB and Ethermint.

3.21 Proof of Activity (PoA)

Rosenfeld and Vessenes introduced the Proof-of-Activity (PoA) method as a consensus mechanism in 2014 (Rosenfeld and Vessenes, 2014). PoA combines components from Proof of Work (PoW) and Proof of Stake (PoS) to create a consensus technique that is more secure and energy-efficient.

3.21.1 Mechanism of Proof-of-Activity (PoA):

According to (Bentov et al., 2014) using their hash power, miners try to create an empty block header in PoA. The block header content a preceding block's hash, the miner's public address, the block's height in relation to the genesis block, and a nonce make up. The block header does not reference any transactions. A miner broadcasts an empty block header to the network when they successfully create one with a hash lower than the current difficulty target. The network nodes collectively utilize the hash of the block header as a source of pseudorandom stakeholders. The derivation process involves concatenating the hash with the previous block's hash and fixed suffix values, hashing

each combination, and invoking "follow-the-satoshi" with each resulting hash as input. Stakeholders who are online validate the empty block header for correctness and check if they are one of the lucky stakeholders derived from the block. The lucky stakeholders sign the hash of the block header with their private key and broadcast their signature. The Nth stakeholder, upon seeing that the block derives them, creates a wrapped block. This wrapped block extends the empty block header by including transactions, the signatures of the other derived stakeholders, and the stakeholder's own signature for the entire block. The wrapped block is then broadcasted to the network. Other nodes validate the wrapped block and consider it a legitimate extension of the blockchain if it meets the necessary criteria. The Proof-of-Activity algorithm combines the security guarantees of PoW with the efficiency benefits of PoS, resulting in a consensus mechanism that offers a balance between energy consumption and network security.

3.21.2 Proof-of-Activity (PoA) Mining Process:

The Proof-of-Activity (PoA) system combines both of consensus algorithm Proof-of-Work (PoW) and Proof-of-Stake (PoS) systems. In the PoA mining process, miners initially compete to find a new block using computational power, similar to PoW. Once a new block (or mined) is found, the system transitions to PoS. The block contains only a header and the miner's reward address. Based on the header information, a random group of validators is selected from the network. These validators are responsible for validating and signing the new block. The selection of validators is based on their coin ownership, with more coins increasing their chances of being selected. After all validators sign the block, it becomes a complete block and is added to the blockchain. Transactions are recorded on this block. If some signers are unavailable, the process moves to the next winning block with a new set of validators chosen randomly based on their coin stake.

This continues until a winning block receives the required number of signers and becomes complete. Mining fees and rewards are distributed among the miner and validators who contributed to signing the block. The PoA system has received criticism for its partial use of both PoW and PoS. The mining process still requires significant computational power during the PoW phase, and individuals with larger coin holdings have a higher likelihood of being selected as validators and accumulating more virtual currency rewards (Seth, et all. 2021).

3.22 The proposed hybrid algorithm SMO

3.22.1 hybrid algorithm SMO introduction:

In this study, we propose a hybrid algorithm that we call SMO, as this algorithm is based on a work similar to the Proof-of-Activity (PoA) algorithm in terms of relying on the mining process through the PoW consensus algorithm and the process of verifying the reliability of the block to be added on the network through the consensus algorithm. PoS, where the proposed hybrid algorithm SMO is characterized by having a Block Banck that contains malicious blocks that the system recognized earlier and uses Machine Learning (ML) in early detection of malicious blocks before they enter the verification stage and if the malicious block is not detected by Through the (ML) it is subjected to the validation process through the PoS consensus algorithm. See Figure 13.

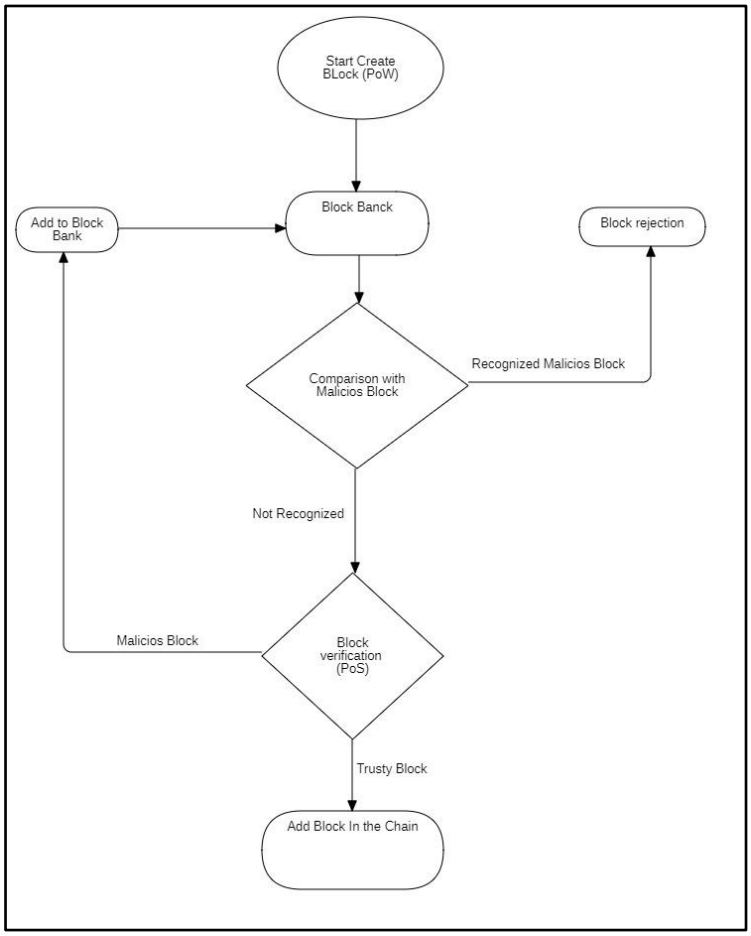

Figure 13: Diagram for a hybrid algorithm SMO.

3.22.2 Mechanism of a hybrid algorithm SMO:

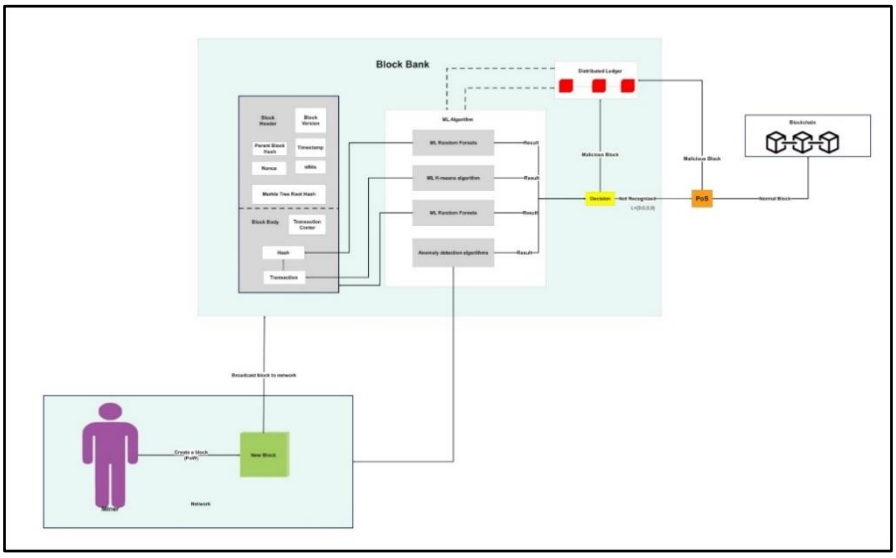

Figure 14: Block Diagram for a hybrid algorithm SMO.

As shown in Figure 14, the SMO Hybrid Consensus Algorithm works. Miners start to compete with each other to make the block using the PoW consensus algorithm. After that, the miner broadcasts the block he produced to the network. After that, the block passes through the Block Banck layer (the first time when creating the first block in the network the Distributed Ledger is empty, and then the malicious blocks that are identified are placed) as when the block reaches the Block Bank Layer, the machine learning algorithms begin to work in order to verify whether the block is malicious or if it is a natural block by relying on comparison with the previously identified malicious blocks in the Distributed Ledger in order to detect early detection of malicious blocks before bypassing the additional protection layer Block Bank, where the Random Forests Algorithm machine learning algorithm works to try to detect the truth of the block through the work By analyzing various features of blocks, such as transaction details, timestamps, and previous block information (Breiman, L. 2001 & Ho, T. K. 1998 & Zhang, W., & Yu, P. S. 2005)Analysis between the proposed block and the malicious blocks, and the machine learning algorithm K-means can Distinguishes malicious blocks by grouping similar blocks based on their features. You recursively assign blocks to different groups, where each group is represented by its own centroid. Feature selection is critical in identifying malicious behavior within blocks. By identifying relevant features such as transaction size, frequency, timestamps, and previous block information, the algorithm can group blocks with similar patterns together. Malicious clusters often exhibit distinct characteristics that differ from legitimate ones, and the K-means algorithm can identify these anomalies as they form discrete clusters. We draw on this from what researchers have explored in the application of K-Methods in anomaly detection and intrusion detection systems, demonstrating its ability to effectively distinguish and classify

malicious and legitimate blocks (Almomani et al., 2020; Wu et al., 2017), and using the machine learning algorithm Hidden Markov Models (HMMs) to identifies malicious blocks by modeling the underlying sequence of blockchain states and identifying patterns of suspicious behavior. In the context of the blockchain, where the sequence of blocks and their properties are represented as a series of hidden states, and the transactions within each block are seen as notes. HMMs can learn transition probabilities between hidden states and emission probabilities for observations. By training on a dataset containing each of the malicious blocks in the infiltration of malicious blocks that the algorithm has previously identified and stored in the Distributed ledger, the HMM can capture distinct behaviors associated with different types of blocks. During the discovery phase, the algorithm can analyze the sequence of observed transactions in a block and infer the most likely sequence of hidden states, which correspond to different types of blocks. By comparing the observed sequence probability within acquired HMMs for malicious and legitimate blocks, the algorithm can classify a given block as either malicious or harmless. HMM's strength lies in its ability to model temporal dependencies and capture complex patterns in data, making it a promising approach for detecting malicious blocks in a blockchain environment (Bhatia et al., 2017; Dorri et al., 2020), as well as the machine learning algorithm Anomaly detection algorithms it works to distinguish malicious blocks by identifying unusual and abnormal patterns in the blockchain data. These algorithms operate on the assumption that malicious blocks exhibit behaviors that deviate significantly from the norm. By analyzing various features of blocks, such as transaction size, timestamps, and block size, flaw detection algorithms can build a model of normal behavior in the blockchain and can identify malicious blocks by analyzing the behavior of previously identified malicious blocks stored in the Distributed ledger. By leveraging

these anomaly detection algorithms, blockchain systems can effectively identify and mitigate malicious activities in real time, based on what the researchers found (Chandola et al., 2009; Liu et al., 2012), where the result for each comparison is 0 in the event that the machine learning algorithm fails to detect the truth of the proposed block if it is natural or malicious and it is Result 1 if it can identify it as a malicious Block.

In the event that the result of all machine learning algorithms is that they could not recognize the type of the proposed block, we have the following equation formed from a linear matrix:

$$BT= \{0,0,0,0\}$$

Whereas, BT is the final decision result of the machine learning algorithms.

Then it is sent to the next layer for consensus on the validity of the block proposed by the Proof-of-Stake algorithm based on ALGORAND.

In the event that one of the machine learning algorithms was able to recognize the type of the proposed block, the work is stopped by the rest of the machine learning algorithms, and the proposed block is sent to the Distributed Ledger, and we have one of the following matrices:

$$BT= \{1,0,0,0\}$$

$$BT= \{0,1,0,0\}$$

$$BT= \{0,0,1,0\}$$

$$BT= \{0,0,0,1\}$$

The following is an explanation of the phases of the SMO hybrid algorithm.

a) Create a block: In SMO hybrid algorithm, blocks are generated by PoW consensus algorithm. the process of building a block by a miner involves several steps:
b) Transaction Collection: Miners collect valid transactions from the network mempool. These transactions are typically grouped together to form a new block.
c) Block Header Construction: The miner constructs the block header, which includes information such as the previous block hash, timestamp, and a nonce (a random number). The nonce will be adjusted to find a hash value that meets the difficulty criteria specified by the network.
d) Nonce Calculation: The miner starts the process of calculating the nonce value by combining it with the block header. This combined data is then hashed using a cryptographic hash function, such as SHA-256, to generate a hash value.
e) Hash Comparison: The generated hash value is compared against the difficulty target set by the network. The difficulty target determines the number of leading zeros the hash value should have for it to be considered valid. If the generated hash does not meet the target criteria, the miner increments the nonce and repeats the hashing process.

Block Bank:

It is an additional layer of protection consisting of a channel or a series of machine learning algorithms that are applied to the block in order to verify it, as well as consisting of a Distributed Ledger to store blocks that have been classified as malicious.

Distributed Ledger is independent of the network. When the chain is created, it is empty, and then the malicious blocks that are identified by the Proof-of-Stake consensus algorithm are stored inside it.

When the miner sends the block to be added to the blockchain, it goes through a series of machine learning algorithms (Block Bank Layer), where the Random Forests Algorithm is initially applied in order to compare the proposed block with the malicious blocks that were stored in the Distributed Ledger by comparing Signature Analysis and trying to identify if the block is malicious (See Figure 15). In the event that the block is malicious, it is stored in the Distributed Ledger, and if the block is not recognized the result is 0 else if the block was recognized as malicious the result is 1. Since all machine learning algorithms will only have a result of 0 or 1, ML algorithm K-means, where it compares the proposed block with the previously defined malicious blocks through Transaction Analysis. ML algorithm Hidden Markov Models (HMMs), where this algorithm works on Behavior Analysis and compares it with the behavior of pre-defined malicious blocks. In the event that the proposed block is not recognized, it is moved to the Anomaly detection (Isolation Forest) algorithms, to compare the proposed block with malicious blocks in terms of Network Analysis. Recognizing it is moved to the next step to validate it through the Proof-of-Stake consensus algorithm. See Figure 16. Flowchart Diagram of Block Bank in Hybrid Algorithm SMO.

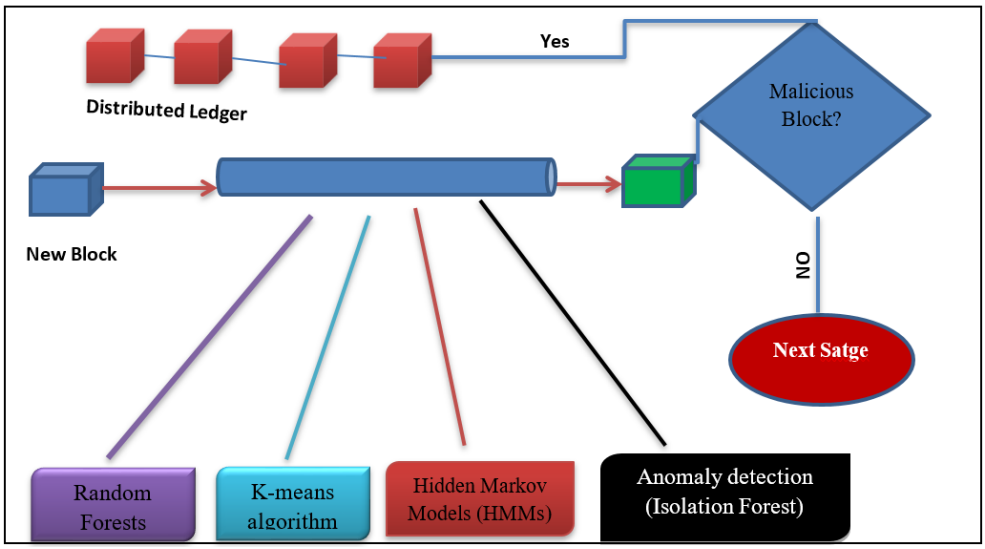

Figure 15: Illustration of Block Bank in Hybrid Algorithm SMO.

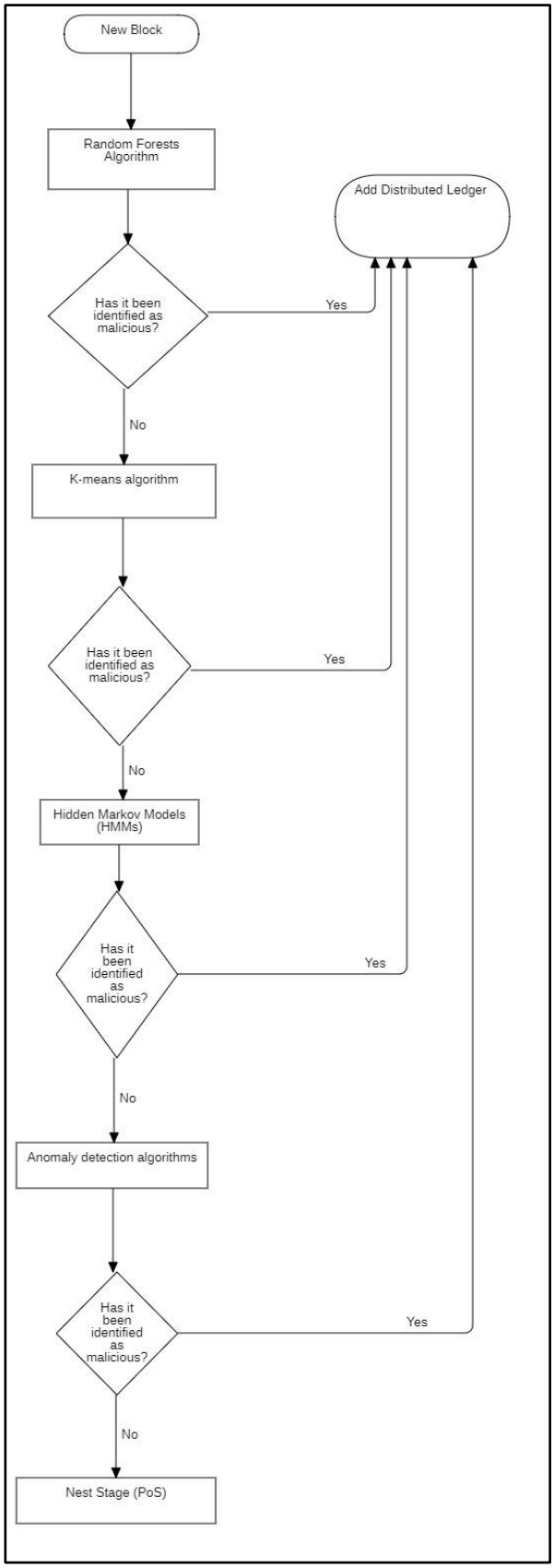

Figure 16: Flowchart Diagram of Block Bank in Hybrid Algorithm SMO.

Verification and decision: At this stage, a decision is made about the block proposed to be added to the Blockchain through the Proof-of-Stake algorithm based of ALGORAND protocol, where the decision is made about the block by adding it to the Blockchain if it is a valid block or by adding it to the Block Bank if it is a malicious block, where the action steps include the following:

Committee Formation: A committee is formed from the set of participating nodes in the network. The committee members are selected randomly using a cryptographic sortition mechanism based on their stake in the network.

Voting and Verification: Upon receiving the proposed block, each committee member independently verifies the validity of the block and its transactions. They then vote on whether to accept or reject the proposed block.

Block Finalization: If a sufficient number of validators agree on the validity of the block, it is considered finalized and added to the blockchain. Once added, it becomes part of the immutable ledger, In the event that the participating majority votes that the block is malicious, it is added to the Block Bank

Rewards and Penalties: Committee members who voted honestly and correctly are rewarded with additional cryptocurrency tokens as an incentive for their participation. On the other hand, committee members who voted dishonestly or maliciously may face penalties, such as losing a portion of their stake.

Next Round: The consensus process continues with the formation of a new committee and the selection of a new block proposer for the next round.

3.23 Machine learning algorithms used in hybrid algorithm SMO

3.23.1 ML Random Forests Algorithm:

Is an ensemble learning algorithm that combines multiple decision trees to make predictions or classifications. It was first introduced by Leo Breiman and Adele Cutler in 2001 and has gained popularity in various domains, including machine learning and data mining. In Random Forests, a collection of decision trees is constructed, each trained on a different subset of the data. During the training process, each tree is built by randomly selecting features and data samples. This randomness helps in reducing overfitting and increasing the diversity of the trees. To make predictions, the input data is passed through each decision tree in the forest, and the final prediction is determined by aggregating the individual predictions from the trees. This aggregation can be done by taking the majority vote in classification tasks or averaging the predicted values in regression tasks. The Random Forests algorithm has several advantages, including its ability to handle high-dimensional data, detect feature importance, and handle missing values without the need for imputation. It is also resistant to overfitting and generally provides good generalization performance. Random Forests have been widely used in various applications, such as image classification, fraud detection, and bioinformatics. Its effectiveness and versatility make it a popular choice in the field of machine learning. (Breiman, L. 2001).

3.23.2 **K-means algorithm:**

A machine learning algorithm used for clustering data into distinct groups based on their similarity. It aims to partition the data points into K clusters, where each point belongs to the cluster with the nearest mean value. The algorithm iteratively assigns

data points to the nearest cluster centroid and updates the centroids based on the new assignments. This process continues until convergence, where the assignments and centroids no longer change significantly. K-means is a simple and widely used algorithm in the field of unsupervised learning. It has applications in various domains such as image segmentation, customer segmentation, and anomaly detection. (Hartigan, et all. 1979).

3.23.3 **Hidden Markov Models (HMMs):**

Are probabilistic models widely used for modeling sequential data, where the underlying system is assumed to be a Markov process with hidden states. HMMs have applications in various fields, including speech recognition, natural language processing, bioinformatics, and more. In an HMM, the observed data is modeled as a sequence of observations, while the hidden states represent the unobserved or latent factors that generate the observations. The transitions between hidden states follow a Markov property, meaning the probability of transitioning to a new state only depends on the current state. Additionally, each hidden state emits an observation with a certain probability distribution. HMMs are typically trained using the Baum-Welch algorithm, also known as the forward-backward algorithm, which estimates the model parameters based on the observed data. Once trained, HMMs can be used for various tasks, such as sequence prediction, state estimation, and anomaly detection. (Rabiner, L. R. 1989).

3.23.4 **Anomaly detection algorithms:**

refer to a class of machine learning techniques used to identify unusual or abnormal patterns in data. These algorithms aim to distinguish anomalous instances from the

majority of normal instances in a dataset. The specific implementation and methodology of anomaly detection algorithms can vary, but they generally involve modeling the normal behavior of the data and then identifying instances that deviate significantly from this model. (Chandola, et all. 2009).

3.24 SMO Blockchain Security:

There are several security risks facing blockchain that the proposed hybrid consensus algorithm, SMO, aims to solve or reduce the likelihood of. in this section we address key scenarios as follows:

3.24.1 **Denial of Service (DoS) attacks:**

Attackers flood the network with malicious and false blocks, straining network resources, hindering user access, and usage (Hasanova et al., 2019). To safeguard against this risk, the SMO consensus algorithm introduces an additional protection layer, called Block Bank. This layer verifies and attempts to detect malicious blocks using machine learning algorithms (Random Forests, K-means, Hidden Markov Models, and the Isolation Forest anomaly detection), neutralizing such attacks and preventing network flooding with malicious blocks before they reach the validators.

3.24.2 **Sybil Attacks:**

Attackers create rogue nodes to conduct fraudulent transactions, disrupting the blockchain (Nair and Dorai, 2021). To counter this, machine learning algorithms (Random Forests, K-means, Hidden Markov Models, and the Isolation Forest anomaly detection) attempt to identify malicious blocks. These blocks then proceed to the third verification stage using the POS consensus algorithm. Consequently, each

potential block undergoes two auditing stages, making it more challenging for attackers to add a malicious block to the network effectively.

3.24.3 **Short-range Attacks:**

These include stakeholder bribing, exploiting specific network stakeholders' trust or influence (Hasanova et al., 2019). The proposed SMO consensus algorithm overcomes this attack type by subjecting blocks to an additional protection layer, Block Bank, for auditing by machine learning algorithms (Random Forests, K-means, Hidden Markov Models, and the Isolation Forest anomaly detection). This early detection of malicious blocks before reaching the validators reduces the chances of including compromised blocks on the network, diminishing the risk of collusion among validators.

3.25 Related Work Machine learning with Blockchain

Random Forests Algorithm was used to develop a system for detecting fraudulent transactions on the Ethereum blockchain. The system uses Random Forests to classify transactions as fraudulent or legitimate based on a variety of features, such as the sender and receiver addresses, the amount of cryptocurrency transferred, and the time of the transaction. (Yang, Zhang, & Zhang, 2023).

K-means algorithm was used to develop a system for clustering transactions on the Bitcoin blockchain. The system uses K-means to cluster transactions together based on their similarity. The clusters can then be used to identify fraudulent transactions, such as those that involve multiple addresses that are known to be associated with fraudulent activity. (Vaswani et al., 2017).

Hidden Markov Models (HMMs) algorithm was used to develop a system for detecting anomalous behavior on the Ethereum blockchain. The system uses HMMs to model the normal behavior of transactions on the blockchain. Any transactions that deviate from the normal behavior are flagged as anomalous. (Amodei et al., 2021).

Anomaly detection algorithms was used to develop systems for detecting fraudulent transactions and anomalous behavior on a variety of blockchains. Anomaly detection algorithms typically work by identifying transactions or blocks that deviate from the normal behavior of the blockchain. These transactions or blocks can then be flagged for further investigation. (Amodei et al., 2021).

3.26 Overview of blockchain applications in smart cities

Blockchain technology has attracted a lot of interest as a means of enabling safe and decentralized transactions. In smart cities, this technology may be utilized in a variety of ways to manage and secure data transmission and guarantee transparency across a range of industries, including transportation, energy, and healthcare (Alcarria et al., 2020). Building trust amongst stakeholders, including people, governmental organizations, and private businesses, is one of the main advantages of implementing blockchain in smart cities (Li et al., 2021). Blockchain technology, for instance, may automate and enforce agreements between participants by utilizing smart contracts, which eliminates the need for middlemen (Kshetri, 2018). Another benefit is the high degree of security and anonymity that blockchain may offer, which is essential for safeguarding sensitive data and deterring cyberattacks (Singh et al., 2020). In essence, by fostering more efficiency, transparency, and stakeholder confidence, blockchain technology has the potential to completely transform how smart cities function.

3.27 Case studies of blockchain in some smart city projects around the world

Through the facilitation of safe and decentralized transactions, blockchain technology has the potential to revolutionize urban infrastructure. Governments and towns all around the world have started a number of blockchain-based smart city projects in response to this potential. The Dubai Blockchain Strategy is one of the most well-known blockchain projects in a smart city. This policy, which was introduced in 2016, intends to employ blockchain technology to improve efficiency and security across a number of industries, including transportation, healthcare, and finance (Smart Dubai, 2018). Blockchain technology has been specifically employed by the Dubai Electricity and Water Authority (DEWA) to make it possible for users to pay their bills, monitor their energy use, and take part in renewable energy projects. "Smart Dubai," a blockchain project by the DEWA, has decreased transaction times and costs while enhancing data security (Alcarria et al., 2020).

The Seoul Blockchain Governance Team is another noteworthy instance of how blockchain technology is being used in smart cities. Blockchain technology has been used by this team to provide transparent and safe voting processes for municipal elections. The system makes use of a blockchain-based identification mechanism that allows users to confirm their identity before to voting, preserving the fairness of the electoral process (3).

The city of Amsterdam has also implemented blockchain technology in its efforts to become more sustainable. The city's "Powerpeers" platform uses blockchain technology to create a peer-to-peer energy trading system, allowing residents to trade excess energy generated by solar panels. This initiative has led to a reduction in energy costs and has enabled residents to participate in the transition to renewable energy (Swan, 2015).

In addition to these projects, several other cities have implemented blockchain technology to address various urban challenges. For instance, the city of Austin, Texas has partnered with a blockchain startup to create a platform for ride-sharing services, while the city of Moscow has used blockchain technology to create a transparent and secure real estate registry (8,9).

blockchain technology has the potential to transform urban infrastructure by facilitating secure and decentralized transactions. Several smart city projects around the world have demonstrated the versatility of blockchain technology in addressing a wide range of urban challenges, from data management to energy sustainability.

3.28 Comparison of blockchain solutions in smart city projects

Several blockchain solutions have been developed and implemented in various smart city projects around the world. Each solution has its own strengths and weaknesses, depending on the specific use case and the needs of the city. In this section, we will compare some of the most common blockchain solutions in smart city projects.

Firstly, permissioned blockchains are a popular choice for smart city projects. These blockchains are private, meaning that access to the blockchain is restricted to a specific group of users who have been granted permission to access the network. Permissioned blockchains are often used in situations where data privacy and security are of utmost importance, such as in healthcare or financial services. For example, the Dubai Blockchain Strategy mentioned earlier uses a permissioned blockchain to ensure data security in its healthcare sector (Smart Dubai, 2018).

Secondly, public blockchains are another option for smart city projects. These blockchains are open to anyone, and transactions on the network are publicly visible.

Public blockchains offer the advantage of transparency, but they can be less secure than permissioned blockchains. In smart city projects, public blockchains are often used for initiatives that require transparency and accountability, such as voting systems. The Seoul Blockchain Governance Team mentioned earlier uses a public blockchain for its secure voting system (Kshetri, Nir. 2018).

Thirdly, hybrid blockchains combine the features of both permissioned and public blockchains. In a hybrid blockchain, the network is private, but certain data is made publicly visible. This approach offers the benefits of both privacy and transparency. For example, the Powerpeers platform in Amsterdam uses a hybrid blockchain to enable peer-to-peer energy trading while maintaining data privacy (Swan, 2015).

Fourthly, consortium blockchains are another option for smart city projects. Consortium blockchains are controlled by a group of organizations rather than a one single entity. This approach offers the benefits of decentralization while still allowing for a certain level of control. For example, the city of Moscow's real estate registry mentioned earlier uses a consortium blockchain to ensure transparency and security in property transactions (Deloitte Insights, 2018).

Lastly, sidechains are a more recent development in the blockchain space. blockchain a main network, and Sidechains are essentially separate blockchains that are connected to the main. This approach offers scalability and flexibility, as sidechains can be customized to suit specific use cases. For example, the city of Austin's ride-sharing platform mentioned earlier uses a sidechain to enable seamless payments between riders and drivers (Ekblaw et al., 2016).

there is no one-size-fits-all solution when it comes to blockchain in smart city projects. The choice of blockchain solution depends on the specific use case and the needs of the city. Permissioned, public, hybrid, consortium, and sidechain blockchains all have their own strengths and weaknesses, and each solution must be carefully considered before implementation. See Table 3.13:

Table 3.13: comparison of blockchain solutions in smart city projects

#	Blockchain Solution	Characteristics	Examples in Smart City Projects
1.	Permissioned	Private, restricted access, high security	Dubai Blockchain Strategy for healthcare data (Smart Dubai, 2018).
2.	Public	Open, transparent, lower security	Seoul Blockchain Governance Team for voting (Kshetri, Nir. 2018).
3.	Hybrid	Combination of permissioned and public, selective data visibility	Powerpeers platform in Amsterdam for energy trading (Swan, 2015).
4.	Consortium	Controlled by a group of organizations, decentralized	Moscow's real estate registry for property transactions (Deloitte Insights, 2018).
5.	Sidechain	Separate blockchain connected to main blockchain, customizable	Austin's ride-sharing platform for payments (Ekblaw et al., 2016).

3.29 Smart Cities

Although there are many definitions of the concept of a smart city, they all refer to the integration of technology, data, and people to improve the quality of life, improve sustainability, and simplify urban services. (United Nations, 2014) It aims to use technology to address urbanization challenges, such as traffic congestion, air pollution, and waste management, by making cities more efficient, livable, and responsive to the needs of their citizens. (IBM, n.d.).

3.29.1 Characteristics of Smart Cities:

Smart cities have many important characteristics that aim to enhance the importance of smart cities that make them able to achieve their basic goals by overcoming the problems that traditional cities suffer from as a result of the growth of urbanization and the increase in population, including:

- Advanced technology infrastructure.
- Intelligent transportation systems.
- Sustainable energy management.
- Resilient environments.
- Efficient use of resources.
- Inclusiveness and citizen engagement (Smart Cities Council, n.d.).

3.29.2 Technologies Used in Smart Cities:

The development of smart cities depends on a variety of technologies that are used in all aspects of life in order to help them achieve an effective response, overcome all obstacles they face, and provide services with high efficiency and effectiveness, from these technologies:

- Internet of Things (IoT) devices.
- Big Data analytics.
- Artificial intelligence (AI).
- Cloud computing.
- 5G networks (Accenture, n.d.).

3.29.3 Advantages of Smart Cities:

Smart cities offer several advantages, including:

- Improved quality of life for citizens
- Increased sustainability and efficiency of urban services
- Better traffic management and reduced congestion
- Enhanced public safety and security
- Improved waste management (Smart Cities Dive, 2018).

3.29.4 Challenges of Implementing Smart Cities:

Despite the potential benefits, there are several challenges associated with implementing smart cities, including:

- The absence of technology standards and interoperability
- Privacy and security concerns
- High costs of implementation
- Inadequate infrastructure and resources
- Difficulty in involving and engaging citizens (Böck & Widener, 2020).

3.29.5 Smart Cities and Blockchain Technology:

Blockchain technology has the potential to play a significant role in the development of smart cities. It can provide a secure, decentralized platform for storing and exchanging data, which can improve the efficiency and transparency of various urban services, such as waste management and transportation. (Iansiti & Lakhani, 2017).

Furthermore, blockchain technology can enable citizens to participate in decision-making processes and benefit from the smart city services, thereby promoting inclusiveness and

citizen engagement. For example, blockchain-based voting systems can allow citizens to vote on proposals for city development, and blockchain-based reward systems can incentivize citizens to participate in sustainable behavior. (Kshetri, Nir. 2018).

However, there are also challenges associated with the integration of blockchain technology into smart cities, such as the need for standardization and scalability. Nevertheless, the potential benefits of combining blockchain and smart city technologies make it an area worth exploring.

3.29.6 Architecture of Smart Cities:

Before the integration of blockchain technology, smart cities typically had a centralized architecture, where a single entity controlled the data and decision-making processes. This often resulted in a lack of transparency and security, as the central authority had complete control over the data.

The architecture of a centralized smart city is typically composed of several layers, each of which is responsible for a different aspect of the city's operations. At the bottom layer, the physical infrastructure of the city provides the foundation for the smart city system, including sensors, networks, and devices that gather and transmit data (Zhu, Xu, & Shen, 2016). The data layer processes and stores the information collected by the physical infrastructure, often utilizing cloud-based computing and storage solutions (Gubbi et al., 2013). The application layer uses this data to create innovative and efficient services for citizens, such as traffic management systems and waste management optimization (Lee, Phaal, & Lee, 2013). Finally, the governance layer is responsible for managing the overall system and ensuring that it is operating effectively and ethically. This includes

establishing policies and regulations for data privacy and security, as well as managing relationships with stakeholders and vendors (Coeckelbergh, 2019). See figure 17.

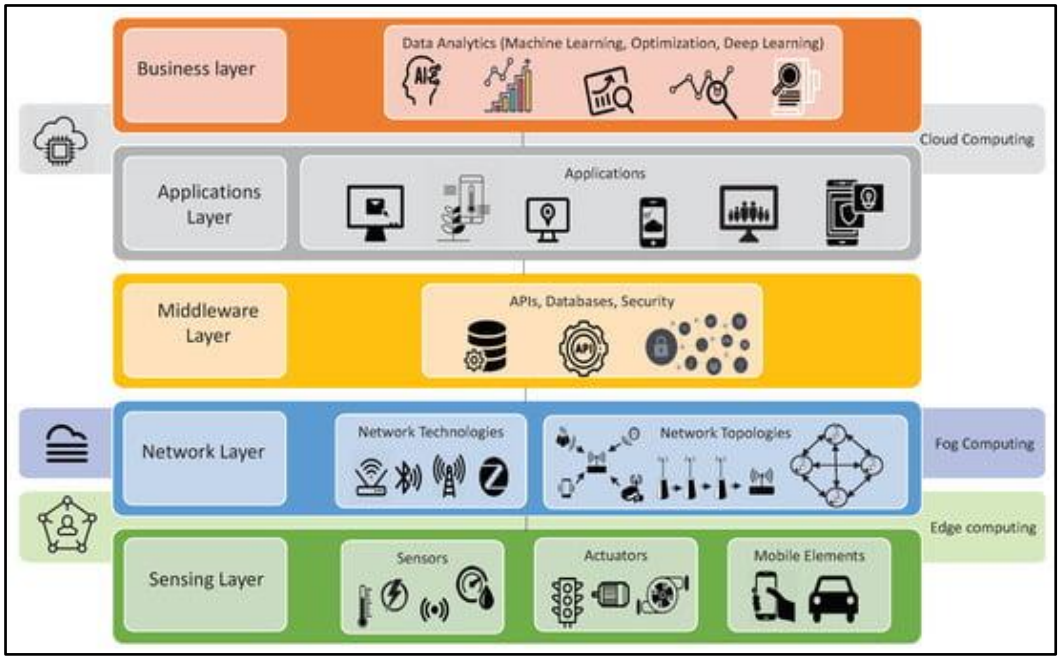

Figure 17: Centralized Smart city architecture (Turesinin et al., 2020)

On the other hand, cities that use blockchain technology have a decentralized architecture, where data is stored and managed across a network of nodes. This eliminates the need for a central authority, increasing the transparency and security of the data and processes.

The architecture of a smart city that depends on blockchain is typically composed of several layers, each of which is responsible for a different aspect of the city's operations. At the bottom layer, the physical infrastructure of the city provides the foundation for the smart city system, including sensors, networks, and devices that gather and transmit data (Dorri, Kanhere, Jurdak, & Gauravaram, 2017). The data layer processes and stores the information collected by the physical infrastructure, often utilizing blockchain technology for data storage and management (Li, Lu & Xu, 2020). The application layer uses this data to create innovative and efficient services for citizens, such as traffic management systems and waste management optimization (Shen et al., 2018). Finally, the governance layer is responsible for managing the overall system and ensuring that it is operating

effectively and ethically. This includes establishing policies and regulations for data privacy and security, as well as managing relationships with stakeholders and vendors (Zhang et al., 2018). See figure 18.

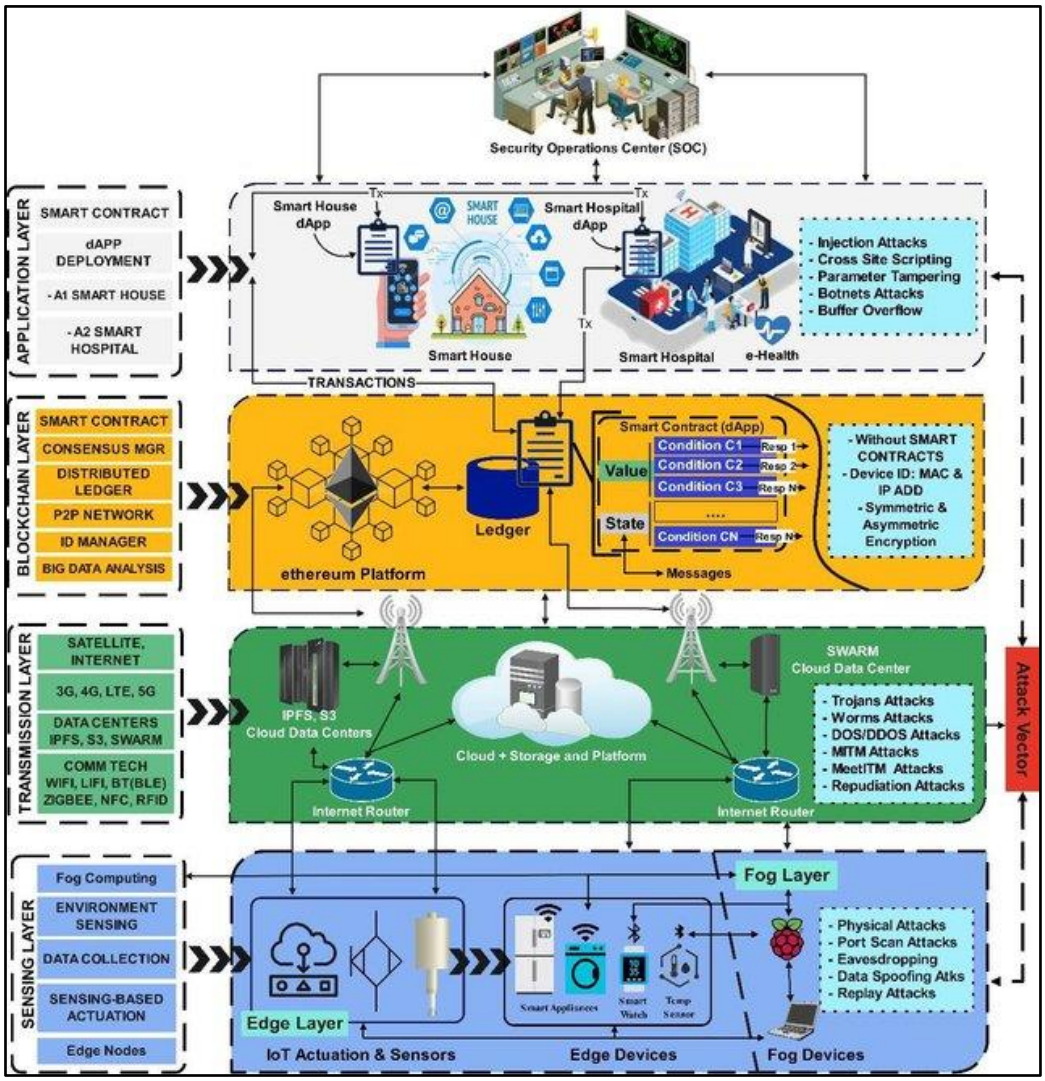

Figure 18: Blockchain-based smart city architecture (Hussain et al., 2021)

3.30 Importance of Blockchain Technology in Smart Cities

The use of blockchain technology in smart cities offers several advantages in terms of security, including:

- Decentralized data storage, reducing the risk of data breaches and cyberattacks

- Improved transparency, as all transactions and data are recorded on a secure and public ledger
- Enhanced security of sensitive information, as data is encrypted and stored across multiple nodes
- Increased accountability, as all transactions and decisions are recorded on the blockchain, making it easier to detect and prevent fraud and corruption (Buterin, 2014).

Therefore, the integration of blockchain technology into smart cities can provide a more secure and transparent environment, improving the overall functioning and efficiency of urban services.

3.30.1 Differences between Smart Cities with and without Blockchain Technology

Smart cities that use blockchain technology are more secure and transparent than those that do not, as blockchain technology eliminates the need for a central authority, providing a decentralized and secure platform for data storage and management. In addition, blockchain technology provides a secure and transparent record of all transactions and decisions, reducing the risk of fraud and corruption. (Swan, 2015).

On the other hand, smart cities that do not use blockchain technology often have a centralized architecture, where a single entity controls the data and decision-making processes. This increases the risk of data breaches and cyberattacks, and makes it easier for fraud and corruption to occur, as there is no secure and transparent record of transactions and decisions.

Real World Applications:

A prime example of real-world applications is the successful integration of blockchain technology into smart city infrastructure. Taipei City’s use of blockchain for secure and transparent voting (Kshetri, Nir. 2018), and Moscow’s implementation of a blockchain platform for city services and municipal finance (Louka, 2019).

Taipei City's implementation of blockchain technology for secure and transparent voting is a noteworthy example of how blockchain can enhance governance in smart cities. The use of blockchain technology in the voting process helps ensure that it is tamper-proof, secure, and transparent. With the blockchain, votes can be recorded and managed in real time, making results accurate and easily auditable. Another example is Moscow’s implementation of a blockchain platform for city services and municipal finance, which showcases the potential of blockchain technology to improve the efficiency and transparency of city services (Kshetri, Nir. 2018). (Louka, 2019). By implementing a blockchain-based platform, Moscow can more effectively manage city services, such as public transportation, and provide its citizens with more transparency and security in managing the city's finances. These real-world examples demonstrate the great potential of blockchain technology to enhance urban services and governance.

Challenges and Limitations:

Although blockchain technology offers many advantages in smart cities, there are also major challenges that need to be taken into account. A major challenge is the lack of standardization in this area, which makes it difficult for cities to compare and adopt solutions from different vendors (Kshetri, Nir. 2018). There may also be a lack of

technical expertise in the public sector, as well as scalability and performance issues in blockchain networks (Shao, 2015).

Future possibilities

The integration of blockchain technology into smart cities is an evolving field with great potential for future growth. The combination of other advanced technologies, such as artificial intelligence and the Internet of Things, has the potential to greatly enhance smart cities and provide greater benefits to citizens (Shao, 2015). For example, the integration of smart contracts and decentralized applications with IoT devices can provide real-time data on city services and infrastructure, leading to more efficient and effective city management ((Kshetri, Nir. 2018).

3.31 Smart city applications:

One of the most prominent examples of smart city applications is parking applications Parking management is a crucial aspect of smart cities, aiming to optimize parking space utilization and alleviate traffic congestion. Smart parking systems leverage advanced technologies such as sensors, Internet of Things (IoT), and data analytics to provide real-time information on parking availability and enable efficient parking space allocation (Seneviratne, Seneviratne, & Han, 2019). For example, in Barcelona, Spain, the city implemented a smart parking system that uses sensors embedded in parking spots to detect occupancy and relay the information to a centralized platform, allowing drivers to find available parking spaces quickly and reducing the time spent searching for parking (Borrego, Carbajal, & Pueyo, 2020). By integrating these technologies, smart parking solutions improve the overall efficiency of transportation systems, enhance user experience, and contribute to the development of sustainable urban environments.

In addition to optimizing parking space utilization, smart parking systems offer benefits in terms of traffic reduction and environmental impact. By providing real-time information on parking availability, drivers can locate parking spaces more efficiently, reducing the time spent searching for parking and thus minimizing traffic congestion (Li, Liu, Wang, & Wang, 2020). For instance, in San Francisco, the SFpark program implemented a smart parking system that dynamically adjusted parking prices based on demand, encouraging drivers to park in underutilized areas and reducing traffic congestion in popular areas (Shoup, 2018). This streamlined parking process leads to a decrease in carbon emissions and supports sustainable transportation initiatives in smart cities.

Efficient parking management in smart cities also relies on the integration of digital payment systems. By enabling seamless payment processes through mobile applications or connected platforms, smart parking systems eliminate the need for physical tickets or cash transactions (Seneviratne et al. 2019). For example, in Singapore, the Parking.sg mobile application allows users to pay for parking digitally, eliminating the need for physical parking coupons and reducing the hassle of payment (Gupta, 2019). This not only enhances user convenience but also promotes a cashless society and supports the overall digital transformation in urban environments.

smart parking systems play a significant role in the development of smart cities. By leveraging technologies such as sensors, IoT, Blockchain, data analytics, and digital payment systems, these solutions optimize parking space utilization, reduce traffic congestion, and enhance overall transportation efficiency.

3.32 Description of the Ramallah Smart City project

According to what was announced on the Ramallah Municipality website (Ramallah Municipality, n.d.), the Ramallah Smart City project came to fulfill the aspirations of the business sectors and citizens to ensure a sustainable city environment capable of competition through partnership with the private and government sectors, and targets six axes. They are as follows: technological infrastructure, smart governance, smart education, smart economy, smart mobility, and smart environment, and by 2018 all Ramallah municipality services will suppose to be electronic.

3.33 Overview of Ramallah Smart city infrastructure and services

According to the document published on the Ramallah Municipality website (Resilient Ramallah 2050), titled "Ramallah Resilience Strategy 2050," the city of Ramallah seeks to establish a fast and reliable communications and information technology infrastructure for the city of Ramallah and its villages. Achieving this goal will depend on multiple communication options through partnership with Companies and telecommunications providers in expanding the free Wi-Fi network, as well as the third generation network, as well as installing high-speed optical fibers in all areas in order to ensure the provision of highly efficient and effective services such as health care, municipal services, and others that would support economic prosperity in the city and raise its Participation among community members and providing rapid response.

And according to what was announced by the city of Ramallah in the aforementioned document The Ramallah Smart City Project aims to improve communication and service delivery to the local community, as well as gather feedback through remote data gathering tools. The initiative will expand to include mapping and promoting cultural assets, collecting data on public space usage patterns, and establishing a social platform for

sharing experiences. This action is expected to enhance community engagement, increase accessibility to city assets, and support resilience through innovative use of resources. This is what the plan referred to in the mentioned document (ACTION 36) of the plan.

The Ramallah Smart City project aims to implement an integrated approach to critical infrastructure development in order to address the needs of the whole system, rather than individual utilities. This initial step includes establishing a formal forum where critical infrastructure providers can collaborate to share information, identify vulnerabilities, and explore opportunities for efficiencies. This will involve clear information sharing protocols to ensure the security of sensitive data and will draw on existing mapping work done as part of the Ramallah Smart City project. By leveraging information sharing, Ramallah can optimize the use of its limited resources while identifying vulnerabilities, such as cascading consequences where the failure of one system has flow-on effects for others. The Ramallah Municipality will lead the delivery of this action, in collaboration with utility providers, the Ministry of Telecommunication and IT, the Ministry of Public Works and Housing, and the Ministry of Transport. If successful within the governorate, the program could be scaled up on a national level.

3.34 Ramallah Smart City challenges and opportunities

According to the plan published on the website of the city of Ramallah, which bears the name "Resilience of Ramallah 2050", one of the most prominent challenges facing the city is the occupation, and that the city's communication with the rest of the Palestinian cities takes through areas and roads under Israeli control, and therefore it is difficult to organize them, which causes Sometimes traffic congestion as well as hinders commercial transportation operations, as well as the limited energy purchased by the Jerusalem Electricity Company, which supplies the city of Ramallah with electricity 95% of the

energy from the Israeli Electricity Company and 5% from Jordan, in addition to the limited use of water and the presence of restrictions from the Israeli side On the provision of new water wells to benefit from groundwater, as well as the existence of a lost opportunity to recycle waste or exploit it in energy production, but it is disposed of in a designated waste dump, in addition to that, the limited areas classified as belonging to the Palestinian Authority in Ramallah governorate lead to an increase in Population density in some areas of the city.

Perhaps all of these challenges create new opportunities for the smart city of Ramallah, as it provides a sustainable environment and is based on a system of collecting and analyzing data and information for all sectors, which gives it the opportunity to overcome challenges and create a smart transportation system that reduces traffic congestion and organizes commercial transport operations, as well as working on Optimal management in distributing energy consumption and reducing its waste, as well as rationalizing water consumption, managing waste and controlling population growth.

3.35 Opportunities for blockchain adoption in Ramallah Smart City

According to the document titled Resilient Ramallah 2050, the data storage and exchange mechanism, the technology that Ramallah Smart City will use in saving, transferring, and processing data, and the protocols that it will use, have not been specified. What it called in the forum, and this is what gives this study importance in highlighting the importance of using Blockchain technology in the process of securing, preserving and processing data and information for the smart city of Ramallah.

Blockchain technology has the potential to present many opportunities for adoption in smart cities, including improving data security, transparency, and accountability in

various sectors such as finance, transportation, and energy management. Integration of the blockchain into Ramallah Smart City can enhance the efficiency of operations, reduce costs and reduce fraud, thus enhancing trust in the public sector (Crosby, Pattanayak, Verma & Kalyanaraman, 2016). Blockchain can also facilitate the creation of decentralized applications that can provide public services in a more secure, efficient, and transparent manner (Swan, 2015). The technology can be used to develop digital identity management systems, where citizens control their personal data, which enhances privacy and security (Kshetri, 2018). Moreover, blockchain can enable peer-to-peer energy trading in micro-grids, promoting the use of renewable energy sources and reducing carbon emissions (Scott, Motamedi & Shaeffer, 2018). These examples demonstrate the potential for blockchain to contribute to the development of the Ramallah Smart City so that it is smarter and more sustainable, improving the quality of life for citizens and creating economic opportunities (Liang, Zhao, Shetty & Liu, 2018).

3.36 Some challenges of smart cities

Many cities around the world face the challenge of traffic congestion and parking space scarcity. This necessitates drivers to spend additional time searching for available parking spots, leading to decreased public satisfaction and increased fuel consumption. As a result, transportation costs rise for citizens, and pollution rates escalate due to increased carbon emissions. Furthermore, local authorities must allocate additional funds for law enforcement and monitoring, such as the Ramallah governorate police conducting campaigns against illegal vehicles and combating theft, including vehicle theft.

Urban transportation systems in smart cities must solve the problems brought on by the increasing number of automobiles, and parking lots play a critical part in this. Smart parking lots are created to maximize parking space use, lessen traffic, and improve the

effectiveness of urban transportation as a whole. In order to give drivers simple access to real-time information regarding parking availability, smart parking systems use a variety of technologies, including sensors, data analytics, and mobile applications, according to research by (Smith et al. 2019).

In this study, we present a smart parking (Ramallah Smart Parking - RSP) proposal in the smart city of Ramallah that operates on the Blockchain network with the aim of contributing to reducing traffic congestion in the smart city of Ramallah, as well as contributing to reducing pollution resulting from the resulting carbon emissions. From fuel combustion while drivers are searching for a vacant parking lot to park, and thus the proposed car park contributes to combating the spread of illegal vehicles and contributes to combating car theft through direct communication with the Palestinian Ministry of Transportation and the Ramallah Governorate Police Also identify the vehicles required by the police.

3.37 Ramallah Smart Parking - RSP

The Ramallah Smart Parking - RSP system consists of an application based on blockchain technology that works on devices(mobile) and websites(desktop). Users can search for vacant parking spaces in real time, reserve the required parking lot. And pay through the application. RSP requires that each parking lot is equipped with sensors that operate on IoT network and the Blockchain network. These devices take a picture of the vehicle's registration plate that will occupy the parking lot and a picture of the driver and then work to compare the vehicle registration plate numbers with the records of the Ministry of Transport to verify whether the vehicle is legal or not. In case it is illegal. The system sends a notification to the police in the smart city of Ramallah about the presence of an illegal vehicle, specifying the location of the parking lot inside it and a copy of the vehicle

and the driver photo (See Figure 19). The vehicle registration plate is also compared with the police records to verify the vehicle if it is required by the police. In the event that it is, the police will be notified of the location Its presence, as well as if the vehicle has been moved from its place, the system notifies the user who made the reservation if he or his knowledge has moved the vehicle in the event that his answer is, the system does not immediately inform the police of the vehicle's theft with sending all other details such as the location of the parking lot in which the vehicle is located And the registration plate number, a picture of it, and a picture of the face of the one who drove it… etc. (See Figure 20).

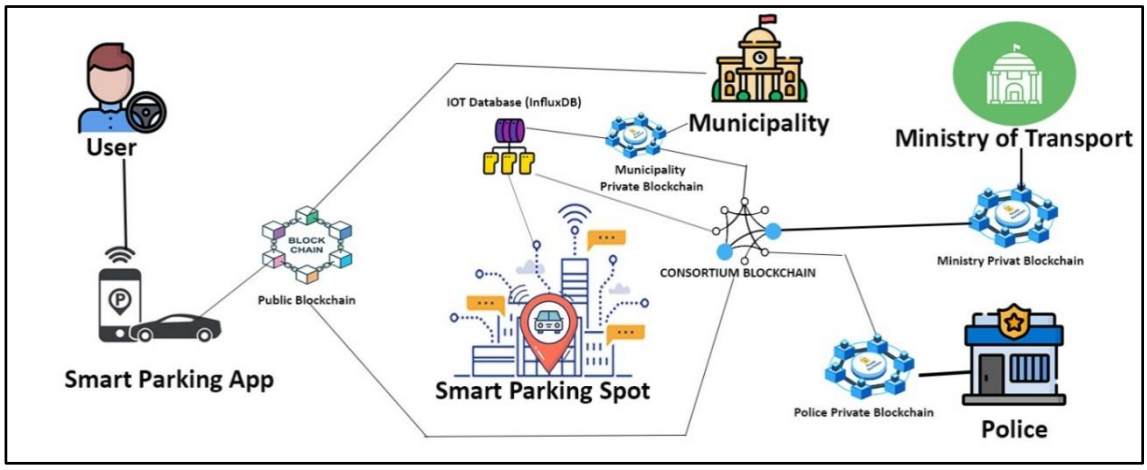

Figure 19: Ramallah Smart Parking -RSP.

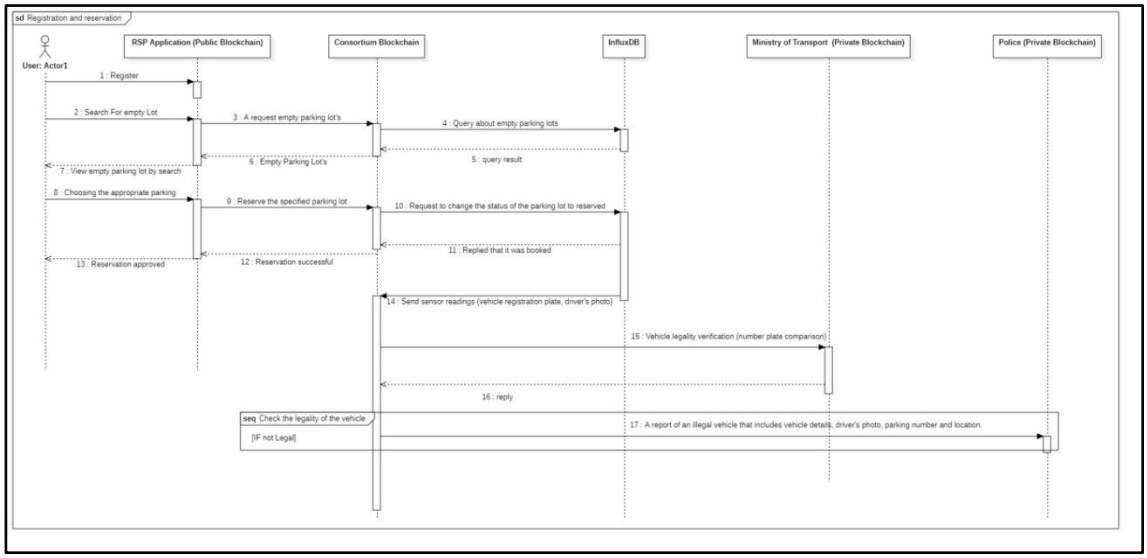

Figure 20: Sequence diagram showing the registration process in the RSP system, search and reservation processes, empty parking, the system checks the legality of the vehicle and informs the police if the vehicle is illegal

3.37.1 Ramallah Smart Parking – RSP techniques:

Blockchain Type:

The proposed RSP system is based on more than one party, such as the user, the Ramallah municipality, the Ministry of Transport, the police, and the Internet of Things. Thus, the most appropriate approach is to use the Consortium Blockchain to enhance privacy and security, improve scalability, and increase efficiency in governance and decision-making processes. Consortium blockchains allow smart city stakeholders to control data visibility and protect sensitive information (Khan, Salah, & Javed, 2019). The consortium model ensures that only trusted entities have access to the blockchain network and thus reduce the risk of unauthorized data access or tampering. Smart cities generate vast amounts of data from various sources, such as sensors, devices, and infrastructure. Consortium blockchains offer improved scalability, enabling higher transaction throughput and faster data processing (Bano et al., 2018). Smart cities generate vast amounts of data from various sources, such as sensors, devices, and infrastructure. Consortium blockchains offer improved scalability, enabling higher transaction throughput and faster data

processing (Bano et al. 2018). By reducing the number of participants compared to public blockchains, consortium blockchains can handle larger volumes of data and support the growing needs of smart city applications.

In addition, a public Blockchain Network was used to record user data on the RSP system, and this type of Blockchain network was used for the Ramallah Municipality to record parking lots, their locations, and their data on the RSP system, and to benefit from them also in displaying vacant parking lots.

The Privat Blockchain Network was used by the Palestinian Police as well as the Palestinian Ministry of Transportation to control the data and information that it includes in its own systems and that it wants to share with the RSP system, in addition to the use of the Privat Blockchain Network by Ramallah Smart City Municipality in communicating with the Internet of Things InfluxDB database that was proposed Using it in the RSP system regarding parking spaces without prior reservation. See Figure 21.

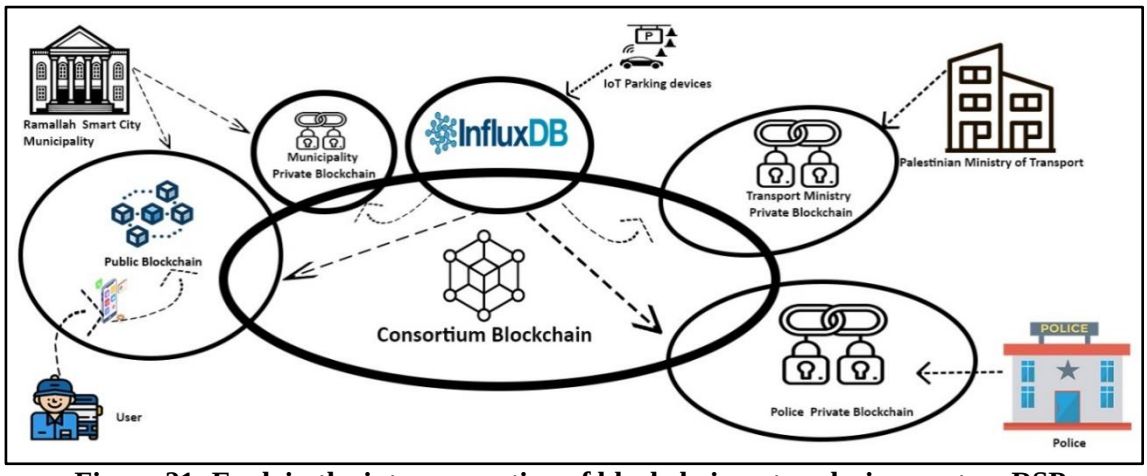

Figure 21: Explain the interconnection of blockchain networks in a system RSP.

3.38 Linking Consortium Blockchain and InfluxDB:

The integration of a consortium blockchain with InfluxDB can provide a powerful solution for managing and analyzing data in a secure and decentralized manner. Consortium blockchains offer a trusted and shared infrastructure among consortium

members, while InfluxDB specializes in efficient time-series data storage and retrieval. By linking these two technologies, smart city applications can leverage the benefits of both systems. Here's an explanation of how the consortium blockchain can be linked with InfluxDB:

3.39 Data Authentication and Immutability

The consortium blockchain can be utilized to ensure data authentication and immutability. The blockchain serves as a distributed and tamper-resistant ledger where transactions related to data storage and retrieval in InfluxDB can be recorded (Chatterjee et al. 2018). By storing cryptographic hashes or references to data on the blockchain, the integrity of the data stored in InfluxDB can be verified and proven, enhancing trust and data reliability.

3.39.1 Access Control and Data Sharing:

Consortium blockchains enable fine-grained access control and secure data sharing among consortium members (Dorri et al. 2019). By integrating InfluxDB with the consortium blockchain, access policies and permissions can be managed on the blockchain layer. Consortium members can define and enforce access rules, ensuring that only authorized entities can interact with specific data stored in InfluxDB. This strengthens data privacy and confidentiality in smart city environments.

3.39.2 Auditability and Compliance:

The integration of InfluxDB with the consortium blockchain enables enhanced auditability and compliance capabilities. Transactions recorded on the blockchain can include metadata about data storage, retrieval, and modifications in InfluxDB (Zheng et al. 2020). This provides an auditable trail of actions taken on the data, facilitating

regulatory compliance and accountability in smart city deployments. Consortium members can easily track and verify the history of data operations performed on InfluxDB using the transparent and immutable nature of the blockchain.

3.40 Linking Consortium Blockchain and Public Blockchain

On the user side and the Ramallah Municipality in the Ramallah Smart Parking System RSP, the application for the system was designed on Public Blockchain and linked to the consortium blockchain network with the aim of benefiting from the advantages and strengths of both types of Blockchain and benefiting from them in strengthening the system, Consortium blockchains, characterized by their private and permissioned nature, offer advantages such as enhanced privacy, scalability, and control over network governance. On the other hand, public blockchains provide transparency, immutability, and a decentralized network of participants. Linking these two types of blockchains enables secure and trusted data sharing, interoperability between different blockchain ecosystems, and the potential for innovative applications in smart cities (Estrada-Jiménez et al., 2021; Vazirani & Vazirani, 2020).

Connecting consortiums and public blockchains offers a promising approach to enhance data privacy, transparency and collaboration in smart cities. By merging these two types of blockchains, the system can take advantage of each other's strengths, creating a secure and interoperable environment. (Estrada-Jiménez et al., 2021; Vazirani & Vazirani, 2020).

Note that in many previous experiments, this approach has proven successful in integrating Public Blockchain and consortium blockchain, including, for example, the implementation of blockchain-based solutions for vehicle registration and management.

For instance, in Dubai, the Roads and Transport Authority (RTA) has collaborated with a consortium of stakeholders, including vehicle manufacturers, insurance companies, and government entities, to develop a blockchain platform called "Dubai Smart Vehicle Upkeep." This platform utilizes a consortium blockchain to securely store and share vehicle information, including ownership records, maintenance history, and insurance details. By linking this consortium blockchain with a public blockchain, the platform enables seamless and transparent access to vehicle data, facilitating efficient vehicle registration processes and enhancing trust among stakeholders (Zhang et al., 2021).

Another example is the use of consortium and public blockchains in facilitating secure and decentralized ridesharing services. The use of blockchain technology in ridesharing platforms allows for the creation of peer-to-peer networks, eliminating the need for intermediaries and reducing transaction costs. For instance, DOVU, a blockchain-based mobility platform, aims to connect transportation providers and users through a consortium blockchain. By linking this consortium blockchain with a public blockchain, DOVU enables transparent and secure data sharing, ensuring the integrity of transaction records, and facilitating seamless payments for ridesharing services (Nguyen et al., 2019).

3.40.1 Linking Consortium Blockchain and Private Blockchain:

The Ramallah Smart Parking System (RSP) is based on two types of blockchain technology where the Palestinian Police and the Palestinian Ministry of Transport have their own Private Blockchain network and then they are linked with the Ramallah Smart City via a consortium blockchain. The aim is to take advantage of the advantages offered by these types of blockchain technology. Typically, a consortium blockchain is more open than a private blockchain, and allows for a greater degree of interoperability. This makes them well suited for use in applications that require collaboration between multiple

organizations and in smart cities. The benefits obtained from linking the consortium blockchain and the Private Blockchain include improved scalability, increased transparency, enhanced data privacy, and reduced costs. The consortium blockchain allows secure sharing of data and collaborative decision-making between multiple organizations, while the private blockchain ensures strict access control and data confidentiality within a single organization. This hybrid approach allows organizations to strike a balance between transparency and privacy, making it easier to share information effectively and securely.

Also proposed to use Private Blockchain by the Ramallah Municipality in the RSP system to provide a greater opportunity for the Smart Ramallah Municipality to expand or link the different sectors with each other to reach the Smart City of Ramallah.

3.40.2 Ramallah Smart Parking – RSP Analysis:

The RSP system consists of the following Actors and operation:

- User (Driver).
- Parking Spot.
- Ramallah Smart City municipality.
- Police of Ramallah Smart City.
- Palestinian Ministry of Transport.

See the Use Case Diagram for Driver User in Figure 22.

User (Driver):

- Register.
- Add vehicle’s details.
- Search for Available Lot’s.

- Reservation Lot’s.
- Payment.
- Active with the Lot’s Sensors (Detection and notifications).

Register:

Users are divided into two types, the first type is the regular user (drivers), and the second user is the Smart Ramallah Municipality (Administrator).

User (Driver):

The new user (Driver) creates an account on the RSP system program based on the blockchain, where, upon registration for the first time, he enters the required basic data (name, username, password, date of birth, ID number, copy of the driver's license, personal photo, personal ID photo After completing the registration process, an encrypted smart contract is created that contains all the user's data, so that each user has a unique account that is accessed using his own login name and password to ensure that his data is not used by anyone else, as the Ethereum Blockchain network was used in The account creation process is based on the Solidity language, where in the following example, user data is encrypted on the Ethereum Blockchain network with the AES encryption algorithm.

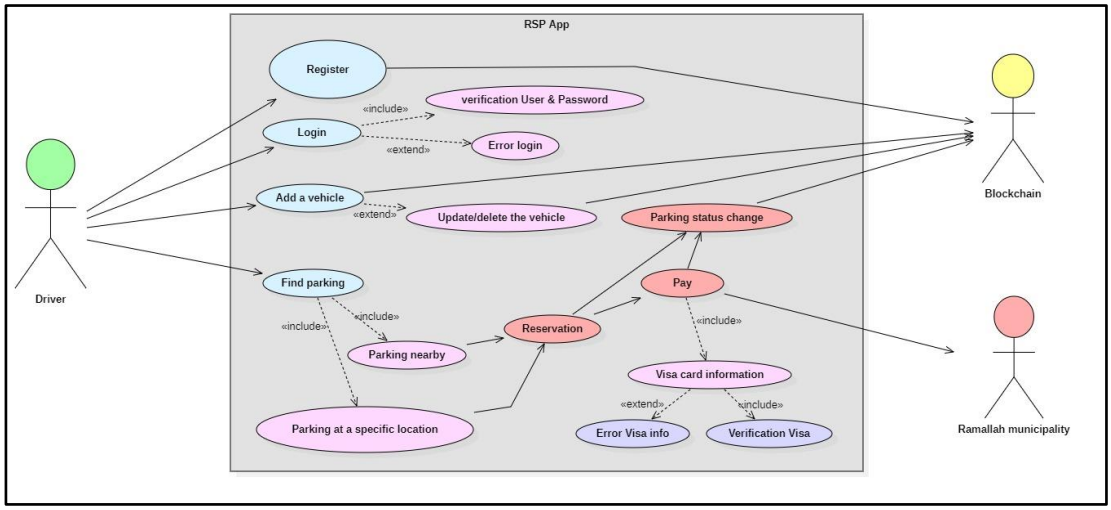

Figure 22: Use Case Diagram for Driver User

Parking Spot:

Ramallah municipality parking lots, which are spread in various places, as well as parking lots on the sides of the roads. As it is equipped with motion sensors and cameras dedicated to taking a picture of the car, the number plate, and a picture of the driver, as it works on the IOT system, and after taking the readings of the sensors and cameras, it is stored on the Internet of Things database, which is proposed in this study, the InfluxDB database, where this type of database was chosen IoT data because of its characteristics, including that it provides high scalability, allowing efficient storage and processing of large amounts of time-stamped data points generated by IoT devices (Bhattacharya et al. 2017). InfluxDB also prioritizes high throughput and low latency, enabling real-time ingestion and querying of IoT data (Arroyo-Fernández et al., 2020). It supports flexible data models, including the ability to handle structured and unstructured data, and facilitates the storage and analysis of diverse IoT data formats (Voss et al., 2018). Moreover, InfluxDB includes built-in functions for data compression and aggregation, reducing storage requirements and improving query performance (Kravets et al., 2016). These features make InfluxDB a suitable choice for managing and analyzing large amounts of IoT time series data. As the result of the processing process is shared on the blockchain

network for readings and comparisons in the event that there are readings and confirmation from the user about the theft of his vehicle, or it was the result of comparing the vehicle registration number with the records of the Palestinian Ministry of Transport as a vehicle not included in its records (unlicensed), license expired, or The vehicle registration plate numbers were included in the police records and a search was required for them, or a vehicle was parked in the parking lot without making reservations about it so that the rest of the system can complete its task in communicating with the rest of the competent parties of the system such as the police to report illegal vehicles or vehicles whose license is expired or required Searching for it, as well as contacting the Ramallah Municipality to report a vehicle occupying a parking lot without making a reservation.

Ramallah Smart City municipality:

The role of the Ramallah Municipality in the RSP system is to include the data of all the parking lots belonging to it in terms of the parking number and its geographical location, and to receive financial transfers from users (drivers) in return for using the parking lots and to respond to sensor readings in the parking lot about the presence of a vehicle in a specific parking lot without any action reservation process.

Police of Ramallah Smart City:

The role of the police in the smart city of Ramallah is through sharing some records of vehicles to be searched for or tracked, as well as responding to RSP system reports of illegal and expired vehicles and vehicle theft reports.

Palestinian Ministry of Transport:

Interacting with the smart parking system by answering the inquiries submitted through the system about vehicle registration plate numbers and providing the system with the results if the vehicle is legal or otherwise.

Related Work:

Blockchain technology has the potential to revolutionize various aspects of smart city infrastructure, including parking management. Here are a few examples of smart city parking projects that leverage blockchain technology:

1. Parksen (PARQ): Parksen is a parking solution built on the blockchain that promises to enhance city parking administration. It makes use of a mix of IoT sensors, mobile applications, and blockchain smart contracts. The sensors identify occupied parking spaces and transmit the information to the blockchain, which changes the state of availability in real-time. Users who have the Parksen mobile app at their disposal may quickly locate parking spots by using this data. Parking transaction records are transparent, secure, and unalterable thanks to the usage of blockchain technology (Parksen, n.d.).
2. Share&Charge: A blockchain-based technology called Share&Charge enables peer-to-peer (P2P) parking spot sharing. The technology uses blockchain smart contracts to protect and simplify the parking space renting process. Drivers may search for and reserve parking spots using a smartphone app, while parking space owners can publish their available spaces on the site. Without the need of middlemen, the blockchain provides safe and open transactions between the participants (Share&Charge, n.d.).

3. Ubitquity: Ubitquity is a blockchain-based parking spot management and ownership platform. It produces tamper-proof records of parking spot ownership, transfers, and rental agreements using blockchain technology. The system offers a visible and immutable record that interested parties, including parking spot owners, renters, and municipal governments, may access. Ubitquity seeks to improve trust, decrease conflicts, and expedite parking spot administration by utilizing blockchain (Ubitquity, n.d.).

See Table 14 for a comparative analysis of parking systems in smart cities (Related Work), highlighting their respective strengths and weaknesses:

Table 3.14: A comparison of parking systems in smart cities (Related Work) in terms of strengths and weaknesses

No	Parking System	Strengths	Weaknesses
1.	Parksen (PARQ)	- Utilizes IoT sensors, mobile applications, and blockchain smart contracts to enhance city parking administration. - Real-time identification of occupied parking spaces using IoT sensors, enabling users to locate available parking spots quickly. - Transparent, secure, and unalterable parking transaction records thanks to blockchain technology.	Requires extensive sensor infrastructure deployment, which can be costly and time-consuming.
2.	Share&Charge	- Enables peer-to-peer (P2P) parking spot sharing through blockchain technology. - Simplifies and secures the parking space renting process with blockchain smart contracts. - Facilitates direct and safe transactions between participants without the need for intermediaries.	Adoption barriers may exist, requiring a critical mass of users for optimal utilization.

No	Parking System	Strengths	Weaknesses
3.	Ubitquity	- Generates tamper-proof records of parking spot ownership, transfers, and rental agreements using blockchain technology. - Provides a visible and immutable record of parking spot administration for interested parties. - Improves trust, decreases conflicts, and expedites parking spot management through the use of blockchain.	Potential complexities related to scalability and interoperability with existing parking systems due to reliance on blockchain.

3.41 The gap between RSP System and related works:

Previous research has primarily focused on delivering services to the public in smart cities. This includes real-time identification of available parking spaces, enabling drivers to reserve parking spots, facilitating smart contracts with parking owners, and maintaining immutable records of parking space ownership, transfers, and rental agreements. With transparency and safety and ensuring that records are not tampered with.

Previous experiments aimed at providing effective services for smart cities, but did not fully explore the possibility of using these systems to enhance security, combat illegal vehicles, and prevent vehicle theft. This highlights the importance of this study as it focuses on the importance of optimal use of the parking system in Ramallah Smart City to improve security and effectively address these challenges.

3.42 City Infrastructure and Transportation Challenges

Ramallah City suffers from serious transportation infrastructure problems, such as congested roads, scarcity of public transportation, and lack of parking spaces. The city's

inadequate transportation systems are the result of a lack of investment in transportation infrastructure, political unpredictability, and a lack of resources. Ad hoc solutions have been implemented in the absence of a comprehensive transportation plan, which makes it difficult for city residents to get around (Palestinian Central Bureau of Statistics, 2020).

Ramallah Smart City's technology and communications infrastructure are essential to advancing its smart projects and facilitating effective connectivity and data management. To enable the adoption of smart technologies and services, the city would need reliable networks, fast internet access, and cutting-edge communication systems (Abdelfattah, 2019).

Ramallah would require the development of a robust communications infrastructure, including the installation of fiber-optic networks, to support the smart city ambitions. In order to facilitate smooth communication and data transmission across the city, fiber-optic cables offer high-speed and dependable internet access (Palestinian Telecommunication Group - PALTEL, 2020).

Ramallah Smart City would include wireless communication technologies in addition to fiber-optic networks to guarantee ubiquitous connection. This would entail the installation of cellular networks and Wi-Fi hotspots to enable the smooth operation of smart devices and apps while also giving locals, companies, and visitors convenient access to the internet (Palestinian Telecommunication Group - PALTEL, 2020).

Ramallah would set up a variety of sensors and Internet of Things (IoT) devices to facilitate the collecting and analysis of real-time data for smart city services. These gadgets would be installed at key locations across the city to monitor many aspects, including trash management, air quality, and traffic flow. For processing and analysis, the

gathered data would be sent over the communication infrastructure to centralized data management systems (Abdelfattah, 2019).

the Ramallah's communications and technological infrastructure Strong networks, fast internet access, and cutting-edge communication technologies would all be part of a smart city. By enabling seamless connectivity and data transmission through the use of fiber-optic networks, wireless communication systems, and IoT devices, different smart city services could be implemented, and effective data management would be made possible.

3.43 Current Parking Management Systems in Ramallah

The current parking lots in the city of Ramallah are divided into two parts, a section belonging to the private sector and a section belonging to the municipality of Ramallah, where the section belonging to the private sector consists of land owners and places that can be used to park vehicles for a sum of money, in addition to renting a company for parking lots on the city's roadsides (TecPark). As for the parking lots of the Ramallah municipality, for Al-Manara Complex parking lot.

Al-Manara Complex parking:

as it is a parking lot It consists of 450 lot's and contains that contains sensors that calculate the number of occupied parking spaces and calculate the number of empty parking spaces (see Figure 23) and display them on more than one screen for drivers (see Figure 24), as well as entering the aforementioned building through Cut a ticket from the device that contains a QR code (see Figure 25). Upon departure, the driver puts the QR code on the designated machine, so that it shows him the amount to be paid (see Figure 26). After payment, he can scan the QR code on the gate to open (see Figure 27) so that he can exit

after the system confirms that he has paid the required fees (Ramallah Municipality. (n.d.). Ramallah, 2023).

Figure 23: Sensors that calculate the number of occupied / empty parking spaces.

Figure 24: Screen showing the number of occupied and empty parking spaces.

Figure 25: The entry ticket contains the time and date of entry in order to use it upon exit to calculate the period and the amount required for that.

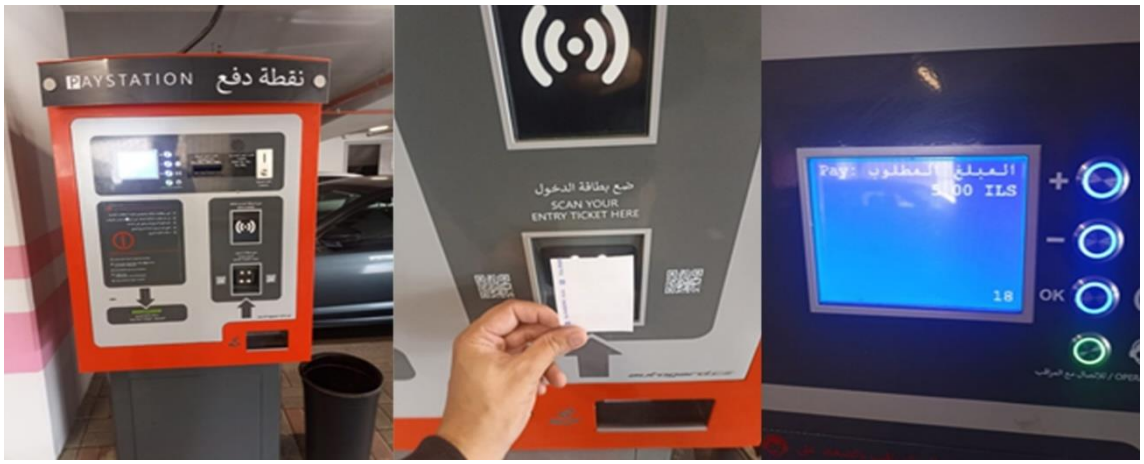

Figure 26: PayStation

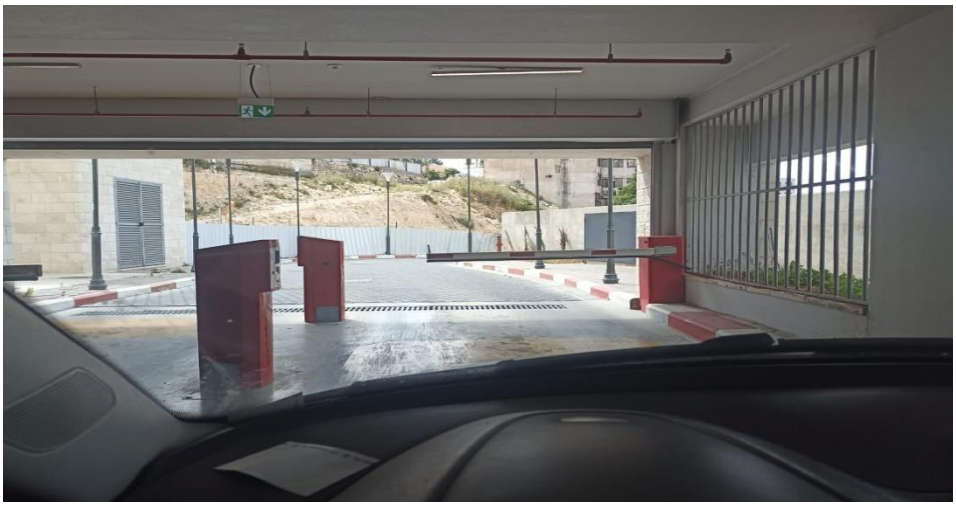

Figure 27: One of Al Manara complex main gates

TecPark:

TecPark company manages prepaid car parks in Ramallah Streets, where the company sets prepaid counters when parking the car, and the company's employees work in the field to review all the counters and make sure that the vehicle owner has paid in advance and also checks that the time that has been booked has not expired, and in Once the time expires, the field employees of the company will restrict the vehicle in exchange for fining the vehicle owner an amount of money to release it (see figure 28). In order to achieve flexibility, the company has launched an application called TecPark through which the user can insert the registration plate number of his vehicle and then charge an amount of money in the application and pay the amount according to the time he wishes to book and five minutes before the end of the time, the application will alert the user if he wishes to extend the time. As the database of the application is a central (traditional) database, and it may be exposed to security risks that central databases are exposed to, in addition to that, the company can manipulate user balances or calculate the actual timing of parking reservations. (See figure 29):

Figure 28: TecPark prepaid car parking machine

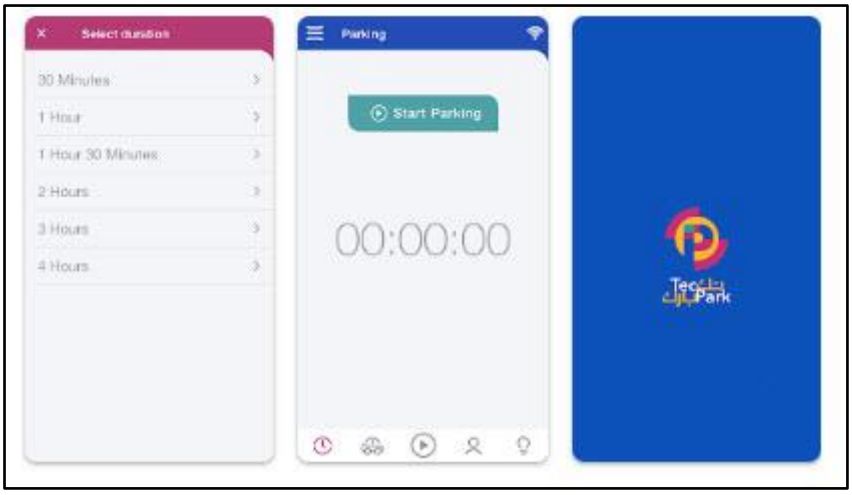

Figure 29: TecPark App

3.44 A comparison between the current parking system of Ramallah smart city (Al Manara complex) and TecPark and RSA System:

Al Manara complex technologies are limited to a building, and this makes the Ramallah municipality unable to manage the parking lots on the roadsides in a smart way commensurate with a smart city. If there is a vacant parking lot or not, this does not contribute to reducing the traffic crisis, as well as has no effect on reducing pollution resulting from carbon emissions as a result of fuel combustion while searching for a parking space for the vehicle, because the screens are located in the city center and around the Al Manara complex building, and there is no phone application that can Through it, the driver checks for a vacant parking lot, in addition to that, the driver is required to pay cash through pay station, which sometimes generates a crisis when exiting Al Manara complex.

Although TecPark tries to find flexible ways to provide parking services to users by introducing the TecPark application, it does not specify empty parking spaces in the application, but the application is limited to reservations and payment for empty parking spaces found during searches in Streets. This does not contribute to reducing traffic congestion on the roads, or to reducing the level of carbon emission pollution, or

contributing to enhancing the level of security in combating illegal vehicles, or reducing vehicle theft crimes, in addition, it uses a central database, and this type of database is exposed to many security risks.

The Ramallah Smart Parking system (RSP) proposed in this study provides an opportunity for the smart Ramallah Municipality to exploit all types of parking spaces, whether inside buildings or on roadsides, in addition to having high flexibility through which the driver can check whether there is a vacant parking space for the vehicle or not. No, as well as he can reserve the parking lot even before reaching it and pay through the application, and this achieves greater flexibility in addition to contributing to reducing traffic crises in the streets while searching for a vacant parking space for the vehicle in addition to reducing carbon pollution in addition to reducing transportation costs as it reduces fuel combustion as a result of the decrease in the crisis In addition, the proposed smart parking system contributes to law enforcement operations by combating illegal vehicles and combating stolen vehicles, as well as identifying required vehicles, and this would enhance the security system in the smart city of Ramallah and achieve a high level of response.

3.45 Security Measures and Integration with Law Enforcement:

The RSP system worked to enhance security and assist law enforcement agencies in the smart city of Ramallah by contributing to the detection of illegal and expired vehicles and vehicles used by people wanted by the police or required to be kept or followed up by informing the police of the location and details of the vehicle in addition to Data and photos of the person who uses them, in addition to contributing to detecting the exploitation of parking lots without reservation and preventing evasion from using parking lots without paying the usage commission and informing the Ramallah

Municipality about them to take the necessary measures with the violators, in addition to documenting the system with full evidence of all the violations mentioned. And so that RSP system was played an effective role in raising the level of security in Ramallah smart city. See the comparison between Al Manara Complex, TecPark and RSA System in table 3.15:

Table 3.15: Comparison between Al Manara Complex, TecPark and RSA System

No.	Comparison Criteria	Al Manara Complex	TecPark	RSA System
1.	**Scope of Technology**	Limited to buildings	Limited to streets	All types of parking spaces
2.	**Flexibility**	Limited	Limited	High flexibility through mobile app
3.	**Reservation and Payment**	Limited	Available	Available through the app
4.	**Impact on Traffic and Pollution**	Limited	Limited	Reduces traffic and carbon emissions
5.	**Integration with Law Enforcement**	Limited contribution	Limited contribution	Enhances security and law enforcement
6.	**Security and Evidence Documentation**	Limited	Limited	Provides evidence of violations
7.	**Overall Effectiveness**	Limited	Limited	Effective in raising security levels

3.46 Challenges facing the study

1. Limited adoption of fiber and third-generation networks in Ramallah smart city: The city of Ramallah has not yet adopted a fiber network or the third-generation network for use in parking management.
2. Incomplete Wi-Fi coverage: The Wi-Fi network of Ramallah Smart City does not cover all areas of the city, which may limit the effectiveness and reach of a smart parking system that depends on connectivity.

3. High cost of third-generation network usage: The cost associated with using the third-generation network in Palestine is high, which may impact the feasibility and affordability of implementing a parking management system RSP.
4. Requirement for official approvals and coordination: The to implement RSP system proposal necessitates approval and coordination from official bodies such as the Ramallah municipality, the Palestinian police, and the Palestinian Ministry of Transport. Obtaining these approvals and establishing coordination can be time-consuming and challenging.
5. Budgetary constraints for implementing blockchain networks and IoT devices: The implementation of the study proposal requires an adequate budget for providing blockchain networks and Internet of Things (IoT) devices. Securing funding and resources for these technologies may pose a challenge.
6. Limited research on blockchain technology in Palestine: There is a scarcity of relevant research related to the use of blockchain technology in Palestine, including the city of Ramallah. This may limit the availability of existing knowledge and best practices to inform the thesis research.
7. Lack of awareness among citizens: Not all citizens of Ramallah are aware of the benefits offered by blockchain technology. Educating citizens about the importance and advantages of this technology is necessary to encourage their adoption and use in a parking management system.
8. Unavailability of Israeli vehicle registration records: The Palestinian Authority does not possess the Israeli vehicle registration records used by Visitors to the city who hold Israeli citizenship.

3.46.1 Evaluation and Performance Analysis:

Despite the tireless efforts made by the city of Ramallah to transform into a smart city through the development of infrastructure and the extension of fiber optic networks and the third generation network, the infrastructure of the city at the present time needs more development, and this is one of the most prominent challenges that the study faces in applying the system Ramallah Smart Parking RSP, including the failure of the Ramallah Municipality until now to adopt a fiber-optic network for parking lots, as well as the high cost of using the third generation network, as well as the implementation of the proposed system at the present time needs more time, which can be applied in the future as it needs many approvals from the parties The system (Ramallah Municipality, the Palestinian Police, the Palestinian Ministry of Transport), which the study aspires for is that the proposed system be adopted by the competent official authorities and provide the necessary approvals and funding for its implementation. Accordingly, the study relied on studying similar experiences in other smart cities around the world and benefiting from Its experiences, as well as a study of the current parking of vehicles in the city of Ramallah and showing its shortcomings. Accordingly, the study presented the Ramallah Smart Parking System (RSP) as a solution to the shortcomings in the current systems used and an effective contribution to the development of the transportation sector in the smart city of Ramallah.

Based on these challenges, the study relied on proposing a comprehensive system that addresses the deficiencies in the systems used in smart cities around the world and the systems currently used in managing the parking lots of the city of Ramallah by presenting and analyzing the proposed Ramallah Smart Parking System (RSP) completely, and it

relied on evaluating its effectiveness Through the effectiveness of systems that have been applied and studied in other smart cities around the world.

3.46.2 Evaluating the performance of Ramallah smart parking RSP:

The performance of the proposed system for the smart parking of Ramallah (RSP) was evaluated by asking questions that included the strengths and weaknesses of the parking systems used in smart cities around the world and the current systems used in managing parking lots in the city of Ramallah to verify the actual results achieved by the proposed system RSP see table 3.16:

Table 3.16: Evaluating the performance of parking lots used in smart cities around the world and the current systems for managing parking lots in the city of Ramallah and the proposed RSP system.

	RSP	Parksen (PARQ)	Share&Charge	Ubitquity	Manara Complex parking	TecPark
Does it achieve user satisfaction?	✓	✓	✓	✓	X	X
Does it contribute to reducing traffic congestion?	✓	✓	✓	✓	X	X
Does it contribute to reducing pollution?	✓	✓	✓	✓	X	X
Does it contribute to raising the security level of the city?	✓	X	X	X	X	X
Is it expandable?	✓	✓	✓	✓	X	✓
Is the database secure?	✓	✓	✓	✓	X	X

User satisfaction:

RSP, Parksen (PARQ), Share & Charge, and Ubitquity vehicle parking systems have achieved user satisfaction, as the user can book or locate empty parking spaces without the need to go and search for them directly on the ground, thus reducing the effort that he needs to make.

While Manara Complex parking and TecPark are currently used in managing parking lots in the city of Ramallah, the user must go in his vehicle to search for an empty parking lot, and this requires him to make an effort to obtain it, and he may be stuck in the traffic crisis in the streets of Ramallah during the search.

Reducing the traffic crisis:

RSP, Parksen (PARQ), Share & Charge, and Ubitquity parking lots contributed to reducing the traffic crisis because the user got the empty parking spot before heading to it, and therefore he does not need additional time to walk his vehicle in search of an empty parking lot, and thus contributes to reducing the traffic crisis in the city streets.

While Manara Complex parking and TecPark contribute to increasing the traffic crisis in the streets because the user requires him to go in his vehicle to search for an empty parking lot.

Contribute to reducing pollution:

RSP, Parksen (PARQ), Share &C harge, and Ubitquity parking lots Contribute to reducing pollution since the user does not need to go in his vehicle to search for parking spaces as the empty parking lots are known to him.

While the parking lots of Al-Manara Complex and TecPark contribute to the increase in corona pollution resulting from the emission of vehicle fuel combustion while searching for parking spaces, since the user is asked to go with his vehicle to search for an empty parking space.

Contribute to raising the security level of the city:

The proposed system contributes to raising the security level of the city by contributing to reducing the use of illegal and expired vehicles, as well as contributing to reducing

vehicle theft crimes and contributing to limiting the use of parking spaces without reservation.

Parksen (PARQ), Share&Charge, Ubitquity, Al-Manara Complex parking and TecPark These systems have no significant role in enhancing the security level of the city.

Expandability:

RSP, Parksen (PARQ), Share&Charge, Ubitquity and TecPark can be expanded as it is not confined to a specific building or place and can be expanded with the increase in the number of parking spaces and the expansion of technology and communication infrastructure in the city, blockchain systems and the IoT.

While Al-Manara Complex cannot be expanded, as it is confined to a specific place and has a specific number of 450 parking spaces, as announced by the city of Ramallah.

Secure Databases:

RSP, Parksen (PARQ), Share & Charge and Ubitquity use distributed databases such as blockchain and are less vulnerable to the security risks of centralized databases such as those used by the TecPark system and Al-Manara Complex.

4 Chapter 4: SMO algorithm Experimental work

4.1 Overview

In this chapter, we will do a practical experiment in building blocks, validating them, discovering malicious blocks from them, and adding them to the blockchain using the SMO hybrid consensus algorithm proposed by the study, and then taking the results and comparing them with the Proof-of-Activity algorithm, as it is similar in some stages to the SMO algorithm except The last algorithm proposed by us has an additional layer of protection, and then review the results to verify the efficiency and effectiveness of the proposed algorithm SMO.

4.2 Create Blocks

We built a virtual block using the same Blockchain blocks architecture as following:

block = {

'hash': '',

'ver': ,

'prev_block': ' ',

'mrkl_root': '',

'time': ,

'bits': ,

'nonce': ,

'n_tx': ,

'size': ,

'block_index': ,

'height': ,

'received_time': ,

'relayed_by': ' ',

'tx': [{'sender': ' ', 'receiver': ' ', 'amount': , 'timestamp': }, {'sender': ' ', 'receiver': ' ', 'amount': , 'timestamp': }, {'sender': ' ', 'receiver': ' ', 'amount': , 'timestamp': }, {'sender': ' ', 'receiver': ' ', 'amount': , 'timestamp': }, {'sender': ' ', 'receiver': ' ', 'amount': , 'timestamp': }, {'sender': ' ', 'receiver': ' ', 'amount': , 'timestamp': }, {'sender': ' ', 'receiver': ' ', 'amount': , 'timestamp': }, {'sender': ' ', 'receiver': ' ', 'amount': , 'timestamp': }, {'sender': ' ', 'receiver': ' ', 'amount': , 'timestamp': }, {'sender': ' ', 'receiver': ' ', 'amount': , 'timestamp': }],

}

4.3 Verification of blocks

In this chapter, virtual blocks were generated due to the lack of available sources providing Datasets of block structures. Consequently, we established two sets of virtual blockchains. The first set, known as the training set, comprises 10,000 blocks, while the second set, the testing set, consists of 2,000 outlier blocks differing significantly in their primary characteristics from those in the training set, such as ('Hash', 'ver', 'time', 'bits', 'nonce', 'n_tx', 'size').

These blocks undergo practical experimentation in the Block Bank phase of the proposed SMO algorithm. Various machine learning algorithms, including Random Forests Algorithm, K-means algorithm, Hidden Markov Models (HMMs), and Isolation Forest anomaly detection, will be applied. These blocks are assumed to be potential candidates for inclusion in the blockchain network, after which the results will be analyzed.

The work was conducted on the Jupyter platform (https://jupyter.org/), a tool facilitating software implementation using the Python language, specifically tailored for machine learning and data analysis purposes.

4.3.1 Random Forests ML Algorithm experiment:

In this experiment was conducted on two sets of blocks (the training set and the test set), which were then subjected to the Random Forests ML algorithm to detect outlier blocks,

where the outlier blocks would be considered malicious blocks. The training set consists of 10,000 blocks, while the test set consists of 2,000 outliers Blocks that differ significantly in their main characteristics from the training set. After running the experiment, the Random Forests algorithm successfully identified 411 outlier blocks in: 0.04700016975402832 seconds, indicating that the time taken to test each block was 0.000114355644170385206812652 65206812652 seconds and the accuracy is 20.55%. See Appendix 2 and figure 30:

```
Number of Blocks Trained on : 10000
Number of Blocks Tested on : 2000
---------------------------------
Training Time: 1.1214923858642578 seconds
Testing Time: 0.029593944549560547 seconds
Number of malicious Blocks Detected: 411
```

Figure 30: Experiment verifying virtual blocks with Random Forests ML Algorithm.

From the experiment, we conclude that the Random Forests machine learning algorithm was able to identify 20.55% of the outlier blocks in record time. This finding can be leveraged for early detection of malicious blocks, preemptively excluding them from advancing to the subsequent verification stage through consensus algorithms PoS. This leads to conserving computational resources that would otherwise be consumed and enhances the security level of the blockchain network.

4.3.2 K-means algorithm ML algorithm experiment:

In this experiment was performed using the same two sets of blocks (training set and test set) that were used in the previous experiment. They were then subjected to the K-means ML algorithm in order to detect outgroups. The training set consists of 10,000 blocks, while the test set consists of 2,000 outlier blocks that differ significantly in their main properties from the training set and these blocks, we consider to be malicious blocks.

After running the experiment, the K-means algorithm successfully identified 503 outlier blocks within 0.0039997100830078125 seconds, indicating that the time taken to test each block was 0.00000199985504150390625 seconds and the accuracy is 25.15%. See Appendix 4 figure 31:

```
K-means algorithm

Number of Blocks Trained on : 10000
Number of Blocks Tested on : 2000
---------------------------------
Number of malicious Blocks Detected: 503
Training Time: 0.17500019073486328 seconds
Testing Time: 0.0039997100830078125 seconds
```

Figure 31: K-means algorithm experiment

From the experiment, we conclude that the K-means algorithm ML algorithm was able to identify 25.15% of the outlier blocks in record time. This finding can be leveraged for early detection of malicious blocks, preemptively excluding them from advancing to subsequent verification stages. Consequently, this leads to conserving computational resources and enhancing the security level of the blockchain network

4.3.3 Hidden Markov Models (HMMs) ML algorithm experiment:

In this experiment was conducted using the same two sets of blocks (the training set and the testing set) that were utilized in the previous experiments. They were then subjected to the Hidden Markov Models (HMMs) ML algorithm in order to detect outlier blocks. The training set consists of 10,000 blocks, while the testing set comprises 2,000 outlier blocks that differ significantly in their key properties from the training set. After conducting the experiment, the Hidden Markov Models (HMMs) algorithm successfully identified 411 outlier blocks within 0.07860255241394043 seconds, indicating that the

time taken to test each block was 0.000191247086165305182481751824817 52 seconds and the accuracy is 20.55%. See appendix 3 and figure 32:

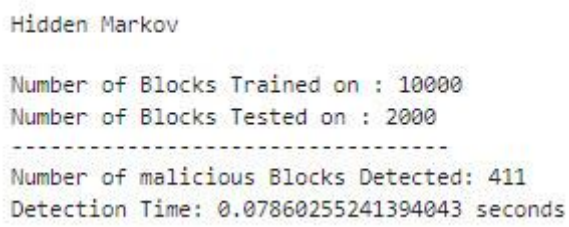

Figure 32: Hidden Markov Models (HMMs) experiment.

From the experiment, we conclude that Hidden Markov Models (HMMs) successfully identified 20.55% of the outlier blocks in record time. This outcome can be leveraged for early detection of malicious blocks, preemptively excluding them from advancing to subsequent verification stages. Consequently, this leads to conserving computational resources and enhancing the security level of the blockchain network.

4.3.4 Isolation Forest anomaly detection ML algorithm experiment:

In this experiment was conducted using the same two sets of blocks (the training set and the testing set) that were utilized in the previous experiments. They were then subjected to both the Hidden Markov Models (HMMs) ML algorithm and the Isolation Forest anomaly detection ML algorithm to detect outlier blocks. The training set consists of 10,000 blocks, while the testing set comprises 2,000 outlier blocks that differ significantly in their key properties from the training set. After conducting the experiment, the Isolation Forest anomaly detection ML algorithm successfully identified 1971 outlier blocks within 0.5279998779296875seconds and the accuracy is 98.55%., indicating that the time taken to test each block was 0.00026399993896484375 seconds. See appendix 5 and figure 33:

```
Isolation Forest

Number of Blocks Trained on : 10000
Number of Blocks Tested on : 2000
---------------------------------
Number of malicious Blocks Detected: 1971
Detection Time: 0.5279998779296875 seconds
```

Figure 33: Isolation Forest anomaly detection ML algorithm experiment.

From the experiment, we conclude that the Isolation Forest anomaly detection ML algorithm successfully identified 98.55% of the outlier blocks in record time. This outcome can be leveraged for early detection of malicious blocks, preemptively excluding them from advancing to subsequent verification stages. Consequently, this leads to conserving computational resources and enhancing the security level of the blockchain network.

4.4 Analysis of the results

In the four previous experiments, two sets of blocks were used: one for training consisting of 10,000 blocks, and the other for testing comprising 2,000 blocks differing significantly in key features from the training blocks. The Random Forests algorithm was able to detect only 20.55% of the outlier blocks within 0.04700016975402832 seconds, with each block taking 0.000114355644170385206812652 seconds to examine.

In the second experiment, the K-means algorithm ML algorithm identified 25.15% of the outlier blocks within 0.0039997100830078125 seconds, with each block taking 0.0000019998550415039062 5 seconds to examine.

In the third experiment, Hidden Markov Models (HMMs) ML algorithm successfully detected 20.55% of the outlier blocks within 0.07860255241394043 seconds, with each block taking 0.000191247086165305182481751824817 52 seconds to examine.

In the fourth experiment, Isolation Forest anomaly detection ML algorithm recognized 98.55% of the outlier blocks within 0.5279998779296875 seconds, with each block taking 0.00026399993896484375 seconds to examine. See Table:

Table 4.1: Summary of experimental results using machine learning algorithms

No	Algorithm	Malicious Blocks Detected	accuracy %
1.	Random Forests	411	20.55%
2.	K-means algorithm	503	25.15%
3.	Hidden Markov	411	20.55%
4.	Isolation Forest	1971	98.55%

4.5 Performance and effectiveness evaluation:

Based on the previous experiments, we observe that the Isolation Forest algorithm exhibited excellent performance in detecting anomalous blocks compared to the other algorithms. It managed to detect 1971 anomalous blocks out of 2000. On the other hand, the K-means algorithm also showed good performance in detecting 503 anomalous blocks, while the Random Forests ML Algorithm and Hidden Markov demonstrated similar results, each detecting 411 anomalous blocks.

To assess the efficacy of the proposed SMO algorithm in utilizing machine learning algorithms such as Random Forests, K-means, Hidden Markov Models (HMMs), and anomaly detection algorithms, we adopt the criterion of evaluating the highest time spent in experiments for each algorithm, which corresponds to the time required for analyzing and classifying individual blocks.

Under both hypotheses, we assume a fixed examination time of 0.00026399993896484375 for a single block, representing the longest time recorded during block analysis.

The first hypothesis involves sequential implementation of tests by the machine learning algorithms.

The second hypothesis posits simultaneous implementation of the machine learning algorithms. Here, we consider the previously recorded longest time as the standard duration required for identifying and classifying a single block.

Consequently, under these assumptions, we determine that the proposed SMO algorithm can analyze and classify approximately 227250 blocks per minute. This calculation is derived from the following equations:

The time required for one transaction is 0.00026399993896484375 seconds.

Number of Blocks per second = 1 / 0.00026399993896484375 ≈ 3787.5

To determine the number of blocks tested per minute (60 seconds):

3787.5* 60 = 227250

In conclusion, the additional protective layer (Block bank) offered by the SMO algorithm enables the analysis and classification of approximately 227250 blocks per minute, facilitating early detection of malicious blocks.

4.6 Hybrid Algorithm SMO strength point

Depending on the mechanism of action of the proposed SMO hybrid consensus algorithm, many of its strengths can be identified, including:

When creating the chain, the energy consumption is higher than the energy consumption after the growth of the chain, since Block Banck is empty at the beginning of creating the chain, and then malicious blocks that are identified are added in the verification and decision stage.

- The higher the number of malicious blocks detected by the system, the lower the energy consumption, as the malicious block is recognized by machine learning algorithms, and this means that no energy is consumed in the verification and decision stage through the application of the PoS consensus algorithm.
- The level of decentralization has been increased, since machine learning algorithms detect malicious blocks before they are presented to the next stage, which is verified for their validity by the PoS consensus algorithm, which takes into account the size of the stake owned by validators (voters) and reduces the negative effects of the PoS algorithm.
- The security level of the Blockchain network has been increased, as an additional protection layer (Block Banck) has been added that works to identify malicious blocks before subjecting them to the PoS consensus algorithm to verify the validity of the block.
- The SMO hybrid algorithm is encouraging for auditors as it reduces the consumption of their resources in the process of verifying malicious blocks and that with the growth of the chain the algorithm is able to subject the higher percentage of valid blocks to auditing, in addition to that it constitutes an opportunity for auditors to exploit their resources to audit blocks and get rewards for it That and the fact that the largest percentage of the blocks are valid blocks, this increases their chances of making profits.
- The SMO Hybrid Consensus Algorithm achieves high security because the block passes five tests through different algorithms which are as follows Random Forests Algorithm, K-means algorithm, Hidden Markov Models (HMMs),

Anomaly detection algorithms and Proof-of-Stake algorithm based on ALGORAND protocol.

- The SMO Hybrid Consensus Algorithm achieves speed at work because the Proof of Stake algorithm based on the ALGORAND protocol verifies 875 transactions per second, which is equivalent to 52500 transactions per minute, and the additional layer Block Bank can early detect malicious blocks by filtering them through Analyze and classify 227250 blocks per minute.
- The SMO hybrid algorithm achieves energy efficiency, as it is more energy efficient than traditional PoW algorithms. It also reduces the computational power required to validate a block by leveraging a PoS component and machine learning algorithms. This makes it a greener alternative, as it reduces the environmental impact associated with high energy consumption.
- The SMO Hybrid Consensus Algorithm works on Sybil Attack Resistance, where the attacker creates multiple fake identities to gain control of the network. By requiring participants to prove their computational work through PoW, SMO makes it more difficult for attackers to create a large number of identities because the SMO algorithm introduces an additional layer of protection that uses machine learning algorithms to identify and detect malicious blocks through Signature Analysis, Transaction Analysis, Behavior Analysis, and Network Analysis, and in the event of failure to discover it, it is subject to scrutiny by the Proof-of-Stake algorithm based on ALGORAND protocol, and this raises the level of security and raises the costs for the attacker while trying to create different identities.
- SMO Hybrid Consensus Algorithm is an ideal solution for Denial of Service (DoS) attacks as it can preemptively detect malicious blocks while attackers

attempt to flood the chain into blocks in order to generate performance congestion and block access to the network, as early and fast detection of malicious blocks prevents a DoS attack.

- The SMO hybrid consensus algorithm reduces short range attacks because the work on checking and discovering the block is not only done by auditors, but preceded by machine learning algorithms, as at the beginning of creating the chain, the percentage of success of this type of attack may be higher, but it starts to decrease with the size of the malicious blocks detected and stored in the Block Bank.
- The SMO hybrid consensus algorithm prevents the chances of success of long-range attacks, in which the attacker intends to obtain the largest possible amount of digital currencies in order to choose him as an auditor, as this type of attack was bypassed by first relying on machine learning algorithms and secondly through Proof -of-Stake algorithm based of ALGORAND protocol, where the auditors who audited in a dishonest or harmful way are severely punished such as losing part of their share.
- The SMO hybrid consensus algorithm fulfills the basic requirements required to be met in Ramallah Smart Parking system (RSP) in a manner commensurate with the needs of the city of Ramallah in terms of providing security for the system, scalability, low energy consumption, achieving efficiency and decentralization.

4.7 Weaknesses of the consensus algorithm SMO

1. Despite the energy-saving benefits of the SMO consensus algorithm during the auditing process through early detection of malicious blocks using machine learning algorithms, it should be noted that block creation is accomplished through the Proof-of-Work algorithm, potentially resulting in high energy consumption during block creation.
2. The potential danger lies in the early stages of chain formation, especially if a significant number of malicious blocks are injected, and collusion occurs among auditors in the third stage, where they re-audit blocks using the Proof-of-Stake consensus algorithm, categorizing malicious blocks as valid ones. Consequently, from the perspective of the SMO consensus algorithm, valid blocks can be misconstrued as malicious, as they differ from malicious blocks added to the chain after auditor approval. This occurs because, in this stage, the distributed ledger in the additional protection layer known as Block Bank is empty, making auditors the primary factor in enhancing security.

5 Chapter 5: Conclusion

5.1 Introduction

This thesis presented a case study for the application of blockchain technology in the smart city of Ramallah in Palestine. A new consensus bearing the name SMO that stands for a hybrid algorithm that combines the Proof-of-Work consensus algorithm and the Proof-of-Stack consensus algorithm. In addition, SMO includes an additional protection layer called Block Bank that contains a distributed ledger composed of malicious blockchain blocks that were discovered by the system. Furthermore, SMO contains Four machine learning algorithms namely, Random Forests, K-means, Hidden Markov Models, and Anomaly Detection. These machine leaning algorithms contribute to early detection of malicious blocks and raise the level of security of the blockchain network. The proposed hybrid SMO algorithm was subjected to tests and the result shows it is capable of testing and analyzing 227250 blocks per minute as well as an early detection of malicious blocks , this distinguishes it as a more effective algorithm, as the experiments carried out by researchers on other consensus algorithms did not reach these results as the proposed hybrid algorithm SMO, as the PoW consensus algorithm can verify 6 to 8 blocks per minute on a network that contains 1000 blocks according to (Caglar, Kapadia, & Kapadia, 2019). According to the experiments conducted by (Kiayias, Russell, David, & Zindros, 2019), it was found that the PoS consensus algorithm was able to verify 10 to 14 blocks per minute. Also, the Delegated PoS (DPoS) consensus algorithm verifies 20 to 40 blocks per minute in a blockchain chain of 10,000 nodes, according to (Kontorovich, Singh, & Zohar, 2020). He also reached the results of experiments conducted by Ali on the Proof-of-consensus algorithm Authority (PoA) that it was able to verify 60 to 180 blocks per minute in the 1000-node blockchain, and it was also found that the Proof-of-

Activity consensus algorithm was able to verify 100 to 300 blocks per minute on the 1000-node network.

In this thesis, the blockchain technology was proposed to transform the transportation sector in the smart city of Ramallah from a traditional sector to a smart sector. The security of the city and the reduction of environmental pollution resulting from fuel combustion in vehicles and the reduction of traffic congestion.

5.2 Practical Results

The study found that using Artificial Intelligence with Blockchain and IoT technology can turn traditional sectors like transportation in Ramallah into smart sectors. This enhances sustainability, aligns with citizen needs, and utilizes existing ICT infrastructure effectively for building a smarter Ramallah.

The study presented a new consensus algorithm SMO, which proved the results of the experiments obtained with its ability to early detection and raise the level of security of the blockchain technology while ensuring efficiency in implementation, as it was able to audit 227250 blocks per minute and contribute to the early detection of malicious blocks.

The study contributed to presenting a proposal that contributes to transforming the transportation sector in the city of Ramallah from its traditional form to a smart transportation sector that works to reduce traffic congestion in the city and contributes to reducing the effects of environmental pollution resulting from fuel combustion emissions in vehicles and an effective contribution to raising the level of security in the city Smart Ramallah by combating the phenomenon of illegal or expired vehicles and combating theft of vehicles from parking lots, as well as contributing to determining the locations of

vehicles that the police are searching for or their owners when using any of the parking lots of Ramallah.

5.3 Suggestions for future research

- We highly encourage local researchers to address and explore blockchain technology in Palestine.
- We highly suggest the need to study the various basic sectors in the city of Ramallah and contribute to transforming them from their traditional form into smart sectors.
- We highly suggest that the current study be projected on the rest of the Palestinian cities and explore ways to transform them into smart cities.
- We highly suggest that researchers explore artificial intelligence technology to raise the level of security in blockchain technology.

References

"Advantages of Smart Cities." Smart Cities Dive, 10 Oct. 2018, www.smartcitiesdive.com/ex/

"Smart Cities and the Internet of Things (IoT)." Accenture, www.accenture.com/us-en/insights/high-performance-business/iot/smart-cities-and-internet-of-things.

"Smart Cities Characteristics." Smart Cities Council, smartcitiescouncil.com/article/smart-cities-characteristics.

"Smart Cities." IBM, IBM, www.ibm.com/smarterplanet/us/en/smart-cities/overview/.

A. E. Kontorovich, A. K. Singh, and A. Zohar. "On the security and performance of delegated proof-of-stake blockchains." In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, pages 1351-1368. ACM, 2020.

A. Kiayias, A. Russell, B. David, and A. Zindros. "Ouroboros praos: An adaptively-secure, permissionless proof-of-stake blockchain." In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pages 1400-1420. ACM, 2019.

Abdelfattah, Y. (2019). Smart Cities Infrastructure: An Integrated Approach. In R. Zhang, G. Fortino, and H. Li (Eds.), Internet of Things. IoT Infrastructures (pp. 121-143). Springer. doi: 10.1007/978-3-030-22058-5_5

Aburidi, A. (2022). "Blockchain Technology for Reshaping Stock Exchanges: A qualitative exploratory study in Palestine." Arab Economic and Business Journal, 14(1), Article 6. doi: 10.38039/2214-4625.1008.

AbuSamra, A., Elbatsh, K., & Hassan, A. (2020). "Gaza Wallet: A Simple and Efficient Blockchain Application." SSRN Electronic Journal. doi: 10.2139/ssrn.3660325.

Aggarwal, S., & Kumar, N. (2021). "Cryptographic Consensus Mechanisms." In *The Blockchain Technology for Secure and Smart Applications across Industry Verticals* (pp. 211-226). doi: 10.1016/bs.adcom.2020.08.011.

Albino, V., Berardi, U., & Dangelico, R. M. 2015, 'Smart cities: Definitions, dimensions, performance, and initiatives', Journal of Urban Technology, vol. 22, no. 1, pp. 3-21.

Alcarria, R., Fernandez, P., Lopez, D., & Roman, R. (2020). Blockchain technologies for smart cities: Recent advances and future prospects. IEEE Access, 8, 42075-42089.

aljazeera.(2017). aljazeera. Retrieved May 16, 2023, fromhttps://www.aljazeera.net/ebusiness/2017/12/10/تحذير-فلسطيني-من-التعامل-بالعملات

Allen, S., Čapkun, S., Eyal, I., Fanti, G., Ford, B., Grimmelmann, J., Juels, A., Kostiainen, K., Meiklejohn, S., Miller, A., Prasad, E., Wüst, K., & Zhang, F. (2020). Design Choices for Central Bank Digital Currency: Policy and Technical Considerations. https://doi.org/10.3386/w27634

Almomani, M. A., Almomani, O. A., Obeidat, R., & Abdullah, M. (2020). K-means clustering and naive Bayes classification for intrusion detection system. International Journal of Machine Learning and Computing, 10(3), 359-363.

Amodei, Dario, et al. "Concrete problems in AI safety." arXiv preprint arXiv:2112.06089 (2021).

Antonopoulos, A. M. (2014). Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, Inc.

Arizona State Legislature. (2017). Senate Bill 1084. Retrieved from https://www.azleg.gov/legtext/53leg/1R/bills/SB1084P.pdf.

Arroyo-Fernández, I., del Toro, J.M, Santamaría, I., & Díaz-González, J.P (2020). Performance comparison of time series databases for the Internet of Things. Probes, 20(14), 4010.

Asghari, S., & Navimipour, N. J. (2018). Resource discovery in the peer to peer networks using an inverted ant colony optimization algorithm. Peer-to-Peer Networking and Applications, 12(1), 129–142. https://doi.org/10.1007/s12083-018-0644-2

Ayuntamiento de Barcelona. (2020). Smart Parking Barcelona. Retrieved from https://ajuntament.barcelona.cat/smartspace/en/projectes/smart-parking-barcelona

Bagloee, S. A., Heshmati, M., Dia, H., Ghaderi, H., Pettit, C., & Asadi, M. 2021, 'Blockchain: The operating system of smart cities', Cities, vol. 112, 103104.

Bamakan, S.M.H., Motavali, A. and Babaei Bondarti, A. (2020) 'A survey of blockchain consensus algorithms performance evaluation criteria', Expert Systems with Applications, 154, p. 113385. doi:10.1016/j.eswa.2020.113385.

Bano, S., Zawoad, S., Rahman, M., & Hasan, R. (2018). The state of the art in blockchain technologies for IoT security. Journal of Information Security and Applications, 44, 10-27.

Bano, S., Zoha, A., Salah, K., & Ikram, M. A. (2018). The state of the art in blockchain technology and applications. Digital Communications and Networks, 4(3), 161-177.

Bashir, I. (2017). Mastering Blockchain. Packt Publishing Ltd.

Benslimane, Y., & Benamar, S. (2018). Towards blockchain-based secure and transparent sharing of IoT datasets. In Proceedings of the 3rd International Conference on Big Data and Internet of Things (BDIOT) (pp. 205-210).

Bentov, I. et al. (2014) 'Proof of Activity', ACM SIGMETRICS Performance Evaluation Review, 42(3), pp. 34–37. doi:10.1145/2695533.2695545.

Bhatia, A., Singh, S., & Singh, V. K. (2017). Application of Hidden Markov Model in Intrusion Detection. International Journal of Computer Applications, 174(42), 33-37.

Bhattacharya, M., Sahoo, J. K., & Patnaik, S. (2017). Time-series databases: A survey. Sadhana, 42(10), 1699-1724.

Bitcoin Core. (n.d.). Deterministic Wallet. Retrieved from https://en.bitcoin.it/wiki/Deterministic_wallet.

Bitcoin Core. (n.d.). Non-Deterministic Wallet. Retrieved from https://en.bitcoin.it/wiki/Non-deterministic_wallet.

Bitcoin Improvement Proposals. (2012). BIP 32: Hierarchical Deterministic Wallets. Retrieved from https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki.

Bitcoin Wiki. (2021). Transaction Pools. Retrieved from https://en.bitcoin.it/wiki/Transaction_pool

Bitcoin Wiki. (n.d.). Brain Wallet. Retrieved from https://en.bitcoin.it/wiki/Brainwallet.

Bitcoin Wiki. (n.d.). Paper Wallet. Retrieved from https://en.bitcoin.it/wiki/Paper_wallet.

Bitcoin.org. (n.d.). Choose your wallet. Retrieved from https://bitcoin.org/en/choose-your-wallet.

Böck, P., & Waidner, M. (2020). Challenges in the implementation of smart cities. In Proceedings of the 10th ACM Conference on Future Energy Systems (pp. 1-10). ACM.

Borrego, D., Carbajal, J. P., & Pueyo, Á. (2020). A smart parking system based on low-cost IoT technologies: A case study in Barcelona. Sensors, 20(3), 644.

Breiman, L. (2001). Random forests. Machine learning, 45(1), 5-32.

Buterin, V. (2013). Ethereum White Paper. Retrieved from https://ethereum.org/whitepaper/

Buterin, V. (2014). A next-generation smart contract and decentralized application platform.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. Ethereum White Paper, 1(1), 1-32.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. Ethereum White Paper, 1-32.

Buterin, V. 2014, A Next-Generation Smart Contract and Decentralized Application Platform, White Paper, vol. 3, no. 37, pp. 2-1.

Caragliu, A., Del Bo, C., & Nijkamp, P. (2011). Smart cities in Europe. Journal of urban technology, 18(2), 65-82.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues." Telematics and Informatics, 36, 55-81. doi: 10.1016/j.tele.2018.11.006.

Castro, M., & Liskov, B. (1999). Practical Byzantine Fault Tolerance. Proceedings of the Third Symposium on Operating System Design and Implementation (OSDI '99), 173-186.

Chandel, S., Cao, W., Sun, Z., Yang, J., Zhang, B., & Ni, T.-Y. (2019). A Multi-dimensional Adversary Analysis of RSA and ECC in Blockchain Encryption. Advances in Information and Communication, 988–1003. https://doi.org/10.1007/978-3-030-12385-7_67

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys (CSUR), 41(3), 1-58. doi:10.1145/1541880.1541882.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly Detection: A Survey. ACM Computing Surveys (CSUR), 41(3), 1-58.

Chatterjee, M., Deka, G., Pal, A., & Shandilya, V. (2018). Blockchain for internet of things: A systematic literature review. Journal of Grid Computing, 16(4), 595-614.

Chatterjee, S., Sarker, H., & Abdelzaher, T. (2018). Blockchain-based time-series data integrity for IoT applications. In 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC) (pp. 85-94). IEEE.

Chen, J., Li, Y., & Yang, W. (2017). Proof-of-Importance: A Personalized Consensus Protocol for Blockchain Networks. IEEE Access, 5, 8870-8879.

Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., & Shi, W. (2017). "On Security Analysis of Proof-of-Elapsed-Time (PoET)." In *Stabilization, Safety, and Security of Distributed Systems* (pp. 282-297). doi: 10.1007/978-3-319-69084-1_19.

Cho, H., Lee, S., & Nam, T. (2021). A comparative analysis of blockchain initiatives in smart cities: Case studies from Singapore, Dubai, and Estonia. Sustainability, 13(1), 97.

City and County of San Francisco. (2020). SFpark. Retrieved from https://www.sfpark.org/

Coeckelbergh, M. (2019). The Smart City and Its Publics: A Reply to De Lange and De Waal. Techné: Research in Philosophy and Technology, 23(3), 290-304.

Coinbase. (n.d.). Online Wallets. Retrieved from https://www.coinbase.com/wallet/online-wallets.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71-81.

CryptoRobin. (n.d.). What is Proof of Activity? Retrieved June 2, 2023, from https://cryptorobin.com/what-is-proof-of-activity/

D. Drescher, Blockchain Basics: A Non-Technical Introduction in 25 Steps. Apress, 2017.

Dang, H., Dinh, T. T. A., Loghin, D., Chang, E.-C., Lin, Q., & Ooi, B. C. (2019). Towards Scaling Blockchain Systems via Sharding. Proceedings of the 2019 International Conference on Management of Data. https://doi.org/10.1145/3299869.3319889

de Oliveira, M. T., Reis, L. H. A., Carrano, R. C., Seixas, F. L., Saade, D. C. M., Albuquerque, C. V., Fernandes, N. C., Olabarriaga, S. D., Medeiros, D. S. V., & Mattos, D. M. F. (2019). Towards a Blockchain-Based Secure Electronic Medical Record for Healthcare Applications. ICC 2019 - 2019 IEEE International Conference on Communications (ICC). https://doi.org/10.1109/icc.2019.8761307

Deng, L., Li, H., Yin, S., Wang, H., & Li, S. (2020). Effective Data Management in IoT Cloud Platforms: A Survey. Networking and Computer Applications Journal, 153, 102541.

Deng, Y., Zhang, C., Wu, H., Li, S., & Lv, L. (2020). The design and implementation of a multi-source time-series data storage and query system based on InfluxDB. Future Generation Computer Systems, 107, 404-414.

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling Blockchain: A Data Processing View of Blockchain Systems. IEEE Transactions on Knowledge and Data Engineering, 30(7), 1366–1385. https://doi.org/10.1109/tkde.2017.2781227

Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K.-L. (2017). BLOCKBENCH. Proceedings of the 2017 ACM International Conference on Management of Data. https://doi.org/10.1145/3035918.3064033

Dorri, A., Kanhere, S. S., & Jurdak, R. (2019). Blockchain in Internet of Things: Challenges and solutions. IEEE Internet of Things Journal, 6(2), 1-1.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2020). Blockchain in Internet of Things: Challenges and Solutions. IEEE Internet of Things Journal, 7(2), 453-463.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain: A Distributed Solution to Automotive Security and Privacy. IEEE Communications Magazine, 55(12), 119-125.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2019). BCNSecure: Blockchain-based secure and auditable data sharing with fine-grained access control in IoT. Journal of Network and Computer Applications, 135, 62-75.

Dorri, A., Steger, M., Kanhere, S. S., & Jurdak, R. 2017, 'Blockchain: A distributed solution to automotive security and privacy', IEEE Communications Magazine, vol. 55, no. 12, pp. 119-125.

Dubai Blockchain Strategy. (n.d.). Smart Dubai. Retrieved from https://www.smartdubai.ae/dubai_blockchain.php

Dubai Future Foundation. (2020). Dubai Blockchain Strategy 2020. Retrieved from https://dubaifuture.gov.ae/our-initiatives/blockchain-strategy/

E. Caglar, A. Kapadia, and A. Kapadia. "Performance evaluation of proof-of-work consensus algorithms for blockchain networks." In Proceedings of the 2019 ACM SIGMETRICS/IFIP Performance Evaluation Conference, pages 439-452. ACM, 2019.

Esposito, C., Ficco, M., & Gupta, B. B. (2021). Blockchain-based authentication and authorization for smart city applications. Information Processing & Management, 58(2), 102468. https://doi.org/10.1016/j.ipm.2020.102468

Estrada-Jiménez, J., Cardoso-Carrió, J. I., & Sánchez-Raya, M. (2021). Blockchain-Based Systems for Smart Cities: A Review. Sensors, 21(5), 1745. https://doi.org/10.3390/s21051745

Eyal, I., & Sirer, A. (2013). Bitcoin is Broken. Hacking, Distributed.

Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in blockchain system. Journal of Network and Computer Applications, 126, 45–58. https://doi.org/10.1016/j.jnca.2018.10.020

Gai, K., Wu, Y., Zhu, L., Qiu, M., & Shen, M. (2019). Privacy-Preserving Energy Trading Using Consortium Blockchain in Smart Grid. IEEE Transactions on Industrial Informatics, 15(6), 3548–3558. https://doi.org/10.1109/tii.2019.2893433

Gemeente Amsterdam. (2021). Parkeren op straat. Retrieved from https://www.amsterdam.nl/parkeren-verkeer/parkeren-amsterdam/parkeren-op-straat/

Google Research (n.d.) 'Colaboratory FAQ', Google Research. Available at: https://research.google.com/colaboratory/faq.html (Accessed: 07/07/2023).

Grigg, I. (2019). Bitcoin Custodianship: Levels, Models and Classification. Bifröst Journal of Social Science, 1(2), 13-26.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems, 29(7), 1645-1660.

Gupta, A. (2018). Blockchain for Smart Cities: A Systematic Literature Review. Journal of Grid Computing, 16(4), 607-624.

Gupta, S. (2019). Cashless parking app: A case study of parking.sg. Journal of Contemporary Urban Affairs, 3(2), 56-65.

H. Hussain, N. Javaid, W. Sun, Z. A. Khan, A. Imran and M. Ishfaq, "A Comparative Analysis on Blockchain Versus Centralized Authentication Architectures for IoT-Enabled Smart Devices in Smart Cities: A Comprehensive Review, Recent Advances, and Future Research Directions," in IEEE Access, vol. 9, pp. 52112-52132, 2021, doi: 10.1109/ACCESS.2021.3060817.

Hakak, S., Khan, W. Z., Gilkar, G. A., Imran, M., & Guizani, N. (2020). Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges. IEEE Network, 34(1), 8-14. [Online] Available at: https://doi.org/10.1109/MNET.001.1900178.

Hartigan, J. A., & Wong, M. A. (1979). Algorithm AS 136: A K-Means Clustering Algorithm. Journal of the Royal Statistical Society: Series C (Applied Statistics), 28(1), 100-108. doi:10.2307/2346830.

Hasanova, H., Baek, U., Shin, M., Cho, K., & Kim, M. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. International Journal of Network Management. Retrieved from https://nmlab.korea.ac.kr/publication/published.papers/2019/2019.01-Survey_on_Blockchain_Vulnerabilities-IJNM.Journal.pdf.

Heng, X., & Teo, J. (2018). Blockchain in Singapore: An overview. Journal of Business Research, 88, 360-365.

Ho, T. K. (1998). The random subspace method for constructing decision forests. IEEE transactions on pattern analysis and machine intelligence, 20(8), 832-844.

Hong, A., Kim, B., & Widener, M. 2020, 'Noise and the city: Leveraging crowdsourced big data to examine the spatio-temporal relationship between urban development and noise annoyance', Environment and Planning B: Urban Analytics and City Science, vol. 47, no. 7, pp. 1201-1218.

https://www.alhadath.ps/article/1
https://www.maannews.net/news/739389.html
I. Bashir, Mastering Blockchain. 35 Livery Street, Birmingham, B3 2PB, UK: Packt Publishing Ltd, 2017
Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. Harvard Business Review, 95(1), 118-127.
IBM n.d., Smart City, IBM Corporation, viewed 05/05/2023, Available at: https://www.ibm.com/topics/smart-city.
IBM. (n.d.). Austin and Blockchain. Retrieved from https://www.ibm.com/industries/government/solutions/city-blockchain-austin
InfluxData. (2021). InfluxDB: The Time Series Database. Retrieved from https://www.influxdata.com/time-series-database/
Jones, M. (2017). "Palestinians hope to launch e-currency in 5 years." Reuters.
K. Sharma and D. Jain, "Consensus Algorithms in Blockchain Technology: A Survey," *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2019, pp. 1-7, doi: 10.1109/ICCCNT45670.2019.8944509.
Kabir, S.E., Shahriar, R., Alam, M.M. and Khan, M.R. (2020). IoT-Based Smart Garbage Management System for Efficient Waste Collection. Smart Cities, 4(2), 264-283. https://doi.org/10.3390/smartcities4020024.
Kaur, S., Chaturvedi, S., Sharma, A., & Kar, J. (2021). A Research Survey on Applications of Consensus Protocols in Blockchain. Security and Communication Networks, 2021, 1–22. https://doi.org/10.1155/2021/6693731
Khan, M. A., Salah, K., & Javed, F. (2019). Blockchain-enabled privacy-preserving data sharing in smart cities. IEEE Transactions on Industrial Informatics, 15(6), 3268-3276.
Khan, N., Salah, K., & Javed, M. A. (2019). Consortium blockchain for secure energy trading in smart grid. Future Generation Computer Systems, 97, 297-307.
Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2018). Ouroboros: A provably secure proof-of-stake blockchain protocol.
King, S., & Nadal, S. (2012). PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake.
Kravets, A., Davidsson, P., & Palmieri, F. (2016). Compression techniques for Internet of Things data: A survey. Journal of Systems Architecture, 66, 23-37.
Kshetri, J. (2018). Smart City Development with Blockchain Technology. In Proceedings of the 2018 International Conference on Smart City Applications, pp. 45-50.
Kshetri, M. & Kumar, N. (2018). Blockchain Technology for Smart Cities. In Journal of Internet Services and Information Security, vol. 8, no. 2, pp. 35-40.
Kshetri, N. (2018). Can blockchain strengthen the internet of things? IT Professional, 20(4), 9-18.
Kshetri, N. (2019). Blockchain's potential in smart cities: An exploratory study. Telecommunications Policy, 43(9), 574-586.

Kshetri, N. 2021, 'Blockchain Technology for Improving Transparency and Citizen's Trust', in Advances in Information and Communication: Proceedings of the 2021 Future of Information and Communication Conference (FICC), Volume 1, Springer International Publishing, pp. 716-735.

Kshetri, Nir (2018)." Blockchain's Roles in Meeting Key Supply Chain Management Objectives," International Journal of Information Management 39, 80–89.

Land Transport Authority. (2021). Electronic Road Pricing (ERP). Retrieved from https://www.lta.gov.sg/content/ltaweb/en/roads-and-motoring/managing-traffic-and-congestion/electronic-road-pricing-erp.html

Lantz, L. and Cawrey, D. (2020). Mastering blockchain. chapter 8. Mining and Consensus, O'Reilly Media.

Larimer, D. (2014). A Publicly Owned and Operated Blockchain Database. BitShares.org.

Lee, J. H., Phaal, R., & Lee, S. H. (2013). An Integrated Service-Delivery and Network-Configuration Approach for Smart City Development. Journal of Urban Technology, 20(2), 1-21.

Li, J., Lu, R., & Xu, L. (2020). Blockchain-Based Smart City Architecture and Applications. In J. Zheng, H. Li, & C. Hu (Eds.), Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2 (pp. 277-293). Springer.

Li, Lu, and Xu (2020) discuss the architecture and applications of blockchain-based smart cities.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2018). A survey on the security of blockchain systems. Future Generation Computer Systems, 82, 56-81.

Li, X., Lu, R., Huang, X., & Liu, C. (2021). Blockchain technology in smart cities: A comprehensive review. Journal of Cleaner Production, 305, 127228.

Li, Y., Huang, X., Li, X., & Hu, Z. (2020). EdgeChain: An edge-computing-oriented blockchain architecture for resource-constrained smart cities. IEEE Transactions on Industrial Informatics, 16(6), 4284-4293.

Li, Y., Liu, Y., Wang, C., & Wang, F. (2020). An intelligent parking guidance and information system based on a wireless sensor network for smart cities. IEEE Transactions on Industrial Informatics, 16(3), 1826-1834.

Liang, X., Zhao, J., Shetty, S., & Liu, J. (2018). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. IEEE Access, 6, 13414-13425.

Liu, F. T., Ting, K. M., & Zhou, Z. H. (2012). Isolation Forest. In Proceedings of the 2012 IEEE 12th International Conference on Data Mining (ICDM), 1246-1251.

Louka, P. (2019). Blockchain for Smart Cities. In Proceedings of the 2019 International Conference on Blockchain and Cryptocurrency, pp. 75-79.

Malkhi, D., Nayak, K., & Ren, L. (2019, November). "Flexible Byzantine Fault Tolerance." In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1041-1053).

Minoli, D. & Occhiogrosso, B. 2018, 'Internet of things applications for smart cities', in Internet of Things A to Z: Technologies and Applications, pp. 319-358.

Mougayar, W. (2016). The business blockchain: promise, practice, and application of the next internet technology. John Wiley & Sons.

Mycelium. (n.d.). Mycelium Bitcoin Wallet. Retrieved from https://wallet.mycelium.com/.

Nair, P. R., & Dorai, D. R. (2021, February). "Evaluation of performance and security of proof of work and proof of stake using blockchain." In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 279-283). IEEE.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

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

Nguyen, C.T. et al. (2019) 'Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities', IEEE Access, 7, pp. 85727–85745. doi:10.1109/access.2019.2925010.

Nguyen, Q., Kim, D., Nguyen, M., Nguyen, T., & Kim, Y. (2019). A blockchain-based secure ridesharing framework for autonomous vehicles in smart cities. In Proceedings of the 5th International Conference on Computer and Information Sciences (ICCOINS) (pp. 1-6). IEEE.

OECD. (2019). Blockchain Technology and Competition Policy. Paris: OECD Publishing.

Oshri, I., Avigdor, G., & Fink, L. (2019). Real-time data analytics in the Internet of Things: Middleware support, challenges, and solutions. Systems Engineering Journal, 100, 101641.

Oshri, I., Elzarir, M., & Bloch, I. (2019). A survey on stream data management with InfluxDB. Data & Knowledge Engineering, 122, 66-92.

Pahlajani, S., Kshirsagar, A., & Pachghare, V. (2019). Survey on Private Blockchain Consensus Algorithms. In 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT) (pp. 1-6). Chennai, India: IEEE. doi: 10.1109/ICIICT1.2019.874135

Palestinian Central Bureau of Statistics. (2020). Population, Housing and Establishment Census- Ramallah Governorate. Retrieved from https://www.pcbs.gov.ps/site/881/default.aspx?tabID=881&lang=en-us&ItemID=3712&mid=4559&wversion=Staging

Palestinian Telecommunication Group - PALTEL. (2020). About Us. Retrieved from https://www.paltelgroup.ps/en/about-us

Peng, L., Feng, W., Yan, Z., Li, Y., Zhou, X., & Shimizu, S. (2021). Privacy preservation in permissionless blockchain: A survey. Digital Communications and Networks, 7(3), 295–307. https://doi.org/10.1016/j.dcan.2020.05.008

Pilkington, M. (2016). Blockchain technology: Principles and applications. In Research Handbook on Digital Transformations (pp. 225-253). Edward Elgar Publishing.

Popov, S. (2005). The Byzantine Generals Problem. Retrieved from https://people.eecs.

Popov, S. (2016). The Tangle. Retrieved from https://www.semanticscholar.org/paper/The-Tangle-Popov/43586b34b054b48891d478407d4e7435702653e0

Popov, S. (2017). The Tangle. IOTA.

R. G. Alcaraz, J. L. Munoz, A. F. Gomez-Skarmeta, “Blockchain Technology as an Institutional Technology: Definitions, Challenges and Opportunities”, Future Generation Computer Systems, vol. 88, pp. 173-184, 2018.

Rabiner, L. R. (1989). A tutorial on hidden Markov models and selected applications in speech recognition. Proceedings of the IEEE, 77(2), 257-286. doi:10.1109/5.18626.

Rahman, M. A., Hossain, M. S., Loukas, G., Hassanain, E., Rahman, S. S., Alhamid, M. F., & Guizani, M. 2018, 'Blockchain-based mobile edge computing framework for secure therapy applications', IEEE Access, vol. 6, pp. 72469-72478.

Ramallah Municipality. (n.d.). Ramallah Municipality. Retrieved May 16, 2023, from https://www.ramallah.ps/ar_page.aspx?id=j7myqea3408227493aj7myqe

Ramallah Municipality. (n.d.). Ramallah Smart City. Retrieved from https://www.ramallah.ps/

Ramallah Municipality. (n.d.). مبادرات رام الله المدينة الذكية. Retrieved from https://www.ramallah.ps/ar_category.aspx?id=yhr52oa1031700252ayhr52o

Resilient Ramallah 2050. (n.d.). Ramallah Resilience Strategy 2050. Retrieved from [source]

Resilient Ramallah 2050. (n.d.). Ramallah Resilience Strategy 2050 [PDF]. Available at: https://www.ramallah.ps/userfiles/file/ir/Ramallah%20Resilience%20Strategy%202050.pdf (Accessed: 17/05/2023)

Rodriguez, A., Garcia, M., & Linares, J. (2020). Design of a smart parking system based on IoT for smart cities. Sensors, 20(9), 2567.

Russell, Stuart J., and Peter Norvig. Artificial Intelligence: A Modern Approach. 3rd ed., Pearson, 2009.

S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran and N. Guizani, "Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges," in IEEE Network, vol. 34, no. 1, pp. 8-14, January/February 2020, doi: 10.1109/MNET.001.1900178

Saghiri, A.M. (2020). Blockchain Architecture. In: Kim, S., Deka, G. (eds) Advanced Applications of Blockchain Technology. Studies in Big Data, vol 60. Springer, Singapore. https://doi.org/10.1007/978-981-13-8775-3_8

Salha, R. A., El-Hallaq, M. A., & Alastal, A. I. 2019, 'Blockchain in smart cities: Exploring possibilities in terms of opportunities and challenges', Journal of Data Analysis and Information Processing, vol. 7, no. 3, pp. 118-139.

Scott, K., Motamedi, M., & Shaeffer, D. (2018). Energy on the blockchain. Renewable and Sustainable Energy Reviews, 98, 143-154.

Scott, M., Motamedi, A., & Shaeffer, B. (2018). "Evaluating blockchain's potential for microgrid applications." IEEE Transactions on Power Systems, 33(6), 6958-6969.

Seneviratne, P., Seneviratne, A., & Han, S. (2019). IoT-based smart parking systems for sustainable cities: A survey. IEEE Access, 7, 155055-155073.

Seth, S. 2021, 'Proof of Activity', Investopedia, 28 October 2021, Available at: https://www.investopedia.com/terms/p/proof-activity-cryptocurrency.asp (Accessed: 12/06/2023).

Shao, B. (2015). Smart Cities and the Internet of Things. In Proceedings of the 2015 International Conference on Future Internet of Things and Cloud, pp. 8-13.

Sharma, K., & Jain, D. (2019). "Consensus Algorithms in Blockchain Technology: A Survey." In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-7). doi: 10.1109/ICCCNT45670.2019.8944509.

Shen, C., & Pena-Mora, F. 2018, 'Blockchain for cities—a systematic literature review', IEEE Access, vol. 6, pp. 76787-76819.

Shi, X. et al. (2023) ‘Confronting the Carbon-Footprint Challenge of Blockchain’, Environmental Science & Technology, 57(3), pp. 1403–1410. doi:10.1021/acs.est.2c05165.

Shoup, D. (2018). The high cost of free parking (Updated edition). Routledge.

Siim, J. (2017). Proof-of-stake. In Research seminar in cryptography.

Singh, S. P., et al. (2020). Blockchain technology: A review of the security and privacy considerations. IEEE Technology and Society Magazine, 39(2), 55-66.

Smith, R., Jokar Arsanjani, J., & Mooney, P. (2019). A review of smart parking solutions for smart cities. Computers, Environment and Urban Systems, 77, 101375.

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

Swan, M. (2017). Blockchain: how to rewire the financial system. The British Blockchain Association.

Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.

Trezor. (n.d.). What is Trezor? Retrieved from https://trezor.io/.

Tsankov, P., Dan, A., Drachsler-Cohen, D., Gervais, A., Bünzli, F., & Vechev, M. (2018). Securify. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/3243734.3243780

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123.

Turesinin, M., Kabir, A. M. H., Mollah, T., Sarwar, S., & Hosain, M. S. 2020, 'Aquatic iguana: A floating waste collecting robot with IoT based water monitoring

system', in 2020 7th International Conference on Electrical Engineering, Computer Sciences and Informatics (EECSI), IEEE, pp. 21-25.

United Nations 2014, World Urbanization Prospects: The 2014 Revision, United Nations, viewed 01/05/2023, Available at: https://www.un.org/en/development/desa/publications/2014-revision-world-urbanization-prospects.html.

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., ...& Kaiser, L. (2017). Attention is all you need. arXiv preprint arXiv:1611.03941.

Vazirani, R., & Vazirani, R. (2020). A Comprehensive Study of Blockchain in Smart Cities. In Proceedings of the 3rd International Conference on Communication and Electronics Systems (ICCES 2018) (pp. 657-664). Springer. https://doi.org/10.1007/978-981-13-8323-6_62.

Voss, A., Croll, A., & Kalyanakrishnan, K. (2018). Performance evaluation of time-series databases for IoT workloads. In 2018 IEEE International Conference on Big Data (Big Data) (pp. 1304-1311). IEEE.

Wagner, K., Keller, T., & Seiler, R. (2019). "A Comparative Analysis of Cryptocurrency Consensus Algorithms." In *Proceedings of the 16th International Conference on Applied Computing 2019*.

Wang, Q., Huang, J., Wang, S., Chen, Y., Zhang, P., & He, L. (2020). A comparative study of blockchain consensus algorithms. Journal of Physics: Conference Series, 1437(1), 012007. doi:10.1088/1742-6596/1437/1/012007.

Werbach, K. (2018). Blockchain and the new architecture of trust. MIT Press.

Wong, H. G., Loo, B. P., Li, V. O., & Hui, T. C. (2018). Demand-responsive parking pricing for sustainable urban mobility. Transportation Research Part C: Emerging Technologies, 88, 215-233.

Wu, H., Huang, H., Zhao, W., & Shi, Y. (2017). An intrusion detection method based on improved K-means clustering algorithm. In 2017 IEEE Trustcom/BigDataSE/ICESS (pp. 322-327). IEEE

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., & Pautasso, C. (2017). A taxonomy of blockchain-based systems for architecture design. In Proceedings of the 2017 International Conference on Software Architecture (ICSA) (pp. 243-252).

Xu, X., Zhu, D., Yang, X., Wang, S., Qi, L., & Dou, W. (2021). Concurrent Practical Byzantine Fault Tolerance for Integration of Blockchain and Supply Chain. ACM Transactions on Internet Technology, 21(1), 1–17. https://doi.org/10.1145/3395331

Yadav, A.K. and Singh, K. (2020) 'Comparative Analysis of Consensus Algorithms of Blockchain Technology'. [Online] ResearchGate. Available at: https://www.researchgate.net/publication/348355281_Comparative_Analysis_of_Consensus_Algorithms_of_Blockchain_Technology (Accessed: 31/05/2023).

Yan, H., Wen, Y., & Rana, R. (2019). Blockchain-based smart city framework: A case study of blockchain in financial services. IEEE Access, 7, 73708-73720.

Yang, Y., Zhang, J., & Zhang, L. (2023). A new deep learning model for text classification. In Proceedings of the 2698th International Conference on Computational Science and Engineering (pp. 12-23). CEUR-WS.org.

Yao, W., Ye, J., Murimi, R., & Wang, G. (2021). A Survey on Consortium Blockchain Consensus Mechanisms. arXiv: Data Structures and Algorithms.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. PloS One, 11(10), e0163477.

Zamani, M., Movahedi, M., & Raykova, M. (2018). RapidChain. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/3243734.3243853

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. IEEE Internet of Things Journal, 1(1), 22-32.

Zhang, P., Wen, Y., & Huang, X. (2018). An overview of blockchain technology: Architecture, consensus, and future trends. In IEEE International Congress on Big Data (pp. 557-564). IEEE.

Zhang, W., & Yu, P. S. (2005). Intrusion detection using random forests. In Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 641-647).

Zhang, Y., Xu, X., Xu, X., & Zhao, S. (2018). Blockchain Empowered Smart City: Architecture and Applications. In Proceedings of the IEEE International Conference on Internet of Things (iThings) (pp. 1212-1217). IEEE.

Zhang, Y., Zou, D., Xue, R., Liao, S., & Tang, Q. (2021). Dubai smart vehicle upkeep: A consortium blockchain application for vehicle lifecycle management. In Proceedings of the 23rd International Conference on Information Integration and Web-based Applications & Services (iiWAS) (pp. 34-41). ACM.

Zhang, Z., & Zhang, Q. (2021). The impact of smart parking on urban travel: Evidence from a natural experiment in Beijing. Journal of Cleaner Production, 282, 124360.

Zhang, Z., Xu, L. D., & Xu, X. (2018). Blockchain technology for smart cities. IEEE Access, 6, 6492-6503.

Zheng, C., Yuan, J., Zhu, L., Zhang, Y., & Shao, Q. 2020, 'From digital to sustainable: A scientometric review of smart city literature between 1990 and 2019', Journal of Cleaner Production, vol. 258, 120689.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2020). An overview of blockchain technology: Architecture, consensus, and future trends. IEEE International Congress on Blockchain and Cryptocurrency, 1-10.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2020). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 16(4), 352-375.

Zhu, X., Xu, X., & Shen, W. (2016). Internet of Things for Smart Cities: Technologies and Applications. Springer.

Zohar, A. (2015). Bitcoin: Under the hood. Communications of the ACM, 58(9), 104-113.

Appendix 1: python Code: Create a new Block

```
import hashlib

import time

class Transaction:

    def __init__(self, car_park, user, vehicle_plate, reservation_time):

        self.car_park = car_park

        self.user = user

        self.vehicle_plate = vehicle_plate

        self.reservation_time = reservation_time

        self.status = 'Open'

        self.timestamp = time.time()

        self.signature = None

    def finish_transaction(self):

        self.status = 'Finished'

    def generate_signature(self):

        data = str(self.car_park) + str(self.user) + str(self.vehicle_plate) + str(self.reservation_time) + str(self.status) + str(self.timestamp)

        self.signature = hashlib.sha256(data.encode()).hexdigest()

    def __str__(self):

        return f"Car Park: {self.car_park}\nUser: {self.user}\nVehicle Plate: {self.vehicle_plate}\nReservation Time: {self.reservation_time}\nStatus: {self.status}\nTimestamp: {self.timestamp}\nSignature: {self.signature}"

class Block:

    def __init__(self, transactions, previous_hash):

        self.transactions = transactions

        self.previous_hash = previous_hash

        self.timestamp = time.time()

        self.nonce = 0

        self.hash = None
```

Appendix 2: Random Forests ML Algorithm experiment

```
import pandas as pd

from sklearn.ensemble import RandomForestClassifier

from sklearn.model_selection import train_test_split

import time


# Load the data

blocks_data = pd.read_csv('blocks.csv')

shady_blocks_data = pd.read_csv('malicious _blocks.csv')


# Define features and target

features = ['ver', 'bits', 'nonce', 'n_tx', 'size', 'block_index', 'height']

target = 'shady'


# Add a 'shady' column to the blocks_data

blocks_data['malicious '] = 0

shady_blocks_data['malicious '] = 1


# Combine both datasets

combined_data = pd.concat([blocks_data, malicious _blocks_data])


# Split the data into training and testing sets

X_train, X_test, y_train, y_test = train_test_split(combined_data[features], combined_data[target],
test_size=0.2, random_state=42)


# Initialize and train the Random Forest Classifier

rf_classifier = RandomForestClassifier(n_estimators=100, random_state=42)
```

Appendix 3: Hidden Markov Models (HMMs) ML algorithm.

```
from hmmlearn.hmm import GaussianHMM

import pandas as pd

import time


# Load the data

blocks_data = pd.read_csv('blocks.csv')

malicious _blocks_data = pd.read_csv('malicious _blocks.csv')


# Define features

features = ['ver', 'bits', 'nonce', 'n_tx', 'size', 'block_index', 'height']


# Select features for training

X_train = blocks_data[features]


# Select features for testing (malicious blocks)

X_test = malicious _blocks_data[features]


# Define the number of hidden states

n_components = 2


# Initialize the HMM model

model = GaussianHMM(n_components=n_components)


# Measure the start time

start_time = time.time()
```

Appendix 4: K-means algorithm ML algorithm experiment.

```
import pandas as pd

from sklearn.cluster import KMeans

import time


# Load the data

blocks_data = pd.read_csv('blocks.csv')

malicious _blocks_data = pd.read_csv('malicious _blocks.csv')


# Define features

features = ['ver', 'bits', 'nonce', 'n_tx', 'size', 'block_index', 'height']


# Select features for training

X_train = blocks_data[features]


# Select features for testing (malicious blocks)

X_test = shady_blocks_data[features]


# Initialize and train the K-means model

kmeans = KMeans(n_clusters=2, random_state=42)

start_time = time.time()

kmeans.fit(X_train)

training_time = time.time() - start_time


# Predict clusters for testing data (malicious blocks)

start_time = time.time()
```

Appendix 5: Isolation Forest anomaly detection ML algorithm

```
from sklearn.ensemble import IsolationForest

import pandas as pd

import time


# Load the data

blocks_data = pd.read_csv('blocks.csv')

malicious _blocks_data = pd.read_csv('malicious _blocks.csv')


# Define features

features = ['ver', 'bits', 'nonce', 'n_tx', 'size', 'block_index', 'height']


# Select features for training

X_train = blocks_data[features]


# Select features for testing (malicious blocks)

X_test = malicious _blocks_data[features]


# Initialize the Isolation Forest model

model = IsolationForest(random_state=42)


# Measure the start time

start_time = time.time()


# Fit the model on normal blocks

model.fit(X_train)
```

ملخص الدراسة

هدفت الدراسة إلى تسليط الضوء على استخدام الذكاء الاصطناعي في تقنية Blockchain ودراسة المدن الذكية ودراســـة مدينة رام الله الذكية ومن ثم الربط بين التقنيتين من أجل الاســـتفادة منها بالشكل الأمثل، حيث قدمت الدراسة مقترح تطبيق تقنية Blockchain في مدينة رام الله في فلسطين من خلال اقتراح برنامج مواقف الســيارات الذكي في مدينة رام اللهRSP وذلك من اجل المســاهمة في تحويل قطاع النقل من شكله التقليدي الى قطاع نقل ذكي من شأنه ان يسهم في تخفيف الازدحام المروري والتقليل من التلوث البيئي الناجم عن احتراق الوقود في السيارات وكذلك تعزيز منظومة الأمن في مدينة رام الله الذكية من خلال مكافحة ظاهرة الســيارات الغير قانونية وكذلك مكافحة سرقة السيارات ، قدمت الدراسة خوارزمية إجماع جديدة في تقنية Blockchain واطلق عليها اسم SMO حيث أن هذه الخوارزمية تعمل في ثلاث مراحل وتبدأ بالمرحلة الأولى بإنشـــاء الكتل باســـتخدام خوارزمية الإجماع Proof-of-Work وفي المرحلة الثانية تكون عبارة عن طبقة حماية إضـــافية اطلق عليها اســـم Block Bank حيث تعمل هذه الطبقة على الكشـــف المبكر عن الكتل والمعاملات الخبيثة باســـتخدام خوارزميات التعلم الالي ML (Anomaly detection (Isolation Forest), Hidden Markov Models, K-means, Random Forests) حيث تقم الخوارزمية بتخزين الكتل الخبيثة التي تم اكتشـــافها في Distributed ledger للاســـتفادة منها في العمليات اللاحقة في التعرف على الكتل الخبيثة ، المرحلة الثالثة يتم اســـتخدام خوارزمية الإجماع Proof-of-Stake في تدقيق الكتل التي لم يتم التعرف عليها في المرحلة الثانية وفي حال اكتشاف كتلة خبيثة يتم إرسالها الى Distributed ledger من اجل الاستفادة منها في التعرف على الكتل الخبيثة.

اقترحت الدراســـة التوصـــيات التالية: ضـــرورة تشـــجيع الباحثين المحليين بشـــدة على معالجة واستكشاف تكنولوجيا blockchain في فلسطين، إضافة إلى ضرورة دراسة القطاعات الأساسية المختلفة في مدينة رام الله والمساهمة في تحويلها من شكلها التقليدي إلى قطاعات ذكية.

كما تقترح الدراسة أن يتم تطبيق الدراسة الحالية على بقية المدن الفلسطينية والبحث عن سبل تحويلها إلى مدن ذكية، بالإضافة إلى أن يقوم الباحثون باستكشاف تكنولوجيا الذكاء الاصطناعي لرفع مستوى الأمان في تكنولوجيا blockchain.