SAMUEL OBISESAN A REVIEW OF BLOCKCHAIN TECHNOLOGIES MASTER THESIS 2023
IN THE FIELD OF
INFORMATION SECURITY AND PRIVACY

NEAR EAST UNIVERSITY

INSTITUTE OF GRADUATE STUDIES

DEPARTMENT OF SOFTWARE ENGINEERING

A REVIEW OF BLOCKCHAIN TECHNOLOGIES IN THE FIELD OF INFORMATION SECURITY AND PRIVACY

M.Sc. THESIS

Samuel O. OBISESAN

Nicosia

January, 2023

NEAR EAST UNIVERSITY

INSTITUTE OF GRADUATE STUDIES

DEPARTMENT OF SOFTWARE ENGINEERING

A REVIEW OF BLOCKCHAIN TECHNOLOGIES IN THE FIELD OF INFORMATION SECURITY AND PRIVACY

M.Sc. THESIS

Samuel O. OBISESAN

Supervisor

Assoc. Prof. Dr. Boran ŞEKEROĞLU

Nicosia

January, 2023

Approval

We certify that we have read the thesis submitted by Samuel Obiesan titled "A review of blockchain technology in the field of information security and privacy" and that in our combined opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Software Engineering.

Examining Committee	Name-Surname	Signature
Head of the Committee:	Assoc. Prof. Dr. Yöney K. Eker	
Committee Member*:	Dr. Ahmet Ilhan	
Supervisor:	Assoc. Prof. Dr. Boran Şekeroğlu	

Approved by the Head of the Department

05.../02.../2023

Assoc. Prof. Dr. Boran Şekeroğlu

Head of Department

Approved by the Institute of Graduate Studies

..../...../23...

Prof. Dr. Kemal Hüsnü Can Başer

Head of the Institute

NEAR EAST UNIVERSITY INSTITUTE OF GRADUATE STUDIES 1988

Declaration

I hereby declare that all information, documents, analysis and results in this thesis have been collected and presented according to the academic rules and ethical guidelines of Institute of Graduate Studies, Near East University. I also declare that as required by these rules and conduct, I have fully cited and referenced information and data that are not original to this study.

Samuel O. Obisesan

08/03/23

Day/Month/Year

Acknowledgments

Foremost, I would like to give thanks to the Almighty, my family and friends despite the challenges. I appreciate the unconditional support of my supervisor Assoc. Prof. Dr. Boran Şekeroğlu throughout my research study, for his motivation, guidance, patience, enthusiasm and immense knowledge. Also, I could not have imagined having a better advisor for his guidiance throughout the course of my study.

Samuel Obisesan

Abstract

A Systematic Analysis on the Impacts of Blockchain Technologies in the Field of Information Security and Privacy

Samuel O. Obisesan
MA, (Software Engineering)
January, 2023, 92 pages

The present thesis analyses the impacts of blockchain technologies in the field of information security and privacy. The Data was collected through a systematic analysis of related literatures and Concept Matrix was opted to help identify the concepts that are relevant to the topic in each of the selected articles. The objectives of the thesis are: (i) to determine if blockchain is a proven technology and if it delivers what it promises; (ii) to determine the latest blockchain applications focused on security; (iii) to determine how blockchain is used to improve information security; (iv) to determine how blockchain is used to improve information privacy and (v) to determine the methods available for blockchain solutions to manage security and privacy. In this thesis, the selected literatures were obtained from different online databases such as IEEE Xplore, google scholar, Science Direct, ACM digital library, online university library and springer link. All the literature found based on key words defined were examined according to inclusion criteria. The final selected papers were relevant to answer the research question as the expected main outcome of this study. However, there were 93 publications found in total, however only 20 were determined to be related to the research issue and were reviewed. The outcomes from the concept matrix revealed that Blockchain technology has the potential to transform people's lives because of its operating mechanism and architecture, which ensure network openness, trust, security, and integrity. This study connected security attacks in blockchain technology to common security issues and concerns. Investigation from this study recommends the deployment of an advanced encryption approach to increase security, which could also be applied to other types of assaults.

Key Words**:** *Blockchain, technology, information security, privacy*

ÖZ

Blockchain Teknolojilerinin Bilgi Güvenliği ve Gizlilik Alanındaki Etkilerine İlişkin Sistematik Bir Analiz

Samuel O. Obisesan
MA, (Software Engineering)
January, 2023, 92 pages

Bu tez, blok zincir teknolojilerinin bilgi güvenliği ve mahremiyet alanındaki etkilerini analiz etmektedir. Veriler, ilgili literatürlerin sistematik bir analizi yoluyla toplandı ve seçilen makalelerin her birinde konuyla ilgili kavramların belirlenmesine yardımcı olmak için Kavram Matrisi seçildi. Tezin amaçları: (i) blok zincirinin kanıtlanmış bir teknoloji olup olmadığını ve vaat ettiklerini yerine getirip getirmediğini belirlemek; (ii) güvenlik odaklı en son blok zinciri uygulamalarını belirlemek; (iii) bilgi güvenliğini geliştirmek için blok zincirinin nasıl kullanıldığını belirlemek; (iv) bilgi gizliliğini geliştirmek için blok zincirinin nasıl kullanıldığını belirlemek ve (v) güvenlik ve gizliliği yönetmek için blok zinciri çözümlerinde mevcut yöntemleri belirlemek. Bu tezde seçilen literatürler IEEE Xplore, google alim, Science Direct, ACM dijital kütüphane, online üniversite kütüphanesi ve springer link gibi farklı çevrimiçi veri tabanlarından elde edilmiştir. Tanımlanan anahtar kelimelere dayalı olarak bulunan tüm literatür dahil etme kriterlerine göre incelenmiştir. Nihai olarak seçilen makaleler, bu çalışmanın beklenen ana sonucu olarak araştırma sorusunu yanıtlamakla ilgiliydi. Ancak toplamda 93 yayına ulaşılmış, ancak bunlardan yalnızca 20'sinin araştırma konusuyla ilgili olduğu belirlenerek gözden geçirilmiştir. Konsept matrisinden elde edilen sonuçlar, Blockchain teknolojisinin ağ açıklığı, güven, güvenlik ve bütünlük sağlayan işletim mekanizması ve mimarisi nedeniyle insanların hayatlarını dönüştürme potansiyeline sahip olduğunu ortaya koydu. Bu çalışma, blok zinciri teknolojisindeki güvenlik saldırılarını ortak güvenlik sorunları ve endişeleriyle ilişkilendirdi. Bu çalışmadan elde edilen araştırma, güvenliği artırmak için diğer saldırı türlerine de uygulanabilecek gelişmiş bir şifreleme yaklaşımının kullanılmasını önermektedir. Anahtar.

Kelimeler: *Blockchain, teknoloji, bilgi güvenliği, mahremiyet*

Table of Contents

CHAPTER III

CHAPTER IV

CHAPTER V

CHAPTER VI

List of Tables

List of Figures

CHAPTER I

Introduction

1.1 Background of the Study

Digital currencies like bitcoin, ethereum, and hyperledger are built on top of blockchain technology. It is one of the most advanced and well-known technologies to emerge during the most recent wave of technological and industrial revolutions. Bitcoin: A Peer-to-Peer Electronic Cash System In terms of privacy and security, the blockchain has a very high tendency to achieve point-to-point and other features, as well as a distributed ledger, asymmetric encryption, intelligent contracts, consensus mechanism, and other vital technologies that can guarantee the privacy and security issues in the transaction process. Digital banking (Zhu, 2019), IoT (Fremantle, 2017), edge computing (Xu, Wang, Bhargava, and Yang, 2019), artificial intelligence (AI) (Salah, 2018), supply chain management (SCM), and many other industries have all benefited from the expansion of blockchain technology in recent years. Several governments around the world are making it easier for block chain technology to spread.

Users' privacy is jeopardised since in order to establish agreement, all nodes in the network must divulge the chain's transaction information (Liu, 2018). For this reason, it is important to examine focused privacy protection techniques. In the last several years, many methods and popular applications for blockchain privacy protection have evolved, which may prevent assaults or tampering with privacy from various viewpoints. The importance of privacy must be taken into account while preserving the interests of users. A detailed study on how blockchain maintains privacy is needed so that it may be used as a reference and support for current and future research projects.

Individuals and organisations alike face significant cybersecurity issues as a result of data theft, which compromises not only a person's right to privacy but also one of the basic features of cybersecurity, namely confidentiality. Many countermeasures have been tried over the last few decades, but as cyber thieves improve their skills, many of them have fallen short of expectations. Blockchain technology is the most recent addition. Dispersed network data is subject to theft and copying, and tracking down the cyber-thief might be challenging. Blockchain technology removes a slew of problems on several levels. A distributed database or a book that records and distributes all the events

and transactions that have transpired might be described as a blockchain. In such transactions, the data submitted cannot be seen by anybody but the person making the transaction. There was a record of each and every transaction. It is possible to use blockchain technology in both financial and non-financial areas.

Blockchains are public registers such that all transactions are gathered in a list of blocks (Rajput, 2015). When numerous blocks are added together, a chain-like shape results. Blockchain Technology is built on the foundations of cryptography and distributed systems. Encryption techniques have been known to obscure content so that only the intended users are accessible to it. But certain information needs to be available to a specific set of people, and this will increase the risk of the information getting tampered with. Blockchains solve the issue. Any change made to the data is logged and validated as it is accessed and updated. Thereafter, it is encrypted so that further changes can not be made to the update after verification. The main records are then updated with these adjustments. This process is repeated every time a change is made, and the information is preserved in a new block. It is remarkable to see how closely the initial and latest versions of the material are linked. Thus, the changes made can be seen by everyone, but modification can only be done on the latest block. By combining information copied across the network in real time, the blockchain imitates a distributed database. This indicates that the database is spread across various places and that the records are open to the public and easily verified. Since there is no centralised version, data corruption is ineffective. Modifying records is so tedious, which makes it easier to detect if someone is trying to tamper with the information.

As a result, the following characteristics of a blockchain may be considered;

- It's continually being improved on. As a consequence, data may be seen and edited at any time by users.
- A distributed system is one in which data is stored in several locations throughout the network. In the event that one record is updated, all other records are automatically updated as well.
- It's backed up by facts. Users must use cryptographic techniques to validate data changes.

- Distributed systems and cryptographic approaches ensure that data and security procedures cannot be tampered with.

There are two sorts of blockchains: permissionless and permissioned. In a permissionless blockchain, any peer can join and leave the network as a reader or writer. Because the information is decentralised, it may be accessed by anybody. Forbidden blockchains have a limited readership and authorship capacity. Individuals' ability to read and write is controlled by a single, centralised authority (Zhu, 2019).

1.2 Statement of the Problem

Is the blockchain secure, despite its efficiency and the nature of the technology? Is it feasible to produce private and tamper-proof records with blockchain-based technology that provides both trust and privacy? Many in the development sector, enterprises, and governments are wary of using blockchain technology for a variety of purposes, including remittances, smart contracts, and the provision of health care. The usage of Blockchain technology raises another issue, which is privacy.

Considering the fact that they are open and tamper-proof, blockchain networks are ripe for attack. Despite the fact that the transactions are anonymous, the attacker can still use the transaction graph to determine the link between the two parties involved. The public openness of the blockchain will put users' personal information and financial transactions at risk.

It can be said that any node in the command chain can access the full scope of information available to it. Even though the blockchain provides some anonymity for transactions, as computing power improves, this anonymity is no longer sufficient to safeguard user identity. An attacker can get access to sensitive information by monitoring and judging the relevance of public data in the global ledger.

Any party to a transaction has the opportunity to download a permissionless ledger, so even those who aren't members may see the whole history of transactions. Privacy might be severely compromised in a permissioned ledger by using authorised agents' or smart contract capabilities, depending on the access privileges of the agent or smart contract authors. Diverse security vulnerabilities continue to blight the larger crypto network, which is isolated from the blockchain. Trade security and privacy are

the first issues that need to be addressed. Digital currency hacks have a long history, and some have resulted in huge sums of money being traded.

Despite the many benefits of blockchain technology, are these security and privacy characteristics being fully utilised by organisations? Is there a link between blockchain technology and the security and privacy of an organisation?

Therefore, the goal of this study is to carefully look at how blockchain technology affects information security and privacy.

1.3 Research Aims and Objectives

It is the goal of this research to examine the effects of blockchain technology on information security and privacy. To accomplish this goal, the following research questions must be answered:

1. Do you think blockchain is a proven technology?
2. Are there any new uses of blockchain technology that focus on security?
3. What are the benefits of using a blockchain-based security system?
4. How might blockchain technology be utilised to enhance data security?
5. What security and privacy controls may be included in blockchain solutions?

1.4 Significance of the Study

The use of blockchain technology is becoming increasingly popular. This technology is used in a wide range of applications. Transactions on the blockchain are quicker and cheaper than any other method. It will increase the security of sensitive data, especially the immutability and transparency of blockchains are often cited as additional advantages. Future scholars will be able to utilise these findings as a reference in their own work because of the study's widespread use. In addition, the conclusions from this research will serve as a guide for new and established firms on how to maximise the advantages of digital transformation.

1.5 Definition of Terms

1. **Blockchain Technology:** Blockchain is very complex system and comprises of distributed digital ledgers of cryptographically signed transactions that are grouped into blocks.
2. **Information:** Information is processed, organized and structured data. It provides context for data and assists in decision-making.
3. **Information Security:** The practice of preventing unauthorized access, use, disclosure, disruption, alteration, inspection, recording, or destruction of information is known as information security.
4. **Information Privacy:** The relationship between data collection and dissemination, technology, the public expectation of privacy, and the legal and political challenges surrounding them is known as information privacy.

CHAPTER II

Literature Review

2.1 History and Background of Blockchain Technology

The foundations of blockchain technology have been laid In the late '80s and early '90s,. while working on Paxos in 1989, Leslie Lamport wrote the ACM Transactions on Computer Systems paper The Part-Time Parliament (Lamport, 1998) and submitted it for publication in 1990. There is a consensus model proposed in the study for a network of computers with unreliable computer systems. Electronic ledgers based on a signed chain of information were used to digitally sign papers in 1991, with the capacity to prove immediately that no signed documents had been altered (Narayanan, 2016). In 2008, Satoshi Nakamoto published a paper in which he merged and applied these ideas to electronic currency. As of late 2009, the Bitcoin cryptocurrency blockchain network was named after Nakamoto, a pseudonym that he used to set up the network. Nakamoto's work serves as a roadmap for the majority of existing cryptocurrency schemes (although with variations and modifications). Bitcoin was the first of many uses of the blockchain.

In November 2008, the idea of a "blockchain" was initially proposed (Satoshi, 2008). The author of the pseudonym Satoshi Nakamoto wrote a whitepaper on the Bitcoin electronic cash system (Satoshi, 2008). In 2009, the system went live and became the first to offer a fully working distributed ledger. An open ledger of all transactions is maintained by Satoshi (2008), a decentralised peer-to-peer (P2P) network. As a result, the whole history of transactions is available to everyone on the network. However, transactions can only be written or updated by parties who have been authorised to do so. Many basic difficulties were handled in an innovative and viable manner by Bitcoin at its core, which effectively incorporated contributions from decades of study (Florian, 2016). Although blockchain technology is still a relatively new approach to computer science, it is becoming more and more popular. Currently, it is being investigated and tested for a wide range of applications and use cases.

Since the early 1980s, there has been discussion on totally dispersed money (Florian, 2016). A single organisation does not have control or management of distributed money. A bank or any other middleman should be fully eliminated, allowing ownership rights to only be transferred between the sender and the recipient of a payment. A trust architecture that relies on a central authority, offering a clearinghouse service for transaction verification and ownership record organisation has always failed to provide dispersed currencies (Andreas, 2017). Because of this, the data held on centralised ledgers is completely under the jurisdiction of these authorities. To address this issue, the notion of a distributed ledger was proposed. There should not be a single or exclusive set of authorities that control the saved data. The term "Distributed Ledger Technology" refers to the notion of storing transaction data in redundant ledger copies over a wide area (DLT).

In the years before Bitcoin, there were other e-cash systems (including ecash and NetCash), but none of them were widely used. Bitcoin's widespread adoption was aided by the widespread usage of a blockchain, which allowed the digital currency to be disseminated without a central authority or single point of failure. As a result, users may conduct transactions directly with one other rather than relying on a third party. Those who successfully released new blocks and maintained copies of the ledger, known as miners in Bitcoin, might likewise benefit from the regulated release of new money. There was no need for the miners to organise because payments were made automatically. In order to ensure that only genuine transactions and blocks were added to the network, a self-policing approach based on a blockchain and consensus-based maintenance was developed.

The use of a blockchain as a distributed ledger is a cutting-edge innovation. However, previous to the introduction of Bitcoin, all attempts to build a fully distributed money failed because of one key unsolvable issue. Double-spending coins are a problem for decentralised currencies. It is possible to transfer the same coin to several recipients at the same time since digital copies are so easy to generate. One of the most difficult problems distributed currencies face is the so-called "double-spending dilemma" (Usman, 2017). In 2008, Satoshi Nakamoto came up with a solution to this dilemma by releasing Bitcoin (Satoshi, 2008). The word "blockchain" captures the essence of this

solution's methodology. Because all transactions are recorded sequentially, the double-spending problem is eliminated.

When two or more transactions are found to be in conflict, just the first one is approved and the others are deleted. Thus, a distributed timestamp server is what the blockchain is all about (Satoshi, 2008). One ledger can serve as the only source of truth in this model. Everyone has to agree on the current status of the ledger in a decentralised P2P ecosystem.

With the help of the Bitcoin blockchain, it is possible for users to remain completely anonymous. Although users' identities are hidden, the public may see all of their transactions. Pseudo-anonymity is provided by Bitcoin since no identification or authorisation procedure is necessary (as is often required by Know-Your-Customer (KYC) standards).

As a result of the anonymity provided by Bitcoin, mechanisms for establishing trust have to be implemented. For many years, both parties relied on trusted intermediates to provide this assurance before using blockchain technology.

With these features, parties with no prior knowledge of one another (known as "permissionless blockchain networks") can trust each other in blockchain networks that allow anybody to establish an account and participate anonymously. Individuals and organisations may interact more directly with one another when they have this level of confidence, which can speed up and reduce the cost of transactions.

2.2 Concept of Blockchain Technology

The "blockchain" can be considered as a novel technology that trancends a virtual money and can provide a different perspective than what has previously been available in terms of openness and privacy (Nakamoto, 2008). Considering different implementations of blockchain can define several levels of privacy and anonymity as well as transparency and immutability of records (Gordon & Manoj 2018), his necessitates the development and implementation of privacy and anonymization technologies that ensure the inclusion of these features in blockchain. For blockchain 3.0 (Efanov, 2018), this technology reaches all areas of application, not just

cryptocurrencies, taking on strength in the digital society in which we are immersed. As a result, it's critical to look at the processes that enable worldwide privacy, traceability, anonymity, and, above all, security, which are all notable contributions of blockchain technology.

A blockchain could be a chain of hinders that contain explicit information (database), anyway in an extremely secure and genuine implies that is arranged along in a very system (shared) (BBP, 2017). In other words, blockchain might be a collection of PCs linked to one another rather than a single server, implying that the entire system is decentralized.

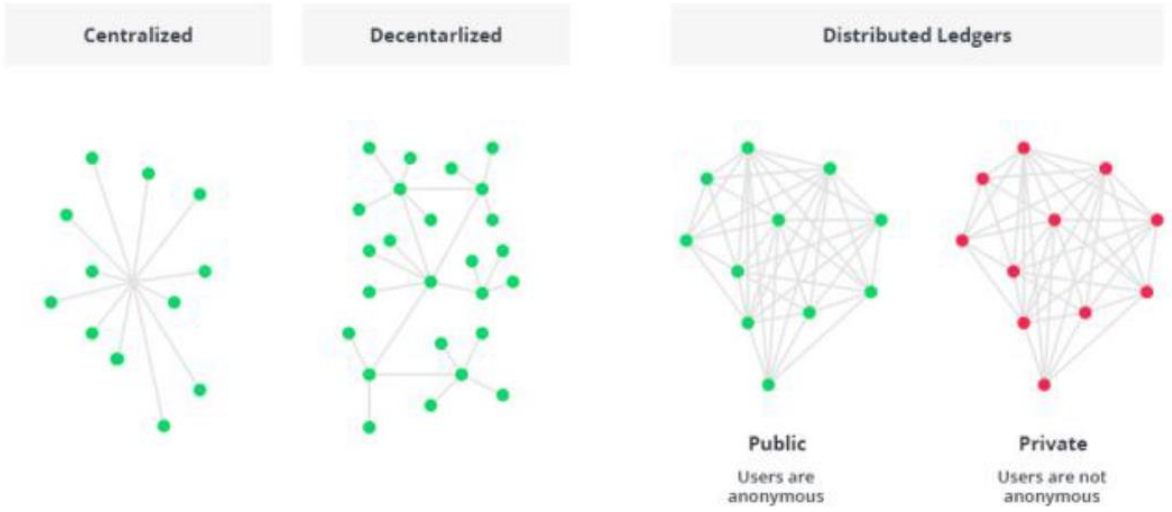


Figure 1: Centralized, Decentralized, and Distributed Ledger

Blockchain technology allows for the construction of a decentralized ecosystem in which cryptographically certified transactions and data are not controlled by a third party. Any transaction that has ever been performed is stored in an immutable ledger with a timestamp and other details in a verifiable, secure, visible, and permanent manner.

The term blockchain, initially block chain, was invented in 2009 in the original source code for the virtual currency Bitcoin by (the still unknown) Satoshi Nakamoto: "When they solve the proof-of-work, they broadcast the block to everyone and it is added to the block chain" (Nakamoto, 2009).

Blockchain technology consists of tamper-proof and tamper-evident digital ledgers that are implemented as a distributed system without a central repository and

frequently without a central authority, such as a government, bank, or corporation. It allows members of a community to keep track of transactions in a shared ledger. The transactions cannot be changed when they are published in the blockchain network's normal operation. In 2008, BT was combined with other computing concepts and technology to develop a new cryptocurrency based on blockchain. Following the launch of the BTC cryptocurrency in 2009, which allowed digital payments to be transacted within a distributed ledger, BT rose to prominence. The digital rights of Bitcoin users can be digitally signed and transferred to another BTC user. The BTC blockchain announces this transfer publicly to all the network users to independently verify the transaction's validity; moreover, a distributed group of users independently manages and maintains the BTC blockchain, and this, together with cryptographic mechanisms, creates BT's resilience toward subsequent attempts to modify the ledger by counterfeiting the transaction or altering the blocks. Blockchain technology has enabled the development of numerous cryptocurrency systems, such as Ethereum and Bitcoin, and that is why some people tend to restrict BT to cryptocurrency solutions only; however, a variety of industry sectors are considering incorporating BT into their applications (Tikhomirov, 2018).

Since 2008, Satoshi Nakamoto (Nakamoto, 2008) published an article announcing a new digital currency with features that were a technological revolution, not just in the world of finance. Given the concept behind the Bitcoin paradigm, this was a novel method of doing things. This new money gives birth to something far more significant, bringing innovation to existing methods of information organization and storage; blockchain technology is introduced. To begin with, it implies the removal of intermediaries, resulting in the democratization of all participating nodes, creating a network of equals (peer to peer (P2P)) that validates information entered into the blockchain using a consensus process. By avoiding a centralized trust environment and providing higher security against a single point failure, the potential of all network members having a copy of the database (distributed database) is realized, and it begins to create a much more resistant structure to probable attacks. From service availability to the persistence of certified information in the system, blockchain technology delivers many various features to every sector where it is sought to apply. Since the

introduction of this unique notion concerning cryptocurrencies, additional variations of Bitcoin have emerged, introducing cryptocurrencies such as Litecoin, Ripple, Monero, Ethereum, and many others. Projects such as ALASTRIA (Alastria, 2020) were born, which represents a commitment to research and development of blockchain technology in different sectors of the productive fabric. Smart contracts gave blockchain a new feature: they introduced software contracts into the chain of blocks that, by satisfying specific requirements, validated their execution without the need for third parties to interfere (Blockchain 2.0), as Ethereum does. The next stage was to use this technology to other industries, such as the development of decentralized software applications (DApps) using the decentralisation characteristic, which is known as Blockchain 3.0. (Francesco Maesa, 2020). According to the works in (Gordon, 2018, Manoj Kumar 2018, Reyna, 2018, Lin, 2018 and Yang, 2018), blockchain has been employed in a variety of fields, including health, logistics and transportation, IoT, and even industry (Industry 4.0), with new uses being discovered all the time. This is an industry where operations are meticulously digitized and where various sorts of industrial elements, sensors, actuators, and other electronic and thus computer components are used. At the moment, the industry is undergoing significant modernization and dramatic changes in the design of its production processes, which include IoT, Big Data, Augmented Reality, Cloud Computing, 3D Printing, and even Artificial Intelligence, intelligent cities, and other technology fields, which implies this opening of the blockchain technology to a multitude of different devices that interact with each other sharing information, is what we call Industry 4.0 (Lin, 2018).

The truth is that blockchain technology has impacted much more than digital currency creation. It has made possible a new form of information processing, with all that it implies, by designing a blockchain with very specific elements (Lai, 2018):

i. **Ledger:** It is the information storage structure: a distributed ledger. This means that each of the blockchain's participants has an identical copy of the distributed database.

ii. **Consensus Protocols**: Each time a new block is introduced in the network, it needs to be validated by a majority of members belonging to the blockchain network and this is achieved through the consensus protocols. Proof of Work

(PoW), Proof of Stake (Pos), Delegate Proof of Stake (DPos), Practical Byzantine Fault Tolerance (PBFT), Leased Proof-of-Stake (LPos), Proof-of-Activity (Poa), Proof-of-Importance (Poi), Proof-of-Capacity (PoC), Proof-of-Burn (PoB), and Proof-of-Weight (PoW) are among the popularly recognized.

iii. **Miners:** These are the network nodes that create the new blocks. To do so, they must solve a complicated cryptographic problem that necessitates a large amount of computer power; the node that solves the challenge first is in charge of producing the new block and so receives a reward.

iv. **Public Key Infrastructure (PKI):** This type of cryptography makes it possible not only to uniquely identify the participating nodes of the blockchain network, not just to permit communication between them via public–private keys, but also to identify blocks and transactions in the system in a secure and unrepeatable manner. The content of each block in the chain is validated using hash functions (e.g., SHA-256).

v. **Nodes:** Network of nodes that make up the entire blockchain network and between which there is communication, exchanging data, transactions, adding new blocks or validating transactions.

In terms of security, blockchain technology has certain unique characteristics:

i. **Immutability:** Once a transaction is validated, it becomes permanent and cannot be changed.

ii. **Availability:** Being based on a distributed database means high availability.

iii. **Integrity:** The application of cryptographic functions to validate a transaction increases the level of integrity of the information and prevents the inclusion of corrupted information, in this situation, the block would be rejected because the content could not be confirmed using the hash algorithms that were previously recorded.

Furthermore, because each block keeps a reference to its predecessor, including the result of the hash function, we can validate the entire chain.

iv. **Transparency:** The fact that all transactions are stored in the ledger and that any transaction can be traced is particularly attractive for many fields of application.

v. **Auditability:** There is a record of sufficient information about the transactions to leads to any verification of the transactions and their veracity.

vi. **Fault tolerance:** Characteristic related to the concept of decentralization added to the consensus mechanisms that validate transactions.

vii. **Consistency:** The decentralized design of the Ledger and the application of cryptographic functions makes it possible for the information stored in the chain to be preserved permanently and without the ability to change it without being discovered.

viii. **Privacy:** The identity of those involved in a transaction is protected by cryptographic functions, a concept related to the capacity of anonymity in blockchain.

ix. **Anonymity:** Pseudomisation or anonymisation, as appropriate, is provided by cryptographic functions so that the true identity of the participants in the blockchain is not known. The use of public–private key cryptography makes this possible.

The Nakamotos white paper (Dannen, 2017) introduced the concept of electronic cash, and with the launch of the BTC cryptocurrency in 2009, BT became one of the widely talked-about technologies. Blockchain is a database of blocks that are linked together with a cryptography hash function, with replicated information stored in all participants' server. The data in the BT database is immutable. It can grow only by appending new block (data) at the end of the chain by authenticated users (miners) with strong cryptography capability, as they can add the new block through a competitive mining scheme. Bitcoin is not blockchain. Bitcoin is just one of the many applications utilizing BT to support the BTC cryptocurrency network, which allows digital cash to be transferred within a distributed ledger. Ripple (XRP), Ethereum (ETH), Bitcoin Cash (BCH), Litecoin (LTC), and Binance Coin are among the many other cryptocurrencies (BNB). BTC allows users to digitally sign and transfer their BTC ownership to another BTC user. The BTC blockchain announces this transfer publicly to all the network users to independently verify the transaction's validity; moreover, the BTC blockchain is managed and maintained by a distributed set of users, and this, combined with cryptographic techniques, gives BT its non-repudiation

capability against attempts to alter the ledger by forging transactions or changing blocks.

There are three main types of Blockchain Technology: private, public or permissionless, and federated or consortium blockchain. Both private and consortium blockchains are considered as permissioned; a permission management entity is required to grant access rights to trusted and known participants. Multichain, Monax, and Quorum are examples of private blockchains. More than one organization controls a consortium blockchain. The group of organizations that control the consensus mechanism have predetermined nodes in the network. Ripple, R3 (banking), and B3i (insurance) are other examples. In contrast to the previous two types, public blockchain allows anyone to write or read the data stored in the blockchain network, without any permission from any authority, and the operation is entirely decentralized and anomalous. Some examples are Monero, Etherum, and Bitcoin. Public blockchain often uses a consensus-based system.

2.2.1 Blockchain Technology Architecture

Blockchain is a technology where multiple parties involved in communication can perform different transactions without third-party intervention. Miners are particular types of nodes that verify and validate these transactions/communications. A block is a data structure that contains all of the valid transactions. The current transaction's execution is dependent on previously committed transactions. This method helps to avoid/restrict double-spending in the bitcoin system in this way. Figure 2 depicts the Blockchain architecture. It shows the block structure as well as the chain of blocks. The components of a block have two divisions:

i. Block header
ii. List of transactions

i. The block header is comprising of three components. The first component is the hash code of the previous block which ties the current block with the prior one. The second component is composed of mining statistics that are used to generate the block. The Markle tree root (which is nothing more than the current block's hash code) is the final component, and it serves as the foundation for checking the integrity of all transactions in the block. We

utilize the previous block's hash code to construct the next block's hash code. As a result, if an attacker wants to change the contents of a block, he or she must also change the hash code of the rest of the chain, which is almost impossible. Thus, it makes the Blockchain tampered proof. Nonce, timestamp (recorded time), and mining difficulty are among the mining statistics (Economist, 2015). Merkle tree includes a hash chain of data blocks in which transactions are hashed and attached to leaf nodes, while non-leaf nodes include the Merkle tree's cryptographic hash of its child nodes (Nakamoto, 2008). The Merkle tree is described in Figure 3.

ii. The second component of the block is a list of valid transactions. The block size and transaction size determine the number of transactions in a block. Asymmetric cryptography is used for transaction authorization and authentication. A transaction cannot be deleted or changed once it has been added to the chain. Blocks are chained together, with each block containing a hash of the previous block, resulting in a block chain (Blockchain). If a block is genuine and has proof of work, which is a computationally tough hash generated by the mining method, it will be accepted into the chain. Because it uses a secure hashing technique (such as SHA-256) with safe hash pointers pointing to the preceding hash, it assures that if one of the blocks is changed, all subsequent blocks must be recalculated. The following is a taxonomy of block and Blockchain terms. Fig. 4 shows how the longest chain is accepted and added to the Blockchain, while smaller chains are rejected.

iii. Orphan block: Miners try to mine blocks on their own with the list of transactions that are yet to be added. A miner mines a block and then broadcasts it to all other nodes in the network for verification.

The block with the highest consensus among the many blocks in the network will be accepted for inclusion. Other blocks are referred to as orphan blocks and are eventually discarded by the network. Some transactions in orphan blocks have already been incorporated in the legitimate block that was just added, but

others may have yet to be considered. Further mining operations must account for such transactions.

- **Fork:** All chain other than the valid one is called a fork. A newly mined block may be attached to the orphan chain, preventing it from joining the longest chain. Such connected blocks create a fork.
- **Genesis block**: The genesis block is the first block ever created in the system. In the case of the Bitcoin network, the Genesis Block is the first-ever block mined by creator Satoshi Nakamoto. Any Blockchain system's Genesis Block is also known as Block 0. It is the ancestor of all subsequent blocks in the chain (Home Page, 2012).

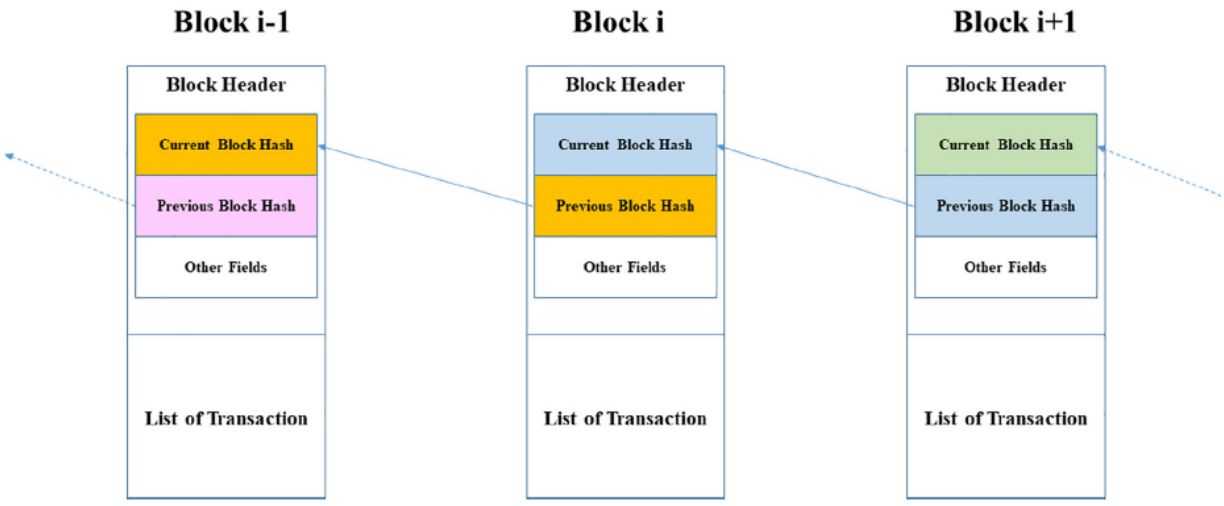


Figure 2: Blockchain Architecture

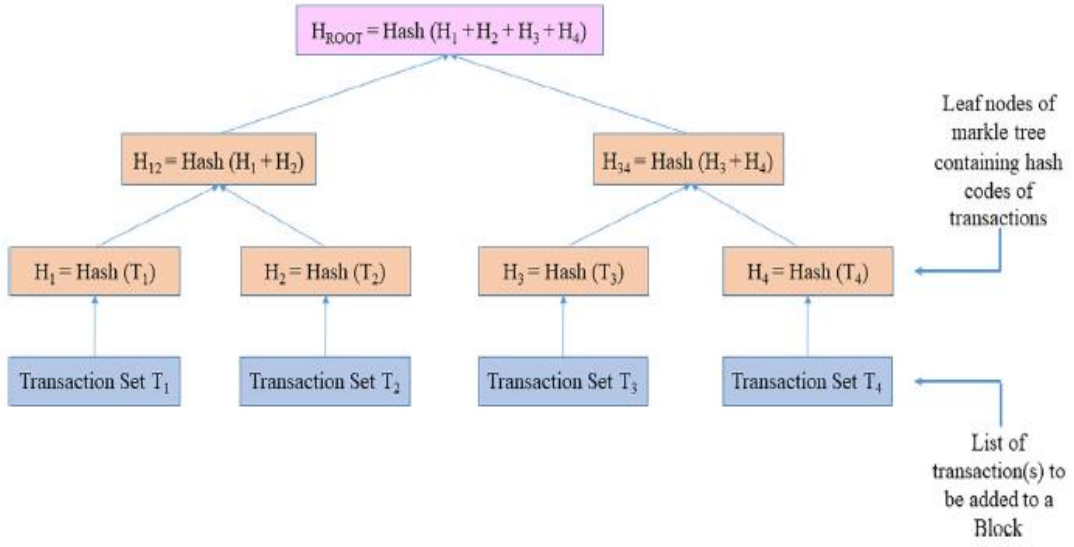


Figure 3: Merkle tree

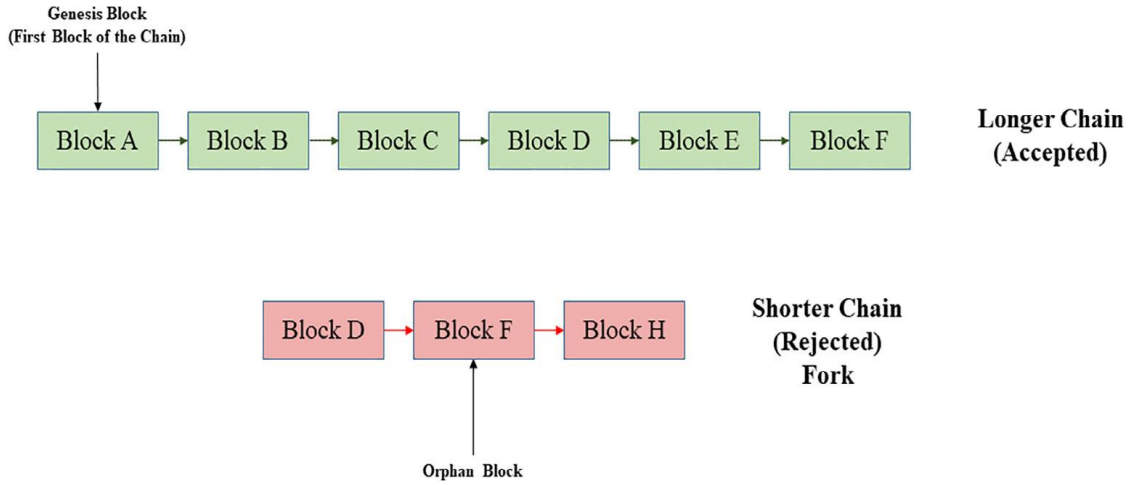


Figure 4: Accepting/Rejecting a Chain.

2.2.2 Categories of Blockchain

The permission model, which determines who can maintain a blockchain network, can be classified (e.g., publish blocks). It is permissionless if anyone can publish a new block. It is permissioned if only certain users can post blocks. A permissioned blockchain network is similar to a restricted business intranet, but a permissionless blockchain network is similar to the public internet, where anybody can participate. Permissioned blockchain networks are frequently established for a consortium, which is a group of companies and individuals.

Permissionless

Permissionless blockchain networks are decentralized ledger platforms that allow anyone to publish blocks without the need for permission from anyone. Permissionless blockchain platforms are frequently open source software that anybody can download for free. Because everyone has the ability to publish blocks, anyone can read the blockchain and conduct transactions on it (through including those transactions within published blocks). Within a permissionless blockchain network, every blockchain network user can read and write to the ledger. Because permissionless blockchain networks are open to everyone, malevolent individuals may try to manipulate the system by publishing blocks in an unauthorized manner. To avoid this, permissionless blockchain networks frequently employ a multiparty agreement or 'consensus' approach that compels users to invest or maintain resources while publishing blocks. This makes it difficult for malicious users to undermine the system. Examples of such consensus models include proof of work and proof of stake methods. Permissionless blockchain networks' consensus methods normally encourage non-malicious activity by paying publishers of protocol-conforming blocks with native coinage.

Permissioned

Permissioned blockchain networks are those in which users who publish blocks must be approved by a third party (be it centralized or decentralized). It is feasible to control read access and who can issue transactions because the blockchain is maintained by only authorized users. Permissioned blockchain networks can either enable anyone to read the blockchain or only allow authorized individuals to read it. They may also allow everyone to submit transactions for inclusion in the blockchain or restrict this access to only approved users. Open source or closed source software can be used to create and maintain permissioned blockchain networks.

Permissioned blockchain networks can have the same digital asset traceability as permissionless blockchain networks, as well as the same distributed, robust, and redundant data storage mechanism. They also employ consensus models for publishing blocks, although these approaches don't always necessitate the expenditure of

resources or their upkeep (as is the case with current permissionless blockchain networks). This is because establishing one's identity is essential to participate as a member of the permissioned blockchain network; individuals who maintain the blockchain have a level of trust with one another, since they were all authorized to publish blocks and since their authorization can be revoked if they misbehave. In permissioned blockchain networks, consensus models are usually speedier and less computationally expensive.

Organizations that require tighter control and protection of their blockchain might use permissioned blockchain networks. Users of the blockchain, on the other hand, will need to have faith in a single body that governs who can publish blocks. Organizations that want to collaborate but don't fully trust each other can use permissioned blockchain networks. They can create a permissioned blockchain network and allow their business partners to record transactions on a shared distributed ledger. Based on how much they trust one another, these organizations can choose the consensus model to utilize. Permissioned blockchain networks enable transparency and knowledge, which can help businesses make better decisions and hold bad actors accountable. This can specifically incorporate auditing and supervision entities, making audits a regular occurrence rather than a one-time affair.

Some permissioned blockchain networks allow users to selectively publish transaction information based on their identification or credentials on the blockchain network. This feature can provide some level of transaction privacy. For example, the blockchain may record that a transaction between two blockchain network members occurred, but only the persons involved have access to the actual contents of the transaction.

To transmit and receive transactions on some permissioned blockchain networks, all users must be approved (they are not anonymous, or even pseudo-anonymous). In such systems, participants collaborate to create a shared business process with built-in disincentives for fraud or other undesirable behavior (since they can be identified). It is clearly understood where the organizations are incorporated,

what legal remedies are available, and how to seek those remedies in the applicable judicial system if bad activity occurs.

2.2.3 Features of Blockchain Technology

A blockchain is distinguished by censorship resistance, immutability, and worldwide usability, and it is maintained by a global network of validators known as miners who earn block rewards known as cryptotokens (Jeremy Gartner, in Shulman, 2018).

Decentralization, according to Vitalik Buterin (2017), guarantees fault tolerance, assault resistance, and collusion resistance. Furthermore, blockchain is decentralized along two of the three axes of software decentralization:

- **Politically decentralized** - implying that no one has authority over it;
- **Architecturally decentralized** - There is no infrastructure central point of failure;
- **Logically centralized** - the system has a single shared state and acts like a single computer.

Anyone can visit a blockchain, download a copy, and participate in its maintenance, thus turning their computer into a node. Edits to the blockchain can only be performed with universal consensus among the persons running a node, and the copy will be actively updated together with every copy on every other node (ConsenSys, 2018).

Mining is the process of using hash verification processes to add a new block (containing thousands of transactions) to a blockchain. In blockchain, the new block is linked to the previous one. The genesis block contains the settings for each blockchain (Dhillon et al., 2017).

The purposed are based on some characteristics, which are presented as follows.

i. **Decentralization**- Blockchain technology does not rely on a centralized transaction system to validate transactions. Cost and performance difficulties arise when central trustworthy agencies are involved. Blockchains rely on encryption and algorithms to maintain data consistency in dispersed networks because a third party is not necessary.

ii. **Persistence**- Validating transactions is quick in blockchain technology. Invalid transactions may be dropped off. Transactions which are already a part of blockchain may neither be deleted nor rolled back. Data tampering could be easily realized.

iii. **Anonymity**- Users interacting with blockchains are assigned system generated addresses. This hides the users identify.

iv. **Auditability**- Transactions in real time rely on previous unspent transactions. As current transaction gets incorporated into the blockchain, the status of unspent transactions changes to spent. This makes it simple to validate and track transactions.

v. **Public Verifiability-** The correctness of the state of system can be confirmed by any user. In systems that rely on central trust agencies, this is not the vase. Users need to engage with the agencies to receive information about the correct state.

vi. **Transparency-** Blockchain data is updated for public verifiability. However, amount of information may be restricted to users depending on their privileges.

vii. **Privacy-** Although privacy is easier to achieve in centralized systems, blockchains with specific protocols can allow certain level of privacy so safeguard sensitive information.

viii. **Integrity-** Blockchain technology protects against unauthorized modifications leading to data integrity. Since the technology provides public verifiability, data integrity may be confirmed by anybody.

ix. **Redundancy-** Blockchain technology relies on decentralized architecture. Unlike centralized systems, which rely on backups and physical servers to achieve data redundancy, data is duplicated across all writers.

x. **Trust Anchor-** Trust anchor is the entity responsible for providing read and write access to a system. They are the highest authorities and they possess grant and revoke rights.

2.2.4 Blockchain Storage Structure

In a blockchain, all valid records of transactions are collected together and stored in groups that are called blocks. A block contains a number of transactions along

with proof of work and the hash of the previous block. Defining the completion of a block depends on its capacity. Mohanta et al. (2019) claim that a block may contain more than 500 transactions and as proposed by Satoshi Nakamoto in 2010 that the average size of a block is approximately 1MB. Each node in the network validate a new transaction that is added to the block and once a block is filled is chained to the existing blockchain. The figure below describes a detailed block in blockchain.

Figure 5: *Block in a blockchain system* (*Inspired by Mohanta et al., 2019)*

A block is composed of two main components, the header of a block and the body that contains a list of transactions. The block's head is separated into five halves,1) *A Nonce is a number that is added to a hashed block in a blockchain to make it difficult to dump when it is rehashed.* A nonce is the number that the miners are working hard to solve (Conti et al., 2018). *2) Data* contains the detailed information of a transaction including the sender and the receiver information, the amount of money to be sent. This part is also very important for the rest of the nodes to validate the transaction. When a node starts a transaction and broadcast it to other nodes in the network to validate it, other nodes base on the old transactions. For instance, a miner looks in the past records to confirm if the sender has the amount of Bitcoins that he wants to send.3) *the root hash of the markle tree,* the transactions in a block are organized in a markle tree structure and can be aggregated in a hash and thus the hash of the current block (Conti et al., 2018). 4) *Hash of the previous block,* blocks are linked cryptographically with a digital fingerprint generated by a hashing function. Blocks are

linked together; a block contains a hash value of the previous block. This is a crucial component that allows a connection between blocks. This is why reversing the blockchain is really difficult.

This system of chaining all the blocks together and a block contains the hash value of a previous block which means that to be able to edit one block, it will require to consult all the previous blocks which have been growing to make a very long chain. Therefore, it becomes more complicated and require a lot of computational power to dump any single block in the chain (Conti et al., 2018). 5) *A timestamp in the block itself, in seconds.* This time allows to determine the exact time in which the block has been mined and validated by other nodes in the blockchain system (Conti et al., 2018).6) Difficult, every hash has a size in bits and the smaller the goal is in the bits, the harder it is to get a matching hash. A hash that has many zeros at the beginning is smaller than the hash without zeros.

2.2.5 Blockchain Technology Security

Blockchain technology allows data to be shared while maintaining transparency. The parties concerned are assured that the information they are working with is error-free and unchangeable. This feature is not only beneficial in the technical domain, but also finds its use beyond that. The following are few reasons that make blockchain technology a favorite in many domains.

i. It ensures transparency: Blockchain technology is an open source technology, such that other users cannot modify it. A blockchain's logged data is impossible to modify, making it a somewhat secure technology. It reduces transaction costs significantly. A blockchain does not need third party to complete peer-to-peer and business transactions. Since no middlemen are involved in the transaction, the process is faster.

ii. Transaction settlements are quicker for blockchain technology as compared to traditional banks which rely on working hours and protocols. The fact that they are in different parts of the world adds to the delay. However, blockchain has no such limitations, allowing for speedier transaction settlements.

iii. It promotes decentralization since there is not central data hub. This allows individual transactions to be authenticated. When information is updated to

different servers, even if the information comes across adversaries, a trivial amount if data will be compromised. Since third parties are no more involved in the transactions, users and developers take the initiative, thus introducing user-controlled networks. Movements of goods, hence leading to transparency. This simplifies several other management processes too. In case of irregularities being detected, one can always trace back to the point of origin, which makes investigations easy for executing required actions. This leads to quality assurance

iv. Blockchain technology eliminates human error since it records data and protects it from being altered. Accuracy is ensured because records are validated as they transit from one node to the next. This ultimately leads to accountability.

v. Smart and Sophisticated contracts can be easily validated, singed and enforced using blockchain technology.

vi. Blockchain Technology eliminates electoral fraud, thus leading to clarity in voting. For Stock Exchanges, the reliability of blockchain technology is being considered. Energy supply can be accurately tracked.

vii. Blockchain technology encourages Peer to Peer Global Transactions. Cryptocurrency transactions are quick, safe, and inexpensive.

viii. Blockchain technology leads to data objectivity. It not only ensures data integrity, but it may also notify users if data is altered. Even if data is breached for an organization, it cannot be used, thus a balance is maintained between security and governance.

ix. Blockchain technology is used to authenticate devices. They may soon replace passwords, thus eliminating human intervention. This is due to the fact that it does not encourage centralized architecture. Because every transaction is digitally time stamped and signed, it emphasizes non-repudiation. Even with the system's new iteration, previous records will be stored in history log. This leads to traceability

2.2.6 Challenges of Blockchain Technology

Despite the benefits of blockchain technology, there are still some issues that need to be addressed. The difficulties are summarized as follows:

i. Blockchain anomalies,
ii. Energy consumption,
iii. Scalability and speed,
iv. Interoperability,
v. Privacy,
vi. Cryptology challenges in the age of quantum computing.

Blockchain Anomalies

Some anomalies may result in the addition of conflicting blocks and the formation of new branches of the chain in PoW based blockchains. In Natoli and Gramoli's study, the conditions that may lead to these anomalies are discussed (Natoli & Gramoli, 2016). This can lead to issues with usability, integrity, and performance (Mohan, 2019). On these conditions, blockchain systems should provide deterministic assurances. These types of anomalies can be solved by adapting implementations and writing smart contracts (Natoli & Gramoli, 2016).

Energy Consumption

Traditional PoW-based blockchain mining activities necessitate expensive hardware and a significant level of energy usage (Flipo & Berne, 2017; Trautman & Molesky, 2019). Energy-efficient blockchain solutions are being tested to replace or reduce the use of traditional PoW-based blockchain systems. Various node selection algorithms are offered, depending on random selection or the amount of cryptocurrency mined by the miners (Rosic, 2017).

POS consensus protocol has started to be preferred in cryptocurrency implementations instead of the PoW approach. To become a trusted validator, nodes must deposit a predetermined amount of cryptocurrency and demonstrate their commitment to the system. The system does not require a calculation-based competition; instead, it selects validators at random. The likelihood of being chosen is related to the quantity of cryptocurrency held. With POS, the system will use significantly less electricity and be lot faster (Sayeed & Marco-Gisbert, 2018; Opray, 2017).

Current enterprise blockchain frameworks, such as Hyperledger and R3 Corda, are token-free platforms that save energy by eliminating this time-consuming process. Hashgraph, Holochain, and Tangle, among other blockchain variants, are also energy-efficient and resource-friendly DLT systems.

Scalability and speed

The ability to handle massive volumes of transactions at rapid speeds is referred to as scalability. This is largely determined by the following variables:

- *Consensus*: The nodes must agree on the transaction's legitimacy. In traditional cryptocurrency systems, adding information to a block using the POW consensus protocol is a relatively slow process. In Bitcoin, creating a block can take anywhere from 10 to 60 minutes (Bitinfocharts, 2019); in Ethereum, it takes roughly 15 seconds (Etherscan, 2019). In a normal blockchain network, all new blocks are broadcasted and validated by all nodes.
- *Storage:* Storage capacity is the most important consideration when deploying blockchain. The exponential increase in block size causes a performance issue. Many techniques make it impossible or impractical to keep all of the data in each node.

This brings out the scalability problem since the broadcast traffic and the size of the ledger data stored in the nodes increases exponentially because of the nature of the blockchain architecture. Furthermore, lightweight devices such as the Internet of Things (loT) lack the necessary resources. Many solutions have started to use all nodes for transaction validation and only a few (full nodes) for data storage. Only storing the summary or link of the data in the nodes is also being implemented, as is keeping the data in the DSN architecture. The co-founder of Ethereum, Vitalik Buterin, once stated that a blockchain solution can only contain two out of the three basic features (decentralization, security and scalability). This is also called the scalability/blockchain trilemma, which is shown in the Figure below. In order to tackle the scalability challenge, decentralization and security will be sacrificed (Gomez, M., 2017).

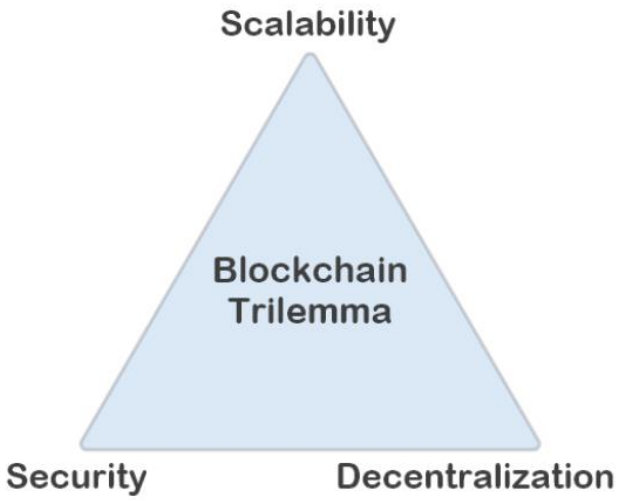


Figure 6: Scalability/Blockchain Trilemma

Interoperability

In recent years, blockchain infrastructure interoperability has emerged as a new problem for the blockchain community. Users of different blockchain systems cannot readily move digital assets between each other without requiring an intermediary, despite the fact that blockchain technology was created and established to eliminate intermediaries and trustworthy third parties. For example, if a user wishes to transfer data or a digital asset from a Hyperledger Fabric network client to an R3 Corda network client, the user must first register with the Hyperledger Fabric network, then decrypt the secured data, and then register on R3 Corda to use this network's functionality and put the aforementioned data into R3 Corda network. This is a huge waste of time and resources. Interoperability of multiple blockchain designs, even between different firms or industries, becomes a need.

In the near future, different blockchain systems will be able to communicate and transfer digital assets. Cross-transactions should be enabled using mechanisms like QuickX. Sidechains have been presented as a promising means for transferring data between blockchains. It is not only a DLT technology, but also a possible architecture for enabling blockchain technology interoperability (Ray, 2018).

Privacy

Another difficult issue that arises from the nature of the blockchain technique is privacy. All participants in a permissionless blockchain architecture have the right to

download the ledger, which means they can look through the whole history of recorded transactions. In these infrastructures, implementing "the right to privacy" is difficult. When working with PII, extra caution is required (Personally Identifiable Information). It is best not to store personally identifiable information (PII) on the blockchain and instead allow users to manage their own data.

To ensure anonymity, Zero Knowledge Proof (ZKP) can be included into blockchain systems. The user can have complete control over his or her data. Any process (such as an identity check) can be validated with ZKP without providing any information about it (Goldreich, 2019; Korkmaz et al., 2019).

Cryptology challenges in the age of Quantum Computing

The security of conventional public-key-based algorithms and blockchain systems is jeopardized by quantum computing and the parallel processing power it promises. Quantum computing is a revolutionary technique that can be used to decrypt ciphers and reveal secrets protected by conventional cryptographic algorithms (Piscini et al., 2018). By simply raising the associated key sizes, symmetric algorithms appear to be secure against quantum computers (and Grover's algorithms). RSA, DSA, Diffie-Hellman Key Exchange, ECC, ECDSA, and other widely used public-key cryptographic algorithms (based on integer factorization and discrete log problem) will be vulnerable to the Shors method and won't be safe any longer (Cromwell, 2015).

Researchers are looking towards post-quantum blockchain (PQB) systems and safe cryptocurrency schemes based on them that can withstand quantum computer attacks. This is currently a work in progress (Gao et al., 2019).

2.2.7 Privacy Challenges of Blockchain

A. Identity privacy challenge

The relationship between the user's real identity and the blockchain address is referred to as identity privacy. The data saved on the blockchain is unchangeable. It is stored on the chain in the form of distributed ledger. The chain can provide comprehensive information to any node. Although transactions on the blockchain have certain anonymity, with the development of compute technology, anonymity cannot

fully protect the privacy of user identity. By monitoring and assessing the significance of public data in the global ledger, an attacker can discover sensitive information. If there are stable connected transactions between multiple addresses, for example, the attacker can study the transaction relationship graph between the addresses and infer some data about the user (Ron & Schar, 2013). Furthermore, the attacker can infer the user's identity and geographical information by searching all potential transactions with an estimated balance for the associated transaction address (Fleder, 2015).

B. Transaction privacy challenge

The transaction records kept in the blockchain and the potential information underlying the transaction are referred to as transaction privacy. Encryption is a common information security solution that prevents an adversary from stealing or interfering with the data. However, it is vital to verify that transaction information is not taken by unauthorized nodes in the process of encrypting transaction information in blockchain. On the other hand, verifying the transaction's legitimacy without releasing sensitive information is important, and the transaction content cannot be totally encrypted. There are inconsistencies between them, as well as hurdles and difficulties in privacy protection technologies.

To summarize, blockchain technology cannot guarantee complete privacy protection for consumers. To achieve blockchain privacy protection, various privacy protection algorithms, protocols, or other measures must be implemented (Liu, 2019). As a result, blockchain privacy and security issues should receive more attention.

2.3 Blockchain Security Issues

The architecture of blockchain consists of six layers. However, as we have explained in the previous section, this thesis will focus on four layers. These layers are application layer, layer, network layer and data layer. The data layer consists of data blocks, chain structure, timestamp, hash functions, Markle tree, and digital signature (Rui Zhang et al., 2019). In comparison to other layers, the network and data layers are more vulnerable to security assaults. Time Hacking attacks, selfish-mining, >50%’ Attack and double spending attacks happen on the data layer. Other layers, such as the application layer, may be vulnerable to other attacks, such as attacks on the wallet

software. Chen et al. (2019) analyze financial losses caused by Denial of Service attacks, which target the network layer with the goal of disrupting the system by injecting malicious attacks that consume the majority of the system's computational capacity. One example is in 2016, approximately US$60M was stolen due to DAO (Decentralized Autonomous Organization) attack in ethereum. Despite the various benefits that this blockchain is offering the society and changing people's lives in many different ways, further enhancement is still needed on its security area. This thesis aims to conduct a study on the impacts of blockchain technologies in the field of information security and privacy.

2.4 Information Security of Blockchain Technology

All users of information systems should practice information security. Blockchain systems involve sensitive information such as users' transaction information which requires security measures to protect such information against unauthorized access. Blockchain is a technology that works over the internet. It involves the virtual communication between the participants of the network. It is rare to find a technology that involves the use of the internet without security problems. Li et al. (2020) examine popular blockchain systems and discuss real attacks observed in those systems. IA triad is a known security model that defines security data objectives namely confidentiality, integrity and availability. And these are the core fundamentals in ensuring the security of information Samonas and Coss (2014). The information security objectives are explained based on bitcoin as the first implemented project behind this technology. Rui Zhang et al. (2019) examined the security properties and needs that must be implemented in blockchain technology to avoid a variety of system threats.

i. ***Confidentiality of transactions*:** Data and derived represented information must be protected in a way that only authorized people can have access to them. Users Transaction information cannot be accessed by unauthorized users. The system must guarantee the consistency and security of the data.

ii. ***Integrity of transactions*:** Accuracy and completeness of the data. Transactions involved in online decentralized systems include asset management, vehicle registrations, warehouse receipts and other assets are managed by different intermediaries. This leads to the risks of faking the certificates, thus data must not be manipulated or misused by unauthorized people.

iii. ***Availability of system and data*:** The participants of the network should be able to access the system and the data of transactions at any moment, anywhere. The system must guarantee the availability of data to authorized people only.

iv. ***Consistency of the Ledger across participants*:** The processes that are involved in the system between involved financial institutions, inconsistencies between ledgers kept by different financial institutions in the network are caused by variances in architecture and business procedures.

v. ***Prevention of double spending*:** This a major issue in the blockchain system. For instance, a single coin may be sent more than once. To overcome this problem, security methods must be installed.

vi. ***Anonymity of users' identity*:** Sharing user data among different financial institutions in a secure manner is expensive due to the repeated user authentication. This leads to the disclosure of user's information by some intermediaries. The system has to ensure that the users' information is only accessed by authorized users.

vii. ***Unlinkability of transactions*:** User's transaction information should not be linked to each other because once all the transactions related to a user are linked. Thus, it is easy to figure out other information about the user.

2.5 Privacy and Information Security Techniques used In Blockchain

The following are techniques that can be leveraged to enhance the security and privacy of existing and future blockchain systems.

1. Mixing

Users' anonymity is not guaranteed by Bitcoin's blockchain: transactions are made with pseudonymous addresses and may be validated publicly, thus anybody can link a user's transaction to her prior transactions by looking at the addresses she used to make bitcoin swaps. More significantly, when a transaction's address is

connected to a user's real-world identity, all of her transactions may be exposed. As a result, mixing services (or tumblers) were created to keep users' addresses separate. Mixing, literally, is a random exchange of a user's money with the coins of other users, obscuring the observer's ownership of coins. However, these mixing services does not provide protection from coin theft.

a. **Mixcoin:** Bonneau et al. proposed Mixcoin (Dave, 1993) in 2014, which allows anonymous payment in Bitcoin and bitcoin-like coins. Mixcoin enables anonymity akin to existing communication mixes to protect against active adversaries. Furthermore, Mixcoin employs an accountability mechanism to identify stealing, demonstrating that by matching incentives, users will use Mixcoin rationally without stealing bitcoins.
b. **CoinJoin**: CoinJoin (Gregory, 2013) is proposed in 2013 as an alternative anonymization method for bitcoin transactions. It is inspired by the concept of shared payment. If a user wants to make a payment, she will identify another user who also wants to make a payment, and the two of them will negotiate a joint payment in one transaction. The possibility of correlating inputs and outputs in one transaction and tracing the exact direction of money movement of a single user is considerably reduced by the joint payment. Users must discuss transactions with whom they desire to make joint payments with CoinJoin. The initial generation of mixing services (such as SharedCoin Moniz, 2006) relied on centralized servers and required customers to trust that the service operator would neither steal nor enable others to steal their bitcoins. Despite the single point of failure, centralized systems may expose users' personal information because they would preserve transaction logs and track all joint payment participants. Furthermore, poor implementation of the CoinJoin protocol will reduce anonymity. Kristov Atlas identified such flaw in the SharedCoin mixing service (Moniz, 2006) and provided a detailed analysis of the flaw in (Kristov, 2014), In (Kristov, 2014), Kristov Atlas created a tool called "CoinJoin Sudoku" (Kristov, 2014) that could identify SharedCoin transactions and discover associations between specific payments and payees,

demonstrating that the SharedCoin mixing service is unable to ensure strong transaction privacy.

CoinShuffle (Tim, 2014) was proposed by Tim Ruffing et al. in 2014, which further extends the CoinJoin concept and increases privacy by avoiding necessary of trusted third-party formixing transactions. CoinShuffe is described as a truly decentralized coin-mixing technology with the capacity to prevent theft. To ensure anonymity, CoinShuffle uses a novel accountable anonymous group communication protocol, which is called Dissent.

2. **Anonymous Signatures**

Digital signature technology was developed several variants. Some signing techniques have the ability to provide anonymity to the signer. This kind of signature schemes are called anonymous signature. The two most essential and typical anonymous signature techniques are group signature and ring signature, both of which were proposed previously.

a. Group Signature: Group signature is a cryptography scheme proposed initially in 1991 (Lin Chen, 2017). Any member of a group can use her personal secret key to sign a message for the entire group anonymously, and any member with the group's public key can check and validate the generated signature and confirm that the signature of some group member was used to sign the message. The procedure of signature verification exposes nothing about the signer's genuine identity other than the group's membership.

A group manager oversees the process of adding members to the group, resolving disagreements, and revealing the original signer. It is also required that an authority entity in a blockchain system has to form and cancel groups, as well as dynamically add new members to the group and delete/revoke membership of specific participants. Since the group signature requires a group manager to setup the group, group signature is suitable for consortium blockchain. Recently, JUZIX added group signature in its platform for providing users with anonymity support.

b. Ring Signature: Ring signature (Ronald, 2017) also can achieve anonymous through signing by any member of a group users. The term "ring signature"

refers to a signature algorithm that employs a ring-like structure. If determining which member of the group uses his or her key to sign the message is difficult, the ring signature is anonymous. Ring signatures differ from group signatures in two principal ways: First, because there is no group management in a ring signature scheme, the genuine identity of the signer cannot be exposed in the event of a disagreement. Second, without any further preparation, any user can create their own "ring." As a result, ring signature can be used on a public blockchain. One of typical applications of ring signature is Cryptonote (Nicolas, 2012). It uses ring signature to conceal the connection between transaction sender addresses. More precisely, Cryptonote constructs the sender's public keywith several other keys, so that it impossible to identifywho actually sent (signed) the transaction. Due to the use of ring signature, the likelihood that an adversary would successfully predict an actual sender of a transaction is 1/n if the number of ring members is n. In 2015, Ethereum adopted ring signature, which provides users with anonymity similar to Cryptonote currencies like Monero.

3. **Homomorphic Encryption (HE)**

Homomorphic encryption (HE) is a powerful cryptography. It may conduct specific sorts of computations directly on ciphertext and guarantee that operations done on the encrypted data, upon decrypting the computed results, produce the same results as operations performed on the plaintext. There are several partially homomorphic crypto-systems (Pascal, 1999) as well as fully homomorphic systems (Craig, 2009).

Homomorphic encryption algorithms can be used to store data on the blockchain without affecting the network's features. This assures that the data on the blockchain is encrypted, which alleviates the privacy problems that come with public blockchains. The use of homomorphic encryption protects data privacy and enables for easy access to encrypted data through the blockchain for auditing and other uses like controlling employee costs. For better control and privacy, Ethereum smart contracts use homomorphic encryption on data stored on the blockchain.

4. **Attribute-Based Encryption (ABE)**

Attribute-based encryption (ABE) is a cryptographic approach in which attributes are used to define and regulate the ciphertext encrypted with a user's private key. If the user's attributes match the ciphertext's attributes, the encrypted data can be decrypted using the user's secret key. ABE's collusion-resistance is a critical security feature. It ensures that when a malicious user collude with other users, he cannot access other data except the data that the can decrypt with his private key.

The concept of attribute-based encryption was proposed in 2005 (Amit, 2005) with single authority. Since then, a number of extensions have been proposed to the baseline ABE, including ABE with multiple authorities to generate users' private keys jointly (Jung, 2015), ABE schemes that support arbitrary predicates (Sergey, 2013).

Despite the fact that attribute-based encryption is extremely effective, few apps have used it to date due to a lack of understanding of both core concepts and efficient implementation. So far, ABE has not been deployed in any form on a blockchain for real-time use. In 2011, a decentralized ABE scheme was proposed (Allison, 2011) to employ ABE on a blockchain. Permissions, for example, might be represented on a blockchain by access token ownership. All nodes in the network will have access to the specific rights and privileges associated with the token if they have been issued one. The token allows the authoritative body that distributes the token to track who possesses particular traits, and this tracking should be done in an algorithmic and consistent manner. Tokens should be utilized as non-transferable quantifiers of reputation or attributes, similar to badges that reflect attributes or certifications.

In (Allison, 2011), it is shown that there is no need of a fixed authority to do attribute-based encryption. Multiple authority can work together in a decentralized network to achieve the same goal. For instance, relying on witnesses for the role of these authorities may be possible in a blockchain, with technologies, recently made possible, such as Steemit, Storj, IPFS, SAFE Network, though implementing attribute-based encryption via a blockchain approach is still a work in progress.

5. Secure Multi-Party Computation

The multi-party computation (MPC) model provides a multi-party protocol that allows them to do a calculation jointly over their private data inputs while maintaining

their input privacy, so that an adversary learns nothing about an authentic party's input but the joint computation's outcome.

Andrew Yao formally defined secure two-party computation in 1982 (Yao, 1982) and generalized it in 1986 (Andrew, 1986) for the Millionaires' problem. Goldreich et al. proposed a generalization of the two-party computation to the multi-party computation in 1987 (GoChain, 2018), assuming that all inputs of the computation and zero-knowledge proofs are parts of secret sharing. Many later and increasingly efficient MPC methods have been built on this generalization. MPC has been a preferred solution to many real-world issues due to its success in distributed voting, private bidding, and private information retrieval. The first large-scale deployment of MPC was in 2008 for an actual auction problem in Denmark (Peter, 2019).

MPC has been utilized in blockchain systems to secure users' privacy in recent years. Andrychowicz et al. designed and implemented secure multiparty computation protocols on Bitcoin system in 2014 (Marcin, 2014). Without any trusted authority, they devised protocols for secure multiparty lotteries. Their protocols ensure that honest users are treated fairly, regardless of how dishonest others act. If a user breaks the protocol or interferes with it, she is considered a loser, and her bitcoins are transferred to the honest users.

Zyskind et al. presented Enigma, a decentralized SMP computation platform, in 2015. (Zyskind, 2015). Enigma ensures the secrecy of its computational model by using an enhanced form of SMP computation and a verifiable secret sharing method. Enigma also uses a modified distributed hash table to store shared secret data efficiently. Furthermore, it makes use of an external blockchain as a non-corruptible record of events and as the network's regulator for identity management and access control. Enigma, like the Bitcoin system, allows users to control and safeguard their personal data without the need for or reliance on a trusted third party.

6. Non-Interactive Zero-Knowledge (NIZK) Proof

Another cryptographic technology that has powerful privacy-preserving properties is zero-knowledge proofs, proposed in the early 1980s (Goldwasser, 1985). The core notion is that a formal proof may be developed to verify that a program

executed with some private input known only to the user can create some publicly available output with no other information being disclosed. In other words, a certifier can show a verifier that an assertion is correct without supplying the verifier with any valuable information.

As a variant of zero-knowledge proofs, it is shown in (Manuel, 1988) that, with the non-interactive variant of zero-knowledge proofs, coined as NIZK, if the certifier and verifier share a common reference string, computational zero-knowledge can be achieved without having the certifier and verifier to interact at all. All account balances in a blockchain application are encrypted and saved in the chain. When a user sends money to another user, he can easily demonstrate that he has adequate balance for the transfer using zero-knowledge proofs while keeping his account balance hidden.

Another variation is the zero-knowledge Succinct Non-interactive ARgument of Knowledge (zk-SNARK) proof, introduced in 2012 by Bitansky and his coauthors (Bitansky, 2012) and is served as the backbone of the Zcash protocol (Eli, 2014). zk-SNARKs are used by Zcash to verify transactions while maintaining user privacy.

The Zcash group recently improved the Ethereum contract language to make zk-SNARK proofs verification more efficient. They added a snark-verify precompile (which works like an opcode) to a fork of "Parity" that uses lib-snark to verify generic proofs. They also employed the new zk-SNARK verifier to enforce a unique currency mixing contract that uses a reduced version of Zerocash, an academic protocol whose implementation is used to develop Zcash. As a result, it's known as "baby" Zoe, which stands for Zerocash over Ethereum. By inserting a "serial number" as a commitment into a Merkle tree, which is maintained by the contract, a user can store discrete amounts (ETH units).

7. The Trusted Execution Environment (TEE) Based Smart Contracts

TEEs provide a completely isolated environment for application execution, thereby preventing other software applications and operating systems from tampering with and learning the state of the program running in them. The Intel Software Guard eXtensions (SGX) is an example of a TEE implementation technique. For example, Ekiden (Raymond, 2018) is a SGX based solution for confidentiality-preserving smart contracts. Ekiden separates computation from consensus. It employs a remote

attestation protocol to validate the execution correctness of compute nodes on chain after performing smart contract computation in TEEs on compute nodes off chain. The consensus nodes are used for maintaining the blockchain and do not require to use trusted hardware. Enigma (Zyskind, 2015) utilizes TEE in its current version to allow users to create privacy-preserving smart contracts using a decentralized credit scoring algorithm. The number and types of accounts, payment history, and credit utilization are all weighted in credit rating.

8. Game-Based Smart Contracts

The game-based solutions for smart contracts verification are very recent developments, represented by TrueBit and Arbitrum. TrueBit uses an interactive “verification game" to decide whether a computational task was correctly performed or not. TrueBit compensates players for checking computation jobs and finding errors, allowing a smart contract to do a computation work securely and with verifiable attributes. Furthermore, the verifier iteratively checks a smaller and smaller fraction of the calculation in each round of the "verification game," allowing TrueBit to drastically minimize the computational burden on its nodes.

Arbitrum has designed an incentive mechanism for parties to agree off-chain on the behavior of virtual machines, so that it only requires the verifiers to verify digital signatures of the contracts. Arbitrum has created an efficient challenge-based mechanism to identify and penalize dishonest actors that try to lie about the behavior of virtual machines. Smart contracts' scalability and privacy have considerably improved thanks to the incentive mechanism of off-chain verification of virtual machine behavior.

2.6 Benefits of Blockchain Technology

The following are some of the benefits of blockchain technology (Grech and Camilleri, 2017):

- **Self-sovereignty** - users identify themselves and retain control over the storage and management of personal data;
- **Trust** - the technical architecture allows for secure transactions (payments or certificate issuance).

- **Transparency and provenance** - to conduct deals with the knowledge that each side has the financial means to do so;
- **Immutability** - records are written and stored indefinitely, with no way of changing them;
- **Disintermediation** - to manage transactions and retain records, there is no need for a central regulating body;
- **Collaboration** - the ability for parties to conduct business directly with one another without the involvement of third parties.

The biggest disadvantages are the high hardware, energy, and time requirements of the mining operation, as well as the complexity and difficulty of understanding the technology. Furthermore, the multitude of development platforms in constant release, as well as the novelty of associated languages, retain blockchain implementations as the domain of geeks, akin to sending e-mails using line commands at the dawn of the internet. As a result, more user-friendly GUIs and tools are required for blockchain to become widespread. As underlined by Atchley (2018), blockchain needs to overcome its usability problem in order to impact on the everyday lives of people. According to the "Trust in Technology" report, blockchain is the least heard about due to usability and understanding concerns (HSBC, 2017).

Greenspan (2015) outlined specific requirements for implementing a decentralized solution and avoiding "pointless blockchain projects," including the need for shared databases with multiple writers, transaction interactions, operating in the absence of trust, and the absence of a trusted intermediary; in all other cases, a regular database (Oracle, SQL Server, MySQL, Postgres, or NosQL) should be used.

According to (Atchley, 2018; Baker Mills, 2017), some issues to consider when building blockchain goods are:

- Interviewing, surveying, and usability testing target people; designing for trust: a transparent product's information architecture is essential for acquisition, retention, and developing trust;
- Visual consistency: for the product interface, a clear visual style, familiar vocabulary, flow, and functions are required.

- Constant and consistent feedback, active guidance to users because of the long duration of validation and confirmation transactions on a blockchain network.

Instead of being followed, the blockchain technique allows electronic data to be disseminated. This circulated record gives straightforwardness, trust, and information security.

Inside the money exchange, the blockchain configuration is being used frightfully intensively. However, this idea is currently employed not only for cryptographic forms of money, but also for record keeping, enhanced functionality, and sensible contracts.

2.7 Empirical Review

The growing interest in disruptive technologies, such as blockchain, has prompted research to determine the current state of the art. Consider several ways that are comparable to the goal being presented, but have significant variations, either in terms of application areas or the issues they aim to answer. The incorporation of sensor networks into blockchain technology has been discovered, particularly in recent research, as a way of taking use of the benefits it offers in terms of security, traceability, transparency, and immutability.

The study (Bernal Bernabe, 2019) is a systematic review of the privacy challenges in blockchain, with the main contributions being to identify and categorize the main privacy challenges in blockchain, as well as to develop a systematic review of the main techniques in privacy preservation and solutions for blockchain, including a taxonomy that categorizes the main techniques used. It also covers various study suggestions and analyses of the major possibilities, such as cryptocurrencies, health, smart cities, IoT, and e-Administration. This research demonstrates some of the challenges that blockchain faces in adapting to the GDPR.

The study conducted in (Casino, 2019) takes the perspective of application blockchain-based applications in multiple domains such as supply chains, business, health, IoT, energy, education or data management. It's a review of the literature that culminates in a description of blockchain technology. Its goal is to categorize the many blockchain applications in various industries and to discuss how blockchain technology may be used to produce value in these industries while considering their limits. In

terms of their interaction with blockchain, business and industrial sectors were the most investigated in 2018, followed by IoT, governance, and data management. The deployment of blockchain technology in the education and banking sectors, on the other hand, has received the least attention. The study sees an opportunity for improvement in terms of privacy and security by using blockchain and the capabilities it provides, such as safe transactions and anonymity.

It also addresses the issue of the blockchain protocol's energy sustainability, as well as the high energy consumption required for its operation and the necessity to identify alternative protocols that are more energy efficient. Regarding the issue of privacy and security on blockchain for data management, according to the author, privacy and confidentiality are still a concern for blockchain because information is stored on a public ledger and the solutions used, such as pseudonyms, do not provide enough assurance. In actuality, pseudonymisation is a strategy for reducing the link between a data set and the original identity to which it belongs, rather than an anonymization method. According to the author, this technology has yet to mature enough to be employed in circumstances where traditional databases are used, and that it does not yet compensate them for including blockchain.

According to (Thomas, 2019), blockchain technology can be used to improve IoT devices and apps. Because of bandwidth constraints, scalability issues, and expensive consensus procedures, the original blockchain topology is challenging to employ in IoT. To address these limitations, this paper presents a lightweight scalable blockchain model (LSB) that increases transaction trust while reducing transaction processing time.

It divides blockchain approaches into permissionless and permissioned, analyzing their benefits and drawbacks. In the health area, the authors found it financially impossible to use blockchain to store medical data for millions of patients, which is understandable given that it was built for modest transactions in the first place. They see it as a disadvantage that they can't delete a patient's records once they've been added to the blockchain, as the GDPR requires. Most data, on the other hand, has its own life cycle, and it is no longer required to store information that is no longer useful. When considering blockchain as a solution in the health field, the solution outside the

chain appears to be the most plausible, but it should be highlighted that because blockchain can only examine the security of data stored within it, the necessity to secure data outside the chain arises. As a result, it believes that medical data encryption, as well as secure key storage, are essential. When implementing security and privacy protection, it examines the necessity of dealing with sensitive information, such as medical data, to ensure the data's confidentiality, integrity, and validity. Although blockchain is a new paradigm with advantages over existing technologies, there are still challenges to be overcome and more medical data management research to be done.

Blockchain architecture, consensus techniques, applications, trade-offs, and problems are the topic of this study (Monrat, 2019). It investigates it use in health, the energy industry, the stock exchange, voting, insurance, identity management, and trade finance. The current regulatory issues, as well as the fact that there is no international model for crypto-currency, are deterrents to its adoption. We expose some of blockchain's vulnerabilities in the face of a potential attack in this paper, which exposes users to cybercrime. The 51 percent attack occurs when one or more malevolent entities gain control of the majority of blockchain nodes, allowing them to reverse transactions by incurring double costs and preventing other miners from verifying the transaction. It leaves issues like security, privacy, scalability, and energy consumption open to further examination, as well as factors that need to be fixed or enhanced.

By paying attention to the use of the blockchain for IoT (Fernandez-Carames, 2018), we can see the growth in the number of IoT devices and the challenges that arise in order to take advantage of the technology. The notion of Blockchain-based IoT (BIoT) emerges, with its architecture proposed and revised. Blockchain is not always the best solution for every situation; it is a matter of determining which of the following characteristics are required for its application in IoT: decentralisation, peer-to-peer exchange, payment systems, sequential public transactions, robust distributed system, and micro-transaction collection. The term "Internet of Things" encompasses a diverse set of applications. It is feasible to improve the low security level of IoT devices using blockchain. The issue of privacy in the IoT is constrained by the device's

resource limitations, which do not always allow for the development of the computing burden required by blockchain.

Furthermore, due to the consumption required by the mining process, energy efficiency in IoT devices is another weak point when it comes to blockchain integration. In terms of hashing algorithms, Script, also known as X11, is faster and uses less energy throughout the mining process. However, the Internet of Things is still in its early stages, and more study is needed to improve several elements. Because power and computing limitations make it difficult for IoT devices to participate directly in the blockchain, the authors of (Yao, 2020) propose a cloud computing service to free IoT devices from complex tasks that require computing power, followed by a model in which the miners and the cloud provider both participate in the blockchain. The authors of (Fan, 2020) focus on the challenges that the Industrial Internet of Things (IIoT) and cloud service providers face in preserving the security and privacy of data collected by sensors.

It implements smart contracts with Ethereum to ensure the security of the information, taking advantage of the blockchain's qualities such as transparency and immutability. Based on a cryptographic solution, (Jangirala, 2020) combines blockchain technology with IoT to create a private blockchain because the data collected through consumers' smart meters is private and confidential, as well as storing transactions encrypted with the service provider's public key, so that they can only be decrypted by the service provider, the receiver of the information contained in the transaction. The emergence of 5G technology in conjunction with the IoT represents a possible solution to the need for sufficient bandwidth to ensure secure real-time data operations on goods in transit in supply chains, where (Bera, 2020) it proposes an access control protocol based on blockchain, which supports several security and functionality features in addition to communication and computing efficiency.

CHAPTER III

Methodology

3.1 Research Design

This chapter focuses on the methodology approached to conduct this thesis. It discusses each and every step taken and work that led to get all the necessary information that was required to achieve the objectives of this thesis.

3.2 Research Process

A literature review is a compilation of previously published material in a certain field, as well as information in that field from a specific time period. In order to do a thorough literature review, you'll need to locate relevant papers on the subject matter you're researching. Methods for accomplishing project goals must be clearly outlined to provide a well-structured and effective thesis. The same is true when performing a literature review. Okoli and Schabram (2010) provide a comprehensive overview of the literature review method in their work, "A Guide to Conducting a Systematic Literature Review of Information Systems Research." This argument is based on Okoli and Schabram's explanation of the process (2010).

3.3 Research Approach

Finding the right research approach is the most critical phase in any investigation. After considering the study questions and objectives, the next step will be taken. This thesis will be conducted using a qualitative research strategy based on a systematic review. It is a meta-analysis that is part of a systematic review. It aims to acquire all of the relevant information to address a certain research topic. The authors devised criteria for selecting whether evidence should be included or excluded before commencing the systematic review. There is less chance of bias and more reliable outcomes as a result of this method.

3.4 Drafting Protocol

A protocol is a plan that centres around the entire steps to follow when conducting a literature review (Okoli and Schabram, 2010). It is worthwhile to have

such a plan before commencing a research as it keeps the researcher organized and displays the entire workflow. As per Okoli and Schabram (2010), drafting protocol stage involves two steps including drafting the research question and creating a research protocol.

3.5 Creating a Research Protocol

After having a clear and concise research question, the next step which is very essential is to have a clear path towards answering the research question (Okoli and Schabram, 2010). The protocol provides a solution to the question of "where to look for literature" i.e. involves the locations to be searched for the literature and the criterias/standards a literature must meet in order to be considered for the inclusion which will be described in the practical screen and search for literature sections respectively. Okoli and Schabram (2010) discuss two important techniques, note-taking and reviewing techniques are helpful for the reviewer to handle the workflow by drawing the connections between literature and to remember the criteria for future inclusion.

Linear notes as one that use headings and subheadings to distinguish between main ideas and subsidiary information methods were opted in this research. Note-taking technique was used after the literature consideration for the inclusion in order to have notes about the main concepts stated in the selected literature for easy track of work.

3.6 Data Extraction

Data extraction is an important phase that lead to get the data needed to answer the research question. Webster & Watson (2002) discuss the concept-centric approach that helps to synthesize the literature when the reading is done. Concept matrix was opted to help identify the concepts that are relevant to the topic in each of the selected articles.

3.7 Appraise Quality

The selected literature must meet some quality standards to be considered vital to the thesis or research at some extent more than others in a review. It is important to

rate the quality of the articles to be used as a basis foundation in the final results. Okoli and Schabram (2010) recommend a standard form to be based on when examining the quality of a paper. Some standards considered are defined 1) The articles that are more considered than the others must have close content relevance to the topic.2) The used methodology to conduct the research must be reliable.3) The research question must be clearly stated in the article to be able to identify the relevance to the topic.

3.8 Synthesis of the Literature

Before starting reporting and writing the review, synthesizing the literature is greatly important. Once all selected articles have been read and concepts are duly identified in each of the selected articles. The next step is to evaluate the resulting concepts, aggregating, discussing, organizing and comparing the papers which results in a complete and wholly combination of information from the selected articles (Okoli and Schabram, 2010).

3.9 Writing the Review

Writing the review is the final step in performing a literature review. This stage involves reporting the findings and writing the review. The most essential thing to do at this stage is to make sure that all the processes used from getting the literature review to getting all information need to do the analysis must be well documented. In this thesis, the selected literatures were obtained from different online databases such as IEEE Xplore, google scholar, Science Direct, ACM digital library, online university library and springer link. All the literature found based on key words defined were examined according to inclusion criteria. The final selected papers were relevant to answer the research question as the expected main outcome of this study. Webster argue that a literature review is a concept centric which simply means that concepts identified in each article must also be discussed along with their respective papers in the results sections.

CHAPTER IV

Findings and Analysis

4.1. Statistics of Selected Literature

A systematic review would not be complete without a search for relevant material. As previously noted, defined keywords were used to search the relevant databases. There were 93 publications found in total, however only 20 were determined to be related to the research issue and were reviewed. The diagram below shows how we arrived at the final total of 20 articles for the review.

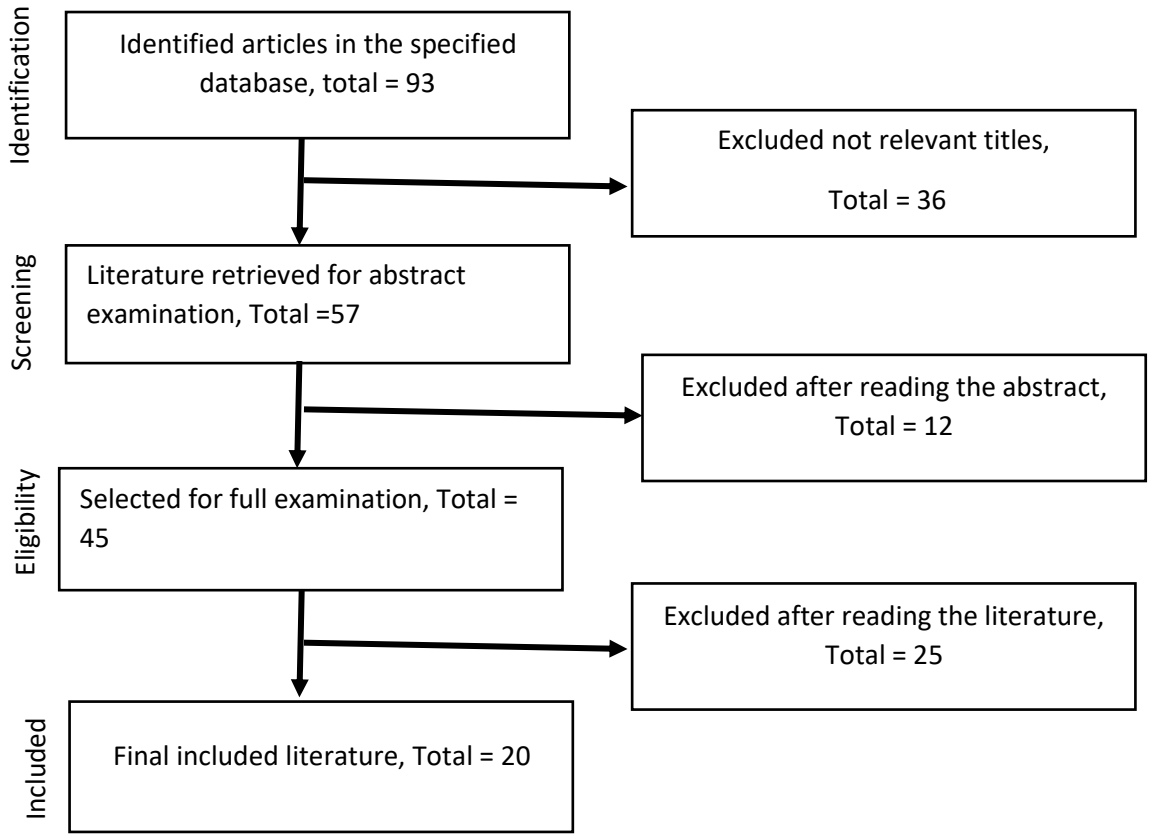


Figure 7**:** PRISMA workflow diagram of article search on impacts of blockchain technologies in the field of information security and privacy

The number of selected literatures per documentation category is depicted in the graph below. Articles on research are based on the work of university students. Journal papers were searched since they include the most up-to-date information and

are based on the work of experienced researchers in the subject. And the articles that contain the contributions made by the conference's researchers.

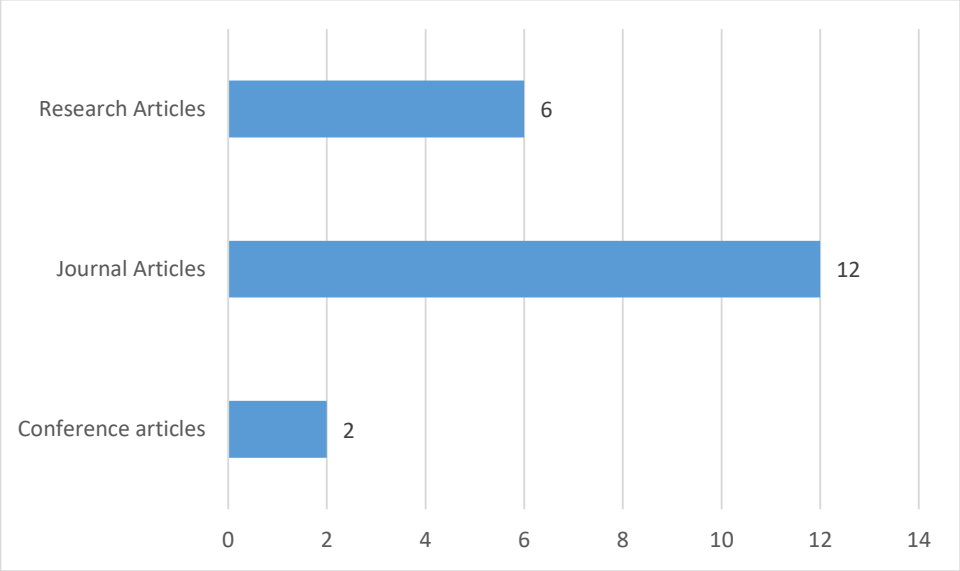


Figure 8: *Selected literature per documentation type*

It is also important to compile all the journals/files where the selected papers were published.

The table below contains the selected 20 articles and their journals where they were published.

S/N	Article	Journal/Field
1.	A survey on the security of blockchain systems by Xiaoqi Li et al, 2017	Future Generation Computer Systems
2.	A survey of Blockchain Security Issues and Challenges by Iuon-Chang Lin et all, 2017	International Journal of Network Security
3.	Blochain adoption is inevitable- Barriers and Risks remain by Kyleen W. Prewett et al, 2019	Corporate Accounting and Finance
4.	Security Concerns and Issues for Bitcoins, by Chinmay A Vyas and Munindra Lunagaria, 2014	International Journal of Computer Applications
5.	A Survey on Ethereum Systems Security: Vulnerabilities, Attacks and Defenses, Huashan Chen et al, 2019	Cryptography and Security
6.	A Survey of Blockchain from Security Perspective, Journal of Banking and Financial Technology, by Dipankar Dasgupta and Kishor Datta Gupta ,2019	Banking and Financial Technology
7.	Security and Privacy on blockchain by RUI ZHANG and RUI XUE, 2019	ACM Computing Surveys

8.	A survey of security threats and defense on blockchain by Jieren Cheng et al, 2020	Multimedia Tools and Applications
9.	Security Issues in Blockchain (ed) World by Esmeralda Kadena and Peter Holiecza, 2018	International Symposium on Computational Intelligence and Informatics
10.	How can Blockchain impact financial services: The overview, challenges and recommendations from expert interviewees by Victor Chang, 2020	Public Health
11.	Banking with blockchain (ed) big data by Hassani, H. et all, University of Arts London, 2018	Management Analytics
12.	Exploring the attack Surface of blockchain: A systematic overview by Muhammad Saad et al, April 2019	Cryptography and Security
13.	A survey on blockchain cybersecurity vulnerabilities and possible countermeasures ,Huru Hasanova et al,2018	International Journal of Network Management
14.	Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack Sayeed and MarcoGisbert , 2019	Applied Science
15	On the Security Risks of the Blockchain Efpraxia Zamani, Ying He & Matthew Phillips , 2018	Journal of Computer Information Systems
16	The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses by Ivan Homoliak et al., 2021	Cryptography and Security
17	A Survey on Security and Privacy Issues of Blockchain Technology by Tam T. Huynh et al.,2019	Mathematical Foundations of Computing
18	Blockchain Security: A Survey of Techniques and Research Directions by Jiewu Leng, et.al, 2020	IEEE Transactions on Services Computing
19	Blockchain Technology: Characteristics, Security and Privacy; Issues and Solutions by Muneer Bani Yassein et al.,2019	ACS/IEEE International Conference on Computer Systems and Applications
20	A Survey on Security and Privacy Issues of Bitcoin by Mauro Conti et al., 2018	IEEE Communications Surveys & Tutorials

Table 1: *Journals/Fields in which the papers were published*

4.2 Concepts Identification

According to Webster and Watson (2002) in their study "Analyzing the Past to Prepare for the Future: Producing a Literature Review," the organising structure of a review is established by concepts discovered in the literature. Another benefit of using this concept-centric approach, according to the authors, is that it aids in the synthesis of relevant material. It was decided to use a concept matrix to identify the most important concepts in the papers that had been chosen for the evaluation. In order to answer the research topic, it is necessary to look at the potential security risks associated with the blockchain. As a result, hunting for security flaws in literature is a worthwhile investment. The table below offers a concept matrix outlining the many blockchain security hacks that have resulted in problems. Security assaults were the most prevalent theme in the articles chosen for this matrix.

Security holes exist at every level of the blockchain's design (Yassein et al., 2019; Chen et al., 2019). The assaults are divided into groups based on the difficulty level they aim to attack.

4.2.1 Distribution of Security Attacks

The concept matrix helped to keep this study organized, it displays the connections between the selected articles. The matrix contains all of the security attacks covered in each article.

Moreover, the concept matrix visualizes the intersections of concepts between articles which provides the frequency of each presented concepts. The figure below presents the distribution of attacks found in the literature. Based on the findings, the majority of the authors identified 51 percent assault, double spending issue, selfish mining issue, and distributed denial of service issue as the most common security concerns. This implies that these are important topics to debate.

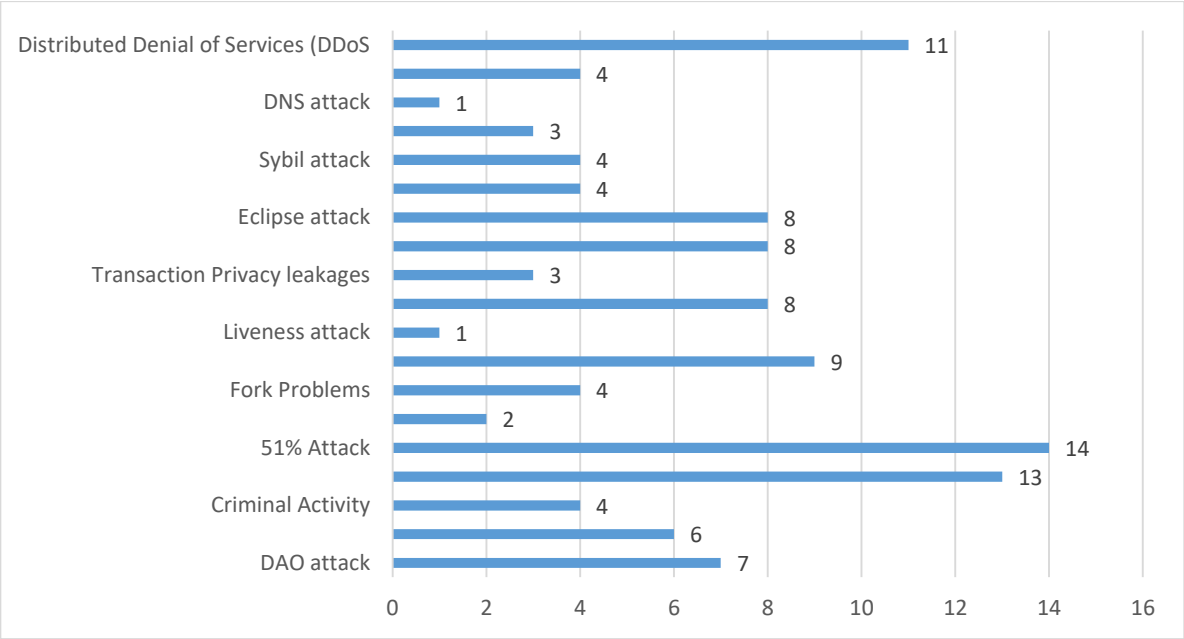


Figure 9: *Distribution of security attack*

4.3 Blockchain security

4.3.1 Blockchain Security Vulnerabilities

Blockchain technology is a recent breakthrough that has been promising secure computing without centralized authority in a distributed system but its layered architecture is susceptible to security risks. Mauro Conti et al. discuss the existing loopholes during the implementation of the bitcoin system that lead to security risks. Chen et al. (2019) surveyed security vulnerabilities and attacks on ethereum blockchain systems that can be applied to blockchain systems in general. Li et al.(2020) conducted a review of real assaults on popular blockchain systems from 2009 to May of 2017 and examined the vulnerabilities. There are vulnerabilities that are associated by both bitcoin and ethereum that occurred during the blockchain operation mechanism. Moreover, there are some sort of vulnerabilities that are related to ethereum blockchain and they are resulted from the development, deployment and execution of smart contracts (Li et al., 2020). Each layer on the blockchain is affiliated to some kinds of security vulnerabilities. The table below summarizes kinds of vulnerabilities that are present to each layer of the blockchain architecture.

S/N	Layer	Vulnerability Explanation
1.	Application layer	Vulnerabilities that are associated with the user interface, when a user is interacting with the blockchain system over applications like google chrome. This includes risks such as when a function's visibility is incorrectly specified which allow permission to unauthorized access. Thus, improper validation and external dependence.
2,	Data layer	Vulnerabilities that are associated with the database, Insufficient transaction information, configuration error in the database.
3.	Consensus layer	51% Vulnerability is inevitable whenever a group of miners join their computational power to make it greater than 50%, thus they can take over the blockchain. Reversing transactions by modifying blocks, performing double spending.
4.	Network layer	Insecure API design, and Improper configuration, Insufficient authentication and other common attacks that attack via internet infrastructure.

Table 2: Layers vulnerability explanation

Vulnerabilities in blockchain in general are initiated during the development process of application, configuration error during the design of the database implementation that left flaws that can lead to allow unauthorized to access the data, and inadequate human usability of applications and internal attackers that attacks the consensus algorithm mechanism by putting together their computing power to work against it.

4.4 Blockchain Security Issues per layered architecture

Blockchain technology promises a major change especially in the financial sector to improve business operations but also to address the issue identified in the traditional financial system including security issues due to its cryptographic mechanism behind it. However, there are possibilities of vulnerabilities that enter the system through different stages of blockchain implementation, including development stage, via user interface, configuration error and so on.

For a blockchain application to function, each of the layers presented in the previous section must perform its responsibility in the architecture. Moreover, each

layer is associated with some vulnerabilities that lead to security issues in the system that cause financial losses to individuals or institutions using the system. This section discusses the common security threats on each layer that are present in the blockchain system.

4.4.1 Application Layer

The application layer is the layer that allows the end user to interact with the system. It allows the interaction between the user and the blockchain system. Applications such as blockchain dApps (distributed applications) and smart contracts operate on this layer. Blockchain wallets allow users to store, transfer and manage their bitcoin and ether. And for a wallet to function, a user needs an account in the wallet. The API is not accessible to clients in the blockchain system. Therefore, an application layer plays a role like a web browser that gives the user interface for the user who is not the developer. Distributed application is provided for the clients to be able to use the system. For instance, dApp is a system terminal that is perceived as a user interface that is necessary for the clients to communicate with smart contracts (Zheyi Lu, 2018). During the user interaction with the system, this is where the security issues emerge in the system. Each layer in the blockchain architecture is susceptible to specific attacks. However, there are security threats that can attack more than one layer. For instance, Distributed Denial of Service attacks (DDos). DDos assaults can occur at the network layer or at the application layer.

S/N	Attacks	Causes	Consequences
1.	Attacks on the wallet's software	Vulnerable signature, lack of control in address creation, Bugs and malware, Flawed key generation	Unauthorized code execution Denial of service Private key leakage
2.	Criminal Attack	Crypto currency application	Ransomware Money laundering Underground market
3.	DAO attack	Reentrancy	Unauthorized code Execution

Table 3: *Application layer types of attacks*

i. ***Attacks on the wallets software*:** Wallet is necessary in blockchain for the user to make transactions. Software wallets are software applications that users can download online so that they can install them on their computer devices including smart phones, desktop, laptop. These wallets, also known as online wallets, are used to store private keys locally (Mosakheil, 2018). Instead of being saved on a local computer, private keys are stored on the cloud. The most common reason for wallet software assaults is a susceptible signature. The blockchain's authentication method relies heavily on the private key. For instance, bitcoin uses Elliptic Curve Digital Signature Algorithm (ECDSA) to sign and validate transactions (Goldfeder, Gennaro, & Kalodner, 2015).The book(Christin & Safavi-Naini, 2014) discusses the poor randomness of key generation in ECDSA algorithm that generate insufficient signature which lead to compromise of private key.ii) Lack of control in address creation, to send or receive bitcoin, payers have the option to specify the trusted party that attests to the identity of the payee, they require the payee to use certified bitcoin address. This can allow the attacker to change the address of the payee to the attacker's address (Mosakheil, 2018).iii) Bugs and malware: There are still different types of bugs in the client software such as in configuration, GUI design, security and so on. These bugs are exploited to attack the blockchain system (Mosakheil, 2018).iv) Flawed key generation, configuration errors in the implementation of ECDSA cause weakness in the wallet which lead to exposure of private keys (Mosakheil, 2018).

ii. ***Criminal activity*:** Bitcoin has been used in illegal activity because bitcoin users can have more than one bitcoin address given that the process is anonymous, it is hard to identify who is doing what. One type of criminal conduct involving bitcoin is ransomware. In May 2017, ransomware entitled WannaCry infected around 230,000 victims across 150 countries in only two days. It targeted a vulnerability in the Windows system to encrypted users' files and then to ask for Bitcoin ransom (Li et al., 2020).

iii. ***DAO attack*:** It is an attack that specifically attacks ethereum. DAO is a smart contract that was released on Ethereum on May 28, 2016, that implements a crowd-funding platform. i) Reentrancy vulnerability means that the execution can be interrupted in the middle by inserting another execution and both can complete without any errors. The intermediate state can be used by an attacker to make several calls to the smart contract. This attack exploits reentrancy vulnerability by publishing a malicious smart contract that has a withdraw () function call to DAO in its callback function. This allows the attacker to steal from DAO (Li et al., 2020); (Chen et al., 2019).

4.4.2 Data Layer

This layer involves the content, data structure and the operation of the blockchain data (Mosakheil, 2018).Blockchain is a distributed based system where each node in the network is able to add transactions in blocks. The data about the sender, the receiver, the amount and the hash value are necessary values stored in a block. This layer is exposed to security issues given that it involves transactions in the network which are the major components in the blockchain system.

Attacks	**Causes**	**Consequences**
Transaction privacy leakage	Transaction design flaw	Deducing the actual transaction input
Private key security	Public-key encryption scheme	Private key leakage

Table 4: *Data layer types of attacks*

i. ***Transaction privacy leakage:*** Normally, transactions are protected by private keys so that the attacker cannot deduce whether the cryptocurrency in different transactions is received by a specific user. However, in monero (a digital currency), user add chaff coins when initiating a transaction so that the attacker cannot infer the actual coins being transferred. However, privacy protection in blockchain is still not very robust. All the transactions do not contain the chaff

coins which lead to privacy leakage since the attacker will be able to infer the actual coins in the transaction (Li et al., 2020).

ii. ***Private Key Security:*** Private key is used for the user identification and it is considered as the security credential in the blockchain system. ECDSA (Elliptic Curve Digital Signature Algorithm) used in blockchain, to generate private key for the user has a weakness of generating not enough randomness so that is it is not easy to guess the signature process which lead to privacy leakage(Li et al., 2020).

4.4.3 Consensus Layer

In the blockchain architecture, the consensus layer is the most important component. It's the layer in charge of enforcing the rules that network members should follow in order to reach a consensus on the published transactions. Since there is no central authority to assure the reliability and consistency in the system, blockchain system adapt the consensus mechanism to do so. This layer is responsible for verifying and validating the blocks and to ensure that the participants in the network agrees on everything happening in the network. Moreover, it deals with the ordering of the transactions. This layer is more critical in the system and it is susceptible to different attacks that lead to serious security issues (Li et al., 2020) and (Homoliak et al., 2021).

Attacks	**Causes**	**Consequences**
51% attack	Consensus mechanism	Unfair income Double spending problem Transaction denial of service
Pool hopping attack	Consensus mechanism	Unfair income
Fork problems	Decentralized node version	Undue rewards to dishonest miners
Selfish mining	Consensus mechanism	Undue rewards to dishonest miners
Liveness attack	Consensus mechanism	Undue rewards to dishonest miners

Table 5: *Consensus layer types of attacks*

i. **51% attack:** A group of miners that join together their computational power to attain more than 50%. By attaining this percentage, attackers can control the entire blockchain by being able to modify and reverse the transactions they made

so that they can perform double spending activity. It is also known as the majority attack; such an attack is able to prevent from being validated. Thus, it leads to transaction denial of service.

ii. **Pool hopping attack:** This attack uses the information about the number of submitted shares in the mining pool in order to do a selfish mining (Conti et al., 2018). A share is gained by the member of the mining pool who announces the valid proof of work. The attacker does a continuous analysis of the number of shares submitted by other miners in order to discover a new block. By doing this analysis, the attacker can switch to another pool to profit the shares (Conti et al., 2018).

iii. **Fork problems**: This problem happens when there is a need to upgrade to a new version of blockchain software. This emerges in a new agreement in the consensus rule. The nodes with the new rules from the new version could not agree with the nodes that are still using the old software version. Thus, incompatibility in the system since the computing power of new nodes are stronger than old nodes, the block which is mining by the old nodes will never be approved by the new nodes which lead to unfair income (Iuon-Chang Lin & Tzu-Chun Liao, 2017).

iv. **Selfish mining**: This attack is the group of miners that work together to waste the computing power of honest miners. Dishonest miners attempt to hold and maintain a long private chain while the honest miners continue mining on the public chain which will not be able to be broadcasted before new blocks mined by the dishonest miners are revealed. This gives the attacker first priority while mining the following block (Li et al., 2020).

v. **Liveness attack**: This assault has three phases: attack preparation, transaction denial, and blockchain retarder. Basically, what this attack does is to delay as much as possible the confirmation time of the target transactions from being broadcasted in the network (Li et al., 2020).

4.4.4 Network Layer

A peer-to-peer network design underpins blockchain. The nodes that compose the network share the data between each other. Data representation and network

services planes are two components of the network layer discussed by Homoliak. Data representation is about storage, encoding and the protection of data while the network service plane is about communication, routing, addressing and naming services. This layer has also a high exposure to different security threats given that there are various underlying technologies happening to this layer. Most of the threats on this layer arise from man in the middle attack since the network layer allows the communication between nodes in a peer to peer architecture.

Attack	**Cause**	**Consequences**
Eclipse attack	Threats on DNS and routing	Selfish mining, double spending
Time jacking	Dishonest miners	Double spending
Sybil attack	Improper configuration Insufficient authentication	Double spending DDos
Balance attack	Improper configuration Insufficient configuration	Double spending
DNS attack	Cache poisoning	Selfish mining
Routing attack	Dishonest ISPs	Denial of service
Distributed Denial of service	Malicious attack	Denial of service

Table 6: *Network layer types of attacks*

i. ***Eclipse attack*:** The attacker maliciously seizes the connections from a node to its peers so that heattacker can take control of all the traffic sent and received by that node (Homoliak et al., 2021). Thus, the attacker can cause serious security issues in the system such as selfish mining and double spending issues.

ii. ***Timejacking attack*:** The attacker publishes the time which is not correct when connecting to a node. When the node's time counter is modified, the susceptible node may accept a different blockchain. This could exacerbate the problem of double spending (Mosakheil, 2018).

iii. ***Sybil attack*:** This attack uses fake identities and assigns them to the victim node’s peers. The attacker will then force the user to select blocks that are only under the attacker's control (Mosakheil, 2018).

iv. ***Balance attack*:** The attacker delays the communications between the nodes that are operating on the same rate of mining power. The main goal of this attacker to disrupt the communication between these nodes is to perform double spending issues (Natoli & Gramoli, 2017); (Li et al., 2020).

v. ***DNS attack:*** The attacker poisons the DNS cache and alter the data in the DNS. When a user sends a request to the server to obtain the IP addresses of the peer's node, the user is directed to the network of the attacker. Thus, the attacker can control the victim node (Homoliak et al., 2021).

vi. ***Routing attack:*** This attack is done on the ISP level where the internet service provider can change the internet routing system to isolate some nodes from the network (Conti et al., 2018).

vii. ***Distributed Denial of service:*** As blockchain operates over P2P, this attack aims to deny the service between the nodes of the networks by injecting the malicious traffic so that it consumes the bandwidth and disrupts the connectivity which leads to the denial of the service (Wani et al., 2021).

4.5 Mapping security Attacks to common Security Impact

The figure below summarizes the potential attacks that were found in the selected literature and their respective consequential security impact.

Attack	Double Spending	Unauthorized Code execution	Denial of Service	Unfair income	Private key leakages	Selfish mining
DAO attack		X				
Attack on wallet software		X	X		X	
Criminal Activity			X	X		
Double Spending				X		
51% Attack	X			X		
Pool hopping attack					X	X
Fork Problems					X	
Selfish Mining attack						
Liveness attack						
Private key security						
Transaction Privacy leakages						X
BGP Hijacking attack						

Eclipse attack	X					
Time jacking	X					
Sybil attack	X		X			
Balance Attack	X					
DNS attack						X
Routing/Propagation/ partition	X		X			X
Distributed Denial of Services (DDos)			X			

Table 7: *Mapping security attacks to common security problems*

4.5.1 Double Spending

Double spending is a way that a user uses a cryptocurrency more than once for a transaction. Xiaoqi Li et al, (2017); Chinmay A. Vyas and Munindra Lunagaria (2014) argue that double spending is easy to happen in blockchain that are based on proof of work algorithm. By varying the time stamp, the attacker uses the same coin for two different transactions. The attacker makes two transactions simultaneously, the first transaction is made and by using the same coin the second transaction is made to another address that the attacker has control of for another transaction. As illustrated in the diagram, numerous attacks generate double spending. One of the most common attacks is 51% attack, this attack is due to the mining process and the consensus algorithm that the blockchain use and it is difficult to prevent it since the majority of the users need to agree on changing the protocol framework (Chinmay A. Vyas and Munindra Lunagaria, 2014), (Xiaoqi Li et al, 2017). The collaborating miners as a result of the 51 percent assault forced the bogus double spend transaction to be accepted in a block (Dipankar Dasgupta and Kishor Datta Gupta, 2019).

Chinmay A. Vyas and Munindra Lunagaria (2014) suggests one possible solution to mitigate the effect of 51% attack as to introduce checkpoints so that blocks before checkpoints cannot be modified. Eclipse attack prevents the victim's nodes to communicate to the rest of the nodes in the P2P network. When the victim's nodes become inaccessible to other nodes in the network, the attack controls the victim's nodes by poisoning their routing table (Huashan Chen et al, 2019), (Huru Hasanova et al, 2018). Since the dishonest nodes or attackers are able to control the victim's connections hence it is possible to modify the transactions and execute double spending (Tam T. Huynh et al., 2019). Ethan Heilman et. al., (2015) proposes some solutions

including deterministic random eviction, random selection, tests before evicts, feeler connections, anchor connections, more buckets, more outgoing connections and ban unsolicited ADDR messages.

The collective goal of these solutions is to ensure that eclipse is more difficult to happen. Sybil and balance attacks also can be executed to double spending issue. Sybil attack attacks a P2P network by inserting fake identities in the network. The network is corrupted by this fake node, hence the validation of unauthorized transactions and modification of transactions which cause double spending issue (Sayeed and Marco-Gisbert, 2019). Balance attack is an attack that target the nodes in the network that have the same mining power. The attacker uses their limited hashing power to delay communication between nodes, resulting in the formation of network subgroups that are not on the same page. Hence the attack exploitation on the network (Sayeed and Marco-Gisbert, 2019). Routing attacks are similar to balance attacks in that they isolate a portion of the network or impede block transmission. This allows the attacker to cause a certain amount miner power to be wasted hence the chance for different attacks to exploit the network causing different issues such as double spending (Mauro Conti et al., 2018). DNS and DDos assaults both function on a P2P network by poisoning the network in order to gain control over the victims' nodes, which are used by dishonest miners to carry out security issues i.e. double spending which is one of the common issues that are caused by these types of attacks that operate on a P2P network (Wani et al., 2021), (Homoliak et al., 2021). Possible countermeasures of double spending issue include to insert observers in the network that monitor to alert double spending issue in the blockchain network so that the merchants can detect the direct incoming connections (Mauro Conti et al., 2018). Other possible countermeasures are discussed by Dipankar Dasgupta and Kishor Datta Gupta (2019) that network encryption randomized is crucial to protect the network, UDP heartbeats are necessary to determine if the messages are being prevented to reach their peers nodes and round-trip time monitoring to avoid the modification in the timestamp.

4.5.2 Unauthorized Code Execution

One of the most common security vulnerabilities in the blockchain is unauthorized code execution. Huashan C. et al (2019) described causes that achieve this consequence i.e. DOA attack exploit reentrancy vulnerability, erroneous vulnerability also paves the way to unauthorized code execution. Furthermore, because the private keys stored in the wallet are compromised, an attack on wallet software results in unauthorized code execution (Chinmay A. V. & Munindra L., 2014; Huashan C. et al, 2019; Dipankar D. & Kishor D. G., 2019; Muhammad S. et al.,2019).

There are typical security ways to avoid this type of security vulnerability. Muneer Bani Yassein et al. (2019) advises security solutions including adapting encryption principle that helps to maintain the confidentiality of the data, using specific keys with encryption methods to enhance the security of the data, using SmartPool which is a new data structure to protect data against attackers.

4.5.3 Denial of Service

Denial of service is one the security issues that cause trouble for services after consuming a huge amount on network bandwidth. It is harder to disrupt a decentralized system and a peer to peer-based architecture than the conventional client to server-based applications. However, blockchain based platforms are also susceptible to denial of service attack and it is more complicated and costlier to overcome in a blockchain based platform due to its P2P architecture (Huru Hasanova *et al*, 2018); (Mosakheil, 2018). A solution for this problem that was discussed by Mosakheil (2018) is blockchain-based DNS method that advances security by removing the single target that attackers can attack to tamper with the entire system. They discuss Nebulis, a project that explore a concept of adopting distributed DNS systems which eliminates a single point of failure in traditional DNS system.

4.5.4 Unfair income/selfish mining

Unfair income refers to dishonest miners that work to invalidate the transactions of honest miners and this is also known as selfish mining which results in unfair income issue. 51% attack is one of the most common attack that lead to unfair income. As it was explained in the earlier sections, how this attack works with the specific goal of putting the computing power together which gives these dishonest

miners to make change to transactions or reverse transactions that definitely lead to unfair income among the miners in the network. This relates to selfish mining attack in which dishonest miners work to confuse honest miners by releasing a big number of blocks simultaneously instead of publishing blocks to the network as they find them. As a result, honest miners are forced to reject their blocks, resulting in a loss of money. Possible proposed solutions to this problem include assigning miners to different branches of pool randomly, freshness preferred solution which means that the recent timestamp will be considered which proves a block that is recently mined. Another important solution proposed is ZeroBlock algorithm, the idea behind this is that each block must be published and received by the network within a maximum acceptable time (Mosakheil, 2018).

4.5.5 Privacy Key Leakage

Private and public keys are supposed to guarantee a certain extend of privacy to blockchain system. During the transaction process, users are pseudonymous privacy. However, it is challenging to guarantee the transactional privacy since the transaction related information i.e. balances for each public key are visible to everyone. By associating separate bitcoin transactions, dishonest users or attackers might reveal user information (Zheng et al, 2017). Key leakage is a serious issue in blockchain. Ivan Homoliak *et al.,* (2021) also argues that the privacy issue refers to revealing addresses of bidders and their bids to the public. Traditional public key infrastructure is vulnerable towards privacy leakage attack (Jieren Cheng *et al,* 2020). Hawk is a new framework for privacy-preserving smart contacts, as detailed by Xiaoqi Li et al., (2017) and Muneer Bani Yassein et al., (2019). The model is designed in a way that the contract can be divided into two parts which are private and public parts. Private parts hold the private data and financial related function codes and the data that do not have private information can be in public part. Furthermore, Zheng et al. (2017) explore mixing and anonymous as two strategies for enhancing blockchain anonymity. *Mixing,* even if the user ‘addresses are pseudonymous but it is still possible to expose the real user’s identity as the users frequently use the same address when making transactions. Mixing introduces a feature of transferring a transaction through multiple input addresses and output addresses. For instance, when a sender X want to send funds to

recipient sender X transfer funds to trusted x1, x2, x3 and so on users to y1, y2, y3, and so on so that they can finally transfer the funds to the intended recipient Y instead of making a direct transaction from X to Y which could allow the attackers to reveal the relationship between users. To enhance anonymity in bitcoin network, the origin of the payment is unlinked from its transactions to prevent the analysis of transaction graphs that provide insight leading to identify the real user identity.

CHAPTER V

Discussion, Theoretical and Practical Implications

5.1 Discussion

The mapping of security assaults to the outcomes of common security issues in blockchain demonstrates some overlaps between attacks and frequent problems. For instance, a 51% attack results in double spending and unequal income distribution. Unauthorized code execution, denial of service, and private key leakage occurs as a result of an attack against wallet software. Additionally, the Sybil attack resulted in duplicate spending and a denial of service issue. Another type of security attack that creates multiple issues is the routing attack, which results in double spending, denial of service attacks, and erroneous income. Other attacks, as illustrated in the mapping table, create one of these issues. This is accomplished through the use of a concept-centric matrix technique, which enables us to extract and classify the security attacks addressed in various publications by various selected scholars. This chapter discusses the study's theoretical and practical ramifications.

5.2 Theoretical implications

Blockchain technology has the potential to transform people's lives because of its operating mechanism and architecture, which ensure network openness, trust, security, and integrity. However, its security and privacy levels remain deficient. Numerous assaults found and analyzed in the blockchain's four tiers can be grouped into two distinct groups. The first group contains attacks that exploit flaws in the P2P network design, while the second category includes attacks that target the consensus mechanism. One of the primary reasons that the consensus layer and network layer should be prioritized as key layers in the blockchain system is that the network layer (peer-to-peer) is responsible for delivering data provided by applications on the bitcoin network. On the other hand, the consensus role is to reach agreement on the data and to enable decision-making. Three layers are involved in this process: the network layer, the application layer, and the consensus layer. The fact that blockchain systems operate on a decentralized foundation with a peer-to-peer network architecture demonstrates their utility. This means that the network's nodes serve as both clients and servers.

Typically, when security measures are implemented to safeguard the network in a client-server architecture, the server is heavily protected by advanced security software due to the fact that it serves many machines (clients) on the network.

As a result, securing each node in a peer-to-peer network where each node works as both a client and a server is challenging. It remains challenging to ensure proper security in a system where each node is autonomous and stores its own data. As a result, assaults on the network layer are characterized as attacks caused by the vulnerability in the P2P network architecture. The data layer serves as the blockchain's database, as it is composed of data blocks that represent the data structure of transactions. Additionally, it concerns itself with key management and cryptographic techniques.

As a result, this layer is vulnerable to attacks that exploit flaws in key management and cryptographic methods. Private and public keys are crucial components of blockchain technology since they must be included in each transaction initiated. At this time, human error has been identified as a substantial contributor to the key leakage problem. A cryptographic algorithm might mitigate this issue sufficiently if human errors could be reduced or eliminated, which is typically not practicable. The hackers stole these keys from the users' mobile PCs, where they were stored, in order to tamper with the blockchain system. Another factor is related to the blockchain's vulnerability, which allows a human to exert complete control over the transaction he initiates. This enables a user to provide incorrect information on purpose, which results in transactional errors. Moe so, people need to be protected from making mistakes, and the blockchain still needs to be improved to make it less likely that someone will submit false information, either by accident or on purpose.

One of the recommended solutions is to deploy an advanced encryption approach to increase security, which could also be applied to other types of assaults. The second kind of assault is those that occur as a result of the blockchain's mechanism architecture and consensus algorithm, which enables dishonest individuals to agree to collaborate in order to receive unfair money. As a result, blockchain technology requires the addition of additional features that can strengthen its consensus algorithm's defenses against dishonest users. Numerous researchers have proposed various

strategies for enhancing the security of blockchain technology. However, some issues are unavoidable due to the vulnerability of the blockchain's architecture and process to these attacks. For example, the 51 percent attack continues to cause issues on the blockchain, namely double spending. To resolve this issue, a majority of users must agree to alter the protocol foundation.

5.3 Practical implications

In the world of information technology, there will always be good actors who work to advance the blockchain for the greater good of society, but there will also be bad actors who are self-interested and exploit its vulnerability for their own nefarious gain. In information technology, the race between good and bad actors is never-ending. Since its inception in 2009, blockchain technology has continued to broaden its uses beyond the financial sector. The market value of crypto assets, particularly bitcoin, continues to rise. Globally, large financial institutions continue to invest in this technology and upgrade their human resources in order to maximize its benefits while also developing defensive measures to combat the aforementioned threats and those that are unknown. From a pragmatic standpoint, we argue that: Is a survey of the literature over the previous decade since the debut of blockchain technology reveals that users are not deterred by security assaults. This is because blockchain technology is gaining traction across the globe and in a wide variety of businesses. Today, bitcoin has a market capitalization of more than $300 billion, and the total value of crypto assets is estimated to be more than a trillion dollars. This demonstrates that the advantages of blockchain technology, and specifically bitcoin, exceed the security concerns. (ii) It will be practically hard to protect the blockchain from security risks and create a zero-risk product. As previously stated, security risks are inherent in all technology products, and as previously stated, information technology will always have both good and bad actors. The most practical outcome of this blockchain technology is that, when the benefits of blockchain are considered, defensive measures and security threats result in reasonable net benefits that incentivize society and blockchain users to continue developing it. (iii) The combination of research and experience gained through blockchain use teaches valuable lessons about how to mitigate the blockchain's inherent security risks. While this thesis focused on the

blockchain's security, we also highlighted some defensive solutions that have been developed to thwart attacks in the past. We also argue that over time, the technology community will continue to learn from experience and plug vulnerabilities, especially in the four layers, reducing this security risk. However, it is practically inconceivable to make blockchain completely immune from security risks. Laws and regulations, including ones that allow criminal investigation and punishment of bad actors, as well as international collaboration, are also expected to be made in the future. This will help deter bad actors, as well as lessen the number of security attacks on blockchain.

CHAPTER VI

Conclusion, Limitations and Future Research

6.1 Limitations and Future Research

Blockchain technology is a vast and complicated subject. Time constraints were a significant factor in comprehending and explaining the blockchain system. The literature for this thesis was gathered through a search of six different databases. However, there are other databases that may have been used to locate new papers or to provide additional interpretations of this thesis. Thus, it is preferred that future studies incorporate a broader range of databases in order to amass more robust data that contributes more to this subject. The concept of blockchain technology is still very new. Gorkhali et al. (2020) contend that the number of journal articles published regarding blockchain in various journals included in the SCI/SSCI database has increased from one in 2016 to 18 in 2017 to 68 in 2019. According to this study, the intended intention was to extract all articles published after the launch of blockchain in 2009, but the first publication included was in 2017, based on the year. Because of the possible value to society, researchers should pursue this topic. Thus, future studies could include reading books to gain a thorough understanding of the blockchain technology concept, which will contribute to developing sufficient information to design protocols that will strengthen the blockchain's security. It would be interesting to examine how the protocol framework might be enhanced in the future. This thesis is limited to discussing the security risks associated with blockchain technology in the context of the bitcoin network, which is widely employed in the financial sector. It could be worthwhile to do a similar examination in other sectors, such as health and transportation, to examine security vulnerabilities there as well. Additionally, additional research is necessary to determine the efficacy of these recommended treatments. Collaborative attacks that involve miners, like the 51 percent attack, are still hard to stop.

It is noteworthy that future research should be made on the intergration of blockchain technologies in machine learning. Numerous studies have demonstrated the effectiveness of the combination of blockchain technology and machine learning, which is poised to revolutionize a wide range of technological fields, including networking and

communications systems. On the one hand, by integrating blockchain technology into machine learning systems, problems may be sorted out more swiftly than ever before using the data gathered and altered by blockchains.

The key characteristics of blockchain (security and trustworthiness) enable Machine Learning solutions used in communications and networking systems to become more trustworthy. Blockchain applications, on the other hand, might have significant intelligence for data processing and the execution of computationally heavy applications by employing Machine Learning techniques. Furthermore, Machine Learning-based blockchain processes can handle many sorts of transactions and enable effective operation, particularly when implemented in smart contracts.

Even though combining blockchain and machine learning has many benefits, there are still a number of significant research challenges that need to be thoroughly examined before this technology is widely adopted. These challenges include resource management, big data processing, scalability, security, and privacy. Future study should pay close attention to big data processing, which makes the design and analysis of the combination of blockchain and machine learning even more challenging. How to address the scalability issue, particularly for large-scale complex systems, is a basic difficulty of the combination of blockchain with machine learning, in contrast to traditional centralized solutions.

One way that blockchain can help Machine Learning is in the areas of sharing data and models, security and privacy, decentralized intelligence, and trustworthy decision-making. By using cryptographic approaches, blockchain-based systems may assure data security and auditability of the collaborative training process and the learned Machine Learning model. They can also store vast amounts of data in a safe and tamper-resistant way. Blockchain technologies also make it possible for a decentralized infrastructure to guarantee safe access control without relying on independent central bodies. Blockchain technology enables Machine Learning to train, learn, and make choices on local devices in distributed, decentralized networks. Particularly, DAPPs and smart contracts could open up new possibilities for modeling interactions between various entities in a decentralized machine learning application. Finally, blockchain technologies make it possible for authorized nodes with access to the system to check

and audit the transparent, immutable records of the training data and variables utilized by Machine Learning algorithms for their decision-making conclusions at any time. In this approach, the collaborative dynamics in decentralized Machine Learning applications are considerably enhanced and the processes of the Machine Learning algorithms are simple to audit.

On the other side, blockchain may benefit from machine learning for scalability, energy and resource efficiency, privacy and security, and intelligent smart contracts. In particular, machine learning-based mining algorithms may manage jobs in a more intelligent manner rather of using the brute force technique by exploiting the training data. Machine Learning algorithms' ability to forecast data and quickly calculate it would also make it practical for miners to choose transactions that are more crucial to complete. Additionally, the combination of blockchain technology and machine learning may completely transform the conventional energy industry, making it far more intelligent and efficient. Blockchain applications may enable predictive analytics by utilizing machine learning techniques. This will guarantee that the needs for energy and resources are appropriately addressed and will increase the effectiveness of blockchain operation. The blockchain can benefit from machine learning approaches to optimize data maintenance and storage by providing more effective data sharding or pruning solutions to handle the scalability challenges. In order to increase the scalability of the blockchain-based system, machine learning techniques may also be used to allow more effective off-chain solutions or to dynamically change the block size. Additionally, the use of trained models and algorithms in blockchain-based communications and networking systems allows for the detection of harmful activity on the blockchain. In this approach, machine learning might help blockchain systems recognize and stop theft, fraud, and unauthorized transactions.

6.2 Conclusion

Due to the way blockchain technology operates, it is an intriguing but also extremely difficult technology. In short, the goal of blockchain technology is to decentralize data storage in a peer-to-peer network in such a way that no single central authority can control the entire network. Blockchain technology introduced a novel

concept to the financial industry, allowing users to conduct transactions within the network without the intervention of central banks, which had previously controlled the transaction process. The goal of this research was to develop a more complete understanding of blockchain technology from a security perspective. To begin with, the study addresses a critical research question: what are the current security concerns surrounding blockchain technology in the technological industry? A concept-centric matrix technique was used to facilitate the classification and categorization of security assaults into their relevant tiers. The initial version of the concept matrix was adjusted to reflect the developing understanding of the subject, paving the way for mapping security assaults to typical security problems. As described in the preceding section of this thesis, the research of twenty articles selected for this study demonstrated that some attacks continue to occur today. This study connected security attacks in blockchain technology to common security issues and concerns, and it showed that 51 percent of attacks result in double spending and unjust income; denial of service attacks were the most prevalent security issues in blockchain technology. Along with the security attacks and their repercussions, the thesis also covers the authors' proposed security solutions.

References

Alastria. Available online: https://alastria.io (accessed on 15 September 2020).

Allison L. & Brent W. (2011). Decentralizing Attribute-based Encryption. In Eurocrypt. 568–588.

Amit, S. & Brent, W. (2005). Fuzzy Identity-Based Encryption. 457–473.

Andreas, M. A. (2017). Mastering Bitcoin: Programming the Open Blockchain. O'Reilly Media, 2 edition, 6.

Atchley, D. (2018). UX Design for Blockchain is still UX Design. tandemly Blog post. Online at https://medium.com/tandemly/ux-design-for-blockchain-is-still-ux-design-2a3e1dd15a99.

Baker-Mills, S. (2017). Blockchain Design Principles. Design at IBM. Online at https://medium.com/design-ibm/blockchain-design-principles-599c5c067b6e.

BBP. (2017). Building Blocks. Online at http://innovation.wfp.org/project/building-blocks.

Bera, B., Saha, S., Das, A.K., Vasilakos, A.V. (2020). Designing Blockchain-Based Access Control Protocol in IoT-Enabled Smart-Grid System. IEEE Internet Things J.

Bernal Bernabe, J., Canovas, J.L., Hernandez-Ramos, J.L. (2019); Torres Moreno, R.; Skarmeta, A. Privacy-Preserving Solutions for Blockchain: Review and Challenges. IEEE Access, 7, 164908–164940.

Bitansky, N., Ran, C., Alessandro, C., & Eran, T., (2012). From Extractable Collision Resistance to Succinct Non-interactive Arguments of Knowledge, and Back Again. 326–349.

Bitinfocharts, (2019). Bitcoin Block Time historical chart. Retrieved from https://bitinfocharts.com/comparison/ bitcoin-confirmationtime.html

Buterin, V. (2014). "Ethereum: A next-generation smart contract and decentralized application platform." *Ethereum Foundation*. [Online] Available: https://github.com/ethereum/ wiki/wiki/White-Paper, Accessed on: 5 December 2016.

Casino, F., Dasaklis, K., Thomas & Patsakis, Constantinos (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues, *Telematics and Informatics*, 36, pp. 55–81.

Chen, L., Qin, B., Wu, Q., Zhang, Y., Zhong L., & Zheng, H. (2017). "Bitcoin and Digital Fiat Currency," *Journal of Cryptologic Research*, vol. 4, no. 2, pp. 176-186, 10.13868/j.cnki.jcr.000172.

Chen, S.; Yan, J.; Tan, B.; Liu, X.; Li, Y. (2019). Processes and challenges for the adoption of blockchain technology in food supply chains: A thematic analysis. In Proceedings of the iconference, Washington, DC, USA, 31 March–3 April 2019.

Chinmay A. V. M. L. (2014) Security Concerns and Issues for Bitcoin, IJCA Proceedings on National Conference cum Workshop on Bioinformatics and Computational Biology

Consensys. (2018). Blockchain Basics. A Curated Collection. ConsenSys Academy.

Conti, M., Sandeep, K., E., Lal, C., Ruj, S. (2018). A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys Tutorials* 20(4) (2018) 3416–3452.

Craig, G. (2009). Fully Homomorphic Encryption Using Ideal Lattices. In Stoc. 169–178.

Cromwell, B. (2015). What Is Post-Quantum Cryptography And What Does It Mean For Us?. Retrieved from https://blog.learningtree.com.

Dannen, C., (2017). *Introducing Ethereum and Solidity*. Vol. 1. Berkeley, Apress.

Dhillon, V., Metcalf, D., & Hooper, M. (2017). Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make It Work for You. Apress.

Efanov, D.; Roschin, P., (2018). The All-Pervasiveness of the Blockchain Technology. Procedia Comput. Sci., 123, 116–121.

Eli, B. S., Alessandro, C., Christina G., Matthew G., Ian M., Eran T., & Madars V. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. In SP. 459–474.

Etherscan, (2019). Ethereum Block Time History, Retrieved from http://etherscan.io/chart/blocktime

Fan, K., Bao, Z., Liu, M., Vasilakos, A.V., & Shi, W. (2020). Dredas:. Decentralized, reliable and efficient remote outsourced data auditing scheme with blockchain smart contract for industrial IoT. Future Gener. Comput. Syst., 110, 665–674.

Fan, Kai, Shangyang Wang, Yanhui Ren, Kan Yang, Zheng Yan, Hui Li, and Yintang Yang. (2018). "Blockchain-based secure time protection scheme in IoT." *IEEE Internet of Things Journal* 6 (3):4671−4679.

Fernández-Caramés, Tiago M., & Paula Fraga-Lamas, (2018). “A review on the use of blockchain for the internet of things.” *IEEE Access* 6: 32979–33001.

Fleder, M., Kester, M. S. & Pillai, S. (2015). “Bitcoin Transaction Graph Analysis,” *CoRR,* abs/1502.01657

Flipo, F., & Berne, M. (2019). The Bitcoin and Blockchain: Energy Hogs. Retrieved from https://theconversation.com

Florian, T. & Bj¨orn, S., (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys Tutorials, 18(3):2084–2123.

Francesco Maesa, D. & Mori, P., (2020). Blockchain 3.0 applications survey. J. Parallel Distrib. Comput., 138, 99–114.

Fremantle, P., Aziz, B., & Kirkham, T. (2017). “Enhancing IoT Security and Privacy with Distributed Ledgers - A Position Paper,” *Proc. 2nd Int. Conf. Internet Things, Big Data Secur.*, April, pp. 344–349.

Gao, M., Wang, H., Zhang, F., Li, T., & Du, X. (2019). “Security and privacy-protection technologies in smart contract,” *Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition),* vol. 39, no. 4, pp. 63-71, 10.14132/j.cnki.1673-5439.2019.04.009.

GoChain. (2018). Proof of Reputation. (March 2018).

Goldfeder, S., Gennaro, R., Kalodner, H., Bonneau, J., Kroll, J. A., Felten, E. W., & Narayanan, A. (2015). Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme. In et al.

Goldreich, O. (Ed.). (2019). Providing Sound Foundations for Cryptography: On the work of Shafi Goldwasser and Silvio Micali. Morgan & Claypool.

Goldwasser, S., Micali, S. & Rackoff, C. (1989). “The knowledge complexity of interactive proof systems,” *SIAM J. Comput.*, vol. 18, no. 1, pp. 186-208, 10.1137 / 0218012.

Gomez, M., Bustamante, P., Weiss, M.B., Murtazashvili, I., Madison, M.J., Law, W., Mylovanov, T., Bodon, H., Krishnamurthy, P. (2019). Is Blockchain the Next Step in the Evolution Chain of [Market] Intermediaries? Available at SSRN 3427506 (3427506), 3–22.

Gordon, W.J.; Catalini, C. (2018). Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. Comput. Struct. Biotechnol, 16, 224–230.

Gorkhali, A., Li, L., & Shrestha, A. (2020). Blockchain: a literature review. Journal of Management Analytics, 7(3), 321-343.

Grech, A., & Camilleri, A. F. (2017). Blockchain in Education. Inamorato dos Santos, A. (ed.). Joint Research Centre. Online at - https://ec.europa.eu/jrc/en/publication/eur scientific-and-technical-research-reports/blockchain-education.

Greenspan, G. (2015). Avoiding the pointless blockchain project. Online at https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project.

Gregory, M., (2013). CoinJoin: Bitcoin privacy for the real world. bitcointalk.org

Moniz, H., Neves, N. F., Correia, M., & Verissimo, P. (2006). Experimental Comparison of Local and Shared Coin Randomized Consensus Protocols. In SRDS. 235–244.

He, X., Yi, J. & Chen, A. (2018). "Application Progress and Development Trend of Block Chain Technology," *World Sci-Tech R & D*, vol. 40, no. 6, pp. 615–626, 10.16507/j.issn.1006-6055.2018.12.007

Home Page, (2012). https://www.investopedia.com/terms/g/genesis-block.asp, accessed: 30/07/2019.

Homoliak, I., Venugopalan, S., Reijsbergen, D., Hum, Q., Schumi, R., & Szalachowski, P. (2020). The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses. IEEE Communications Surveys & Tutorials, 23(1), 341-390.

HSBC. (2017). Trust in Technology Study. Online at http://www.hsbc.com/trust-in-technology-report.

Iuon-Chang, L., & Tzu-Chun L. (2017) "Survey of Blockchain Security Issue and Challenge" in International Network Security journal, Vol.19, No.5, PP.653-659.

Jangirala, S., Das, A.K., Vasilakos, A.V. (2020). Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Mobile Edge Computing Environment. IEEE Trans. Ind. Inform., 16, 7081–7093.

Jung, T., Li, X. Y., Wan, Z., & Wan, M. (2015). Privacy preserving cloud data access withmulti-authorities. In Infocom. 2625–2633.

Korkmaz, U., Altunlu, H. İ., Özkan, A., & Karaarslan, E. (2019). Sustainable Member Motivation System Proposal for NGOs: NGO-TR. UBMYK.

Kristov Atlas. (2014). Weak Privacy Guarantees for SharedCoin Mixing Service.

Lamport, L., (1998). “The Part-Time Parliament.” *ACM Transactions on Computer Systems*, vol. 16, no. 2,, pp. 133–169., https://dl.acm.org/citation.cfm?doid=279227.279229.

Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems* 107 (2020) 841−853.

Lin, C.; Hu, H.; Chang, C.; Tang, S., (2018). A Publicly Verifiable Multi-Secret Sharing Scheme with Outsourcing Secret Reconstruction. IEEE Access, 6, 70666–70673.

Liu, A., Du, X., Wang, N., & Li, S. (2018). “Research progress of blockchain technology and its application in information security,” *Ruan Jian Xue Bao/Journal of Software*, vol. 29, no. 7, pp. 2092–2115, 10.13328/j.cnki.jos.005589

Liu, Z., Wang, D. & Wang, B. (2019). “Privacy preserving technology in blockchain,” *Computer Engineering and Design*, vol. 40, no. 6, pp. 1567–1573, 10.16208/j.issn1000-7024.2019.06.012.

Mohan, C. (2019). State of Permissionless and Permissioned Blockchains: Myths and Reality, BlueTalks @ Rio BNDES

Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. Internet of Things, 8, 100107. Money are challenging the global economic order”. New York: St. Martin's Press.

Monrat, A. A., Schelen, O., & Andersson, K. (2019). A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. IEEE Access 7, 117134–117151.

Mosakheil, J. H. (2018). Security threats classification in blockchains.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. bitcoin.org., https://bitcoin.org/ bitcoin.pdf, (2008).

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

Natoli, C., & Gramoli, V. (2016). The blockchain anomaly. In 2016 IEEE 15th International Symposium on Network Computing and Applications (NCA). 310-317. IEEE.

Nicolas, H. (2012). It will cost you nothing to ”kill” a proof-of-stake crypto-currency. Economics Bulletin, 34(2):1038–1044, 2104.

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research.

Opray, M. (2017). Could a blockchain-based electricity network change the energy market. The Guardian. July, 13.

Pascal, P. (1999). Public-key Cryptosystems Based on Composite Degree Residuosity Classes. In Eurocrypt. 223–238.

Peter, B., Dan L. C., Ivan, D., Martin, G., Thomas, P. J., Mikkel, K., Janus, D. N., Jesper, B. N., Kurt, N., Jakob, P., Michael, I. S., & Tomas, T. (2009). Secure Multiparty Computation Goes Live. 325–343.

Piscini, E., Dalton, D., & Kehoe, L. (2017). Deliotte, Blockchain & Cyber Security.

Rajput, U., Abbas, F., Hussain R., Eun, H. & Oh, H. (2015). "A Simple Yet Efficient Approach to Combat Transaction Malleability in Bitcoin," *International Workshop on Information Security Applications*. Springer International Publishing, pp. 27-37.

Ray, P. P. (2018). A survey on internet of things architectures. *Journal of King Saud University-Computer and Information Sciences, 30*(3), 291–319.

Reyna, A., Cristian M., Jaime, C., Enrique, S., & Manuel D. (2018). "On block-chain and its integration with IoT. Challenges and opportunities." *Future Generation Computer Systems* 88:173–190.

Ron, D., & Shamir, A. (2013). "Quantitative Analysis of the Full Bitcoin Transaction Graph," Internatonal Conference on Financial Cryptography and Data Security, vol. 7859, pp. 6–24, 10.1007/978-3-642-39884-1_2.

Ronald-Peter, D., Kelso, H. S., & Mark J. V. (2017). Crypto report research. Demelza Kelso Hays Research Analyst, IncrementumaG

Rosic, A. (2017). Proof of work vs proof of stake: Basic mining guide. Blockgeeks blog.

Salah, K., Rehman, M. H. U., Nizamuddin, N. and Al-Fuqaha, A. (2018). "Blockchain for AI: Review and Open Research Challenges," in *IEEE Access*, vol. 7, pp. 10127-10149.

Samonas, S., & Coss, D. (2014). The cia strikes back: redefining confidentiality, Integrity and availability in security. Journal of Information System Security, 10(3).

Sayeed, S., & Marco-Gisbert, H. (2018). On the Effectiveness of Blockchain against Cryptocurrency Attacks. Proceedings of the UBICOMM.

Sergey, G., Vinod V., & Hoeteck, W. (2013). Attribute-based Encryption for Circuits. In Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing. 545–554.

Shulman, R. (2018). How Millionaire Jeremy Gardner and Jinglan Wang Built the Largest Blockchain Education Network. Forbes. Online at https://www.forbes.com/sites/robynshulman/2018/02/16/how-millionaire-jeremy-gardner-built-the-largest-blockchain-education-network-around-the-world/#5a46fdc44288.

The Economist. (2015). The trust machine: The technology behind bitcoin could transform how the economy works, (accessed 2020-07 01). https://www.economist.com/leaders/2015/10/31/the-trust machine?fsrc=scn/tw/te/img/cover/st/thetrustmachine.

Thomas, McGhin, Raymond Choo, Kim-Kwang, Zhechao Liu, Charles & He, Charles, (2019). Blockchain in healthcare applications: Research challenges and opportunities, *Journal of Network and Computer Applications*, 135, pp. 62–75.

Tikhomirov, S., Voskresenskaya, E., Ivanitskiy, I., Takhaviev, R., Marchenko, E., Alexandrov, Y. (2018). Smartcheck; Static analysis of ethereum smart contracts. In: *IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain* (WETSEB), IEEE 9–16.

Tim R., Pedro, M., & Aniket, K. (2014). CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. 345–364.

Trautman, L. J., & Molesky, M. J. (2019). A Primer for Blockchain. University of Missouri-Kansas City Law Review, Forthcoming.

Usman W. C., (2017). The Double Spending Problem and Cryptocurrencies, (accessed 2020-07-01). https://ssrn.com/abstract=3090174.

Wani, S., Imthiyas, M., Almohamedh, H., M Alhamed, K., Almotairi, S., & Gulzar, Y. (2021). Distributed Denial of Service (DDos) Mitigation Using Blockchain—A Comprehensive Insight. Symmetry, 13(2), 227.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. MIS quarterly, xiii-xxiii.

Xiaoqi, L., Peng, J., Ting, C., Xiapu, L., & Qiaoyan, W. (2017). A Survey on the Security of Blockchain Systems. Department of Computing, The Hong Kong Polytechnic University, Hong Kong

Xu, J., Wang, S., Bhargava, B. K. & Yang, F. (2019). "A Blockchain-Enabled Trustless Crowd-Intelligence Ecosystem on Mobile Edge Computing," in *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3538-3547, 10.1109/TII.2019.2896965.

Yang, P., & Lida X. (2018). “The Internet of Things (IoT): Informatics methods for IoTenabled health care.” *Journal of Biomedical Informatics.* 87:154−156.

Yao, H., Mai, T., Wang, J., Ji, Z., Jiang, C., & Qian, Y. (2019). Resource Trading in Blockchain-Based Industrial Internet of Things. IEEE Trans. Ind. Inform., 15, 3602–3609.

Yassein, M. B., Shatnawi, F., Rawashdeh, S., & Mardin, W. (2019). Blockchain Technology: Characteristics, Security and Privacy; Issues and Solutions. In 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA) (pp. 1-8). IEEE.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (Big Data congress) (pp. 557-564). IEEE.

Zhu, J. (2019). “Blockchain: the cornerstone of digital finance,” *Informatization Construction*, no. 7, pp. 56.

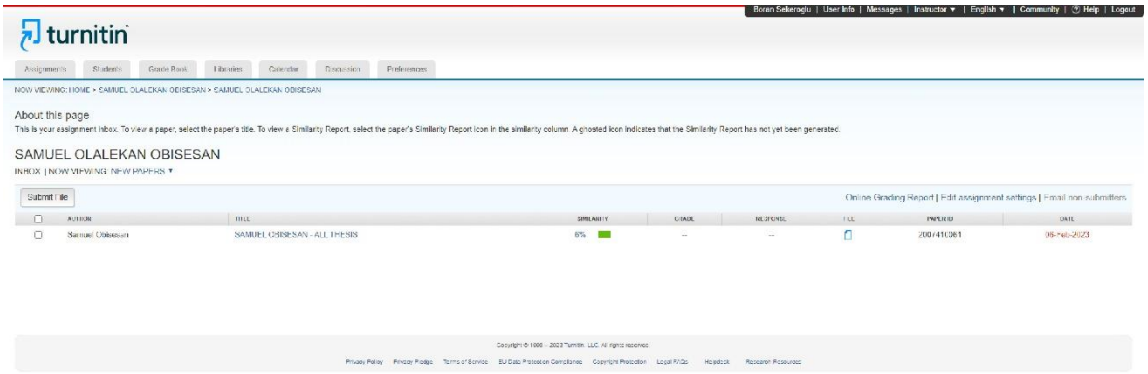
Zyskind, G., Pentland, A.S. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data.

Appendices

Ethics Approval

Appendix

Turnitin Similarity Report



ASSOC.PROF.DR. BORAN ŞEKEROĞLU