

Fall 2023

# Blockchain Securities Issues: Decentralized Identity System With Key Management Perspective

Olalekan O. Adaramola

Follow this and additional works at: <https://digitalcommons.georgiasouthern.edu/etd>



Part of the [Information Security Commons](#), [Science and Technology Studies Commons](#), and the [Technology and Innovation Commons](#)

---

## Recommended Citation

Adaramola, Olalekan O., "Blockchain Securities Issues: Decentralized Identity System With Key Management Perspective" (2023). *Electronic Theses and Dissertations*. 2657.  
<https://digitalcommons.georgiasouthern.edu/etd/2657>

This thesis (open access) is brought to you for free and open access by the Jack N. Averitt College of Graduate Studies at Digital Commons@Georgia Southern. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of Digital Commons@Georgia Southern. For more information, please contact [digitalcommons@georgiasouthern.edu](mailto:digitalcommons@georgiasouthern.edu).

BLOCKCHAIN SECURITIES ISSUES: DECENTRALIZED IDENTITY SYSTEM WITH KEY  
MANAGEMENT PERSPECTIVE

by

OLALEKAN OLA ADARAMOLA

(Under the Direction of Lei Chen)

ABSTRACT

Blockchain was created many years ago to solve the problems of data transfer Integrity, Several years later the issues persist. Blockchain securities are one of the most important considerations to be investigated, and data integrity is about ensuring the accuracy and validity of messages such that when they are read, they are the same as when they were first written. It is of the opinion that passing information across from one person to another cannot be the same as it was first said at the onset. Our work investigated Blockchain security issues, studying Integrity emanating from transactions across the blocks and how to deal with the securities issues. It also investigated decentralization and issues in blockchain to investigate how to mitigate the security issues associated with blockchain. It further discusses the use of key management in solving security issues in blockchain, viewing different key management systems of private and public keys, and solutions in addressing the blockchain problems. Lastly, we contributed the use of Decentralized Identity systems (DIDs) into the blockchain where we use a unique identifier, "ID.me" to verifier the individual credentials before any transaction, this was done by sending a digital ID through the issuer to the verifier to authenticate the integrity and identity of the holder and this proof worthy of protecting the information and maintaining the privacy of the user of the blockchain technology.

KEYWORDS: Blockchain Security, Decentralization, Integrity, Key Management, Decentralized Identity, Unique Identifier, Encryption.

BLOCKCHAIN SECURITIES ISSUES: DECENTRALIZED IDENTITY SYSTEM WITH KEY  
MANAGEMENT PERSPECTIVE

by

OLALEKAN OLA ADARAMOLA

M.S, Georgia Southern University, 2023

A Thesis Submitted to the Graduate Faculty of Georgia Southern University in Partial  
Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE  
INFORMATION TECHNOLOGY

STATESBORO, GEORGIA

© 2023

OLALEKAN OLA ADARAMOLA

All Rights Reserved

BLOCKCHAIN SECURITIES ISSUES: DECENTRALIZED IDENTITY SYSTEM WITH KEY  
MANAGEMENT PERSPECTIVE

by

OLALEKAN OLA ADARAMOLA

Major Professor: Lei Chen  
Committee: Yiming Ji  
Jongyeop Kim

Electronic Version Approved:  
December 2023

## DEDICATION

All glory and praise be to God, for his guidance, direction, and understanding of several topic areas through my master's program. Special appreciation to my family for the financial support in this thesis completion. Finally, I want to thank my faculty advisor for the intellectual support needed to complete this thesis.

## ACKNOWLEDGMENTS

This thesis could not have been completed without the contribution and help of several other people. The author would like to acknowledge the contribution of my committee professors, Dr. Lei Chen, Dr. Yiming Ji, Dr. Jongyeop Kim, and my fellow graduate students.

## TABLE OF CONTENTS

	Page
ACKNOWLEDGMENTS .....	3
LIST OF TABLES .....	6
LIST OF FIGURES .....	7
CHAPTER	
1 INTRODUCTION .....	8
Purpose of the Study .....	8
2 LITERATURE REVIEW .....	10
2.1 Blockchain Integrity is the reliability and trustworthiness of data.....	10
2.2 Blockchain Decentralization .....	15
2.3 Blockchain Key Management.....	23
3 BLOCKCHAIN INTEGRITY, SECURITY ISSUES AND SOLUTIONS .....	32
3.1 Introduction.....	32
3.1.1 Benefits of Blockchain.....	33
3.1.2 Types of Blockchain .....	33
3.1.3 Blockchain Security Issues .....	33
3.1.4 Blockchain Attacks .....	33
3.2 Background.....	35
3.2.1 Blockchain Integrity.....	35
3.2.2 Types of Integrity.....	35
3.2.2.1 Commission: .....	35
3.2.2.2 Omission: .....	36
3.2.2.3 Manipulation: .....	36
3.2.3 The Transfer Concept.....	36
3.3 Blockchain Integrity Issues.....	38
3.4 Method .....	38
3.5 Results and Conclusion.....	40
4 BLOCKCHAIN DECENTRALIZATION, SECURITY ISSUES AND SOLUTIONS.....	42
4.1 Introduction.....	42
4.1.1 Types of Decentralization in Blockchain .....	42
4.1.2 Benefits of Decentralization.....	43



4.1.3	Blockchain Decentralization downsides .....	44
4.2	Background .....	44
4.3	Methods.....	45
4.4	Results.....	49
4.5	Conclusion .....	49
5	BLOCKCHAIN KEY MANAGEMENT ISSUES AND SOLUTION .....	50
5.1	Introduction.....	50
5.2	Background.....	51
5.2.1.	Key management issues and solutions.....	52
5.3	Method .....	53
5.4	Results.....	55
5.5	Conclusion .....	58
6	DECENTRALIZED IDENTITY SYSTEM, DIDs .....	59
6.1	Introduction.....	59
6.2	Background.....	59
6.2.1	Global Unique Identifier .....	59
6.3	Method .....	60
6.4	Results.....	61
6.5	Conclusion .....	67
7	DISCUSSIONS .....	68
8	CONCLUSION .....	68
	REFERENCES .....	70
	APPENDIX A.....	75

## LIST OF TABLES

	Page
Table 3.1: Different Blockchains with transaction in a distributed Ledger .....	37
Table 3.2: Interpretation of the code and generated hash values. ....	40
Table 4.1: Scale of Decentralization.....	43
Table 4.2: Comparison between the Centralized system and Decentralized system of Blockchain.....	45

## LIST OF FIGURES

	Page
Figure 3.1: Blocks of Chains connected. ....	32
Figure 3.2: Simple chain transaction from user A to user B .....	36
Figure 3.3: Transaction among many users in the network being notified. ....	36
Figure 3.4: Synchronization of transactions in a ledger.....	37
Figure 3.5: Components of Integrity.....	38
Figure 3.6: Building blockchain with Python showing the transaction to be made.....	39
Figure 3.7: Printing of transactions in a blockchain across the users .....	39
Figure 3.8: Hash value generated showing various transaction values.....	40
Figure 4.1: Creating a decentralization chain transaction.....	46
Figure 4.2: Decentralization of Blockchain transaction.....	47
Figure 4.3: Payout code for the blockchain decentralization .....	47
Figure 4.4: Final deployment of the transaction into the contract .....	48
Figure 4.5: Compilation and solidification of the final transaction with each user being able to read.....	48
Figure 5.1: Simple frame of the encryption process in the network .....	50
Figure 5.2: Encryption of plaintext message to be converted into a cipher or encrypted text. ....	54
Figure 5.3: Decryption of the encrypted message from ciphertext into plaintext.....	54
Figure 5.4: Process of encryption and decryption of data.....	54
Figure 5.5: Generation of the printing of character string .....	55
Figure 5.6: Generation of the character and key strings .....	56
Figure 5.7: Shuffling code for the characters and the key .....	56
Figure 5.8: Encrypting message with cryptographic for transaction .....	56
Figure 5.9: Printing of Encrypted messages in plaintext .....	57
Figure 5.10: Plaintext input (encrypted message) output as ciphertext .....	57
Figure 5.11: Different ciphertext generated for every time the transaction is run. ....	57
Figure 5.12: Decryption of ciphertext into plaintext message. ....	58
Figure 5.13: Encrypted and Decrypted messages output. ....	58
Figure 6.1: Decentralized Identity model .....	60
Figure 6.2: Model of the Verification credentials with DIDs .....	61
Figure 6.3: Credential Verification with DIDs. ....	61
Figure 6.4: Creating ID.me account for Credentials Verification.....	62
Figure 6.5: Setting of email for account. ....	62
Figure 6.6: Account page creation. ....	62
Figure 6.7: ID.me with user's categories .....	63
Figure 6.8: Authentication Security creation .....	63
Figure 6.9: Account Verification Information page.....	63
Figure 6.10: Credentials Verification completed.....	64
Figure 6.11: Confirmed Verification for Users.....	64
Figure 6.12: Comparison of Different authentication apps on the blockchain. ....	66
Figure 6.13: Comparison of MySecure.IDs with Our ID.me used in the blockchain. ....	66

## CHAPTER 1

### INTRODUCTION

#### Purpose of the Study

Security issues are global, and this affects the use of blockchain technology, hence this study's purpose is to investigate the minimization of security issues in the Technology and proffer a better solution to this problem. This thesis work includes three research studies to demonstrate the working principles of Blockchain technology and the security issues, this investigates the integrity issues, the decentralization of blockchain, and the performance of key management functions in blockchain technology and the factors that are needed for smooth transactions during the working of the blockchain and bring about integrity and satisfaction from the users. The first research approach of the thesis investigates the Integrity of the transaction in the blockchain, which is paramount to the users within the network of the transaction, and this must not be compromised. Some of the transaction Integrity is already compromised, and this does not give the users a sense of security happening within the transaction, and this could result in losses of valuable and secret details. Given that, this thesis looked at criteria that could be responsible for security breaches in the blockchain. The second research in the thesis studied the decentralization Identity system in the blockchain, the types of decentralization, the importance of decentralization, and the challenges of decentralized storage within the blockchain. The third research study is based on the Key management performance in the blockchain, investigating the use of private keys, such as hash, to encrypt the blocks within the chain to prevent those who do not have authority within the network from venturing into the network and hijack or break the secure chain and thereby exposing the transaction to hackers and attackers. All three studies are conducted to determine the best way to secure the blockchain and prevent unwanted users from coming into the network of the blockchain, thereby breaking the security within the blockchain. This study aims to investigate blockchain technology security issues and analyze ways of minimizing the common issues available to the users with a lease of life. The decentralization Identity system analyzed the different types of decentralization, such as Politically and Architecturally centralized, the single unified entity, and politically and logically centralized. Key management involves the encryption of the data and the transmission of private keys from one user to another within the network, the symmetric and the asymmetric keys being the type of keys that are investigated and proposed one will be the best of the key. The use of a hashing algorithm will be employed. This research thesis is sectioned as follows: The literature review for the first, second, and third studies. This research thesis is sectioned as follows: The literature review for the first, second, and third studies is outlined. This is followed by detailed research and procedures in each study, starting with study one, study two, and study three. Lastly, we delve into Decentralized Identity in Blockchain.

### How This Study Is Original

The study deals with the security issues in blockchain and how to minimize them. The author reviews several past works and highlights what is yet to be done to reduce the problem blockchain technology faces and then proffers a solution. Blockchain technology is a revolution in the industry and education sectors and is being used for transaction purposes. It is expected to be more secure and accurate. The integrity of the blockchain, the decentralization, and the key management issues are investigated by the author with the use of key management in a decentralized identity system of the chain. This work looks into the use of a Decentralized Identity system, DIDs in the blockchain implementation, with the integration of an authentication app. ID.me which is different from all other authentication methods earlier used in blockchain technology in the sense that it can carry out total verification of users' credentials such as date of birth, job, email, etc. as opposed to some earlier ones that you can sign in to the blockchain with just an email.

## CHAPTER 2

### LITERATURE REVIEW

#### 2.1 Blockchain Integrity is the reliability and trustworthiness of data.

Wang et al. (2021) discuss the problems and threats of the blockchain system by focusing on analyzing the innovative technologies involved in blockchain security and privacy protection. Blockchain is known as a decentralized, verifiable ledger and non-tamperable that is used in recording transactions of digital assets and then making sure of the transaction record non-tamperability. This scheme is used in different fields such as medicine, education, and government. Research is currently on the security and privacy of blockchain, therefore, to build a blockchain industry ecology there is a need to accelerate the deep integration of blockchain and innovative information technologies. The technology includes artificial intelligence, the Internet of Things (IoT), and big data, this promotes integrated innovation and integrated application and achieves blockchain.

Paduraru et al. (2022) propose Game Blockchain, an open source blockchain framework designed to support secure transactions of NFTs in modern computer games as a framework to link game development with blockchain technologies to enable a trustworthy way of transacting assets and a more secure way between content developers and users. In this work architectural decisions were made through the observation of the gaps in the current tools after discussion with the stakeholders and usability and performance were tested with a publicly available demo in an Unreal Engine, the purpose being to allow game industry stakeholders like content creators, game developers, and regular gamer to create and exchange the game assets in a more secure and well-trusted environment. The paper highlighted the improvement of the security of the traditional database, the dangerous user behavior, and the potential data tampering by blockchain technology which is used in recording the critical operations in a ledger and preserving the user identity regularly all the time. From the technical in look into the scheme, the aim is to provide an architecture that can be used easily, which is flexible, understandable, and with an extensible SDK, In this framework, game developers and regular users will create and trade assets freely without the third-party providers, it used all related services in the game interface itself and not switching from applications or pay additional transfer fees to providers. The development of games is encouraged with shared marketplaces and wallets for both developers and users making it so easy to monetize assets and services.

Niavis and Loupos (2022) Introduced the ConSenseIoT algorithm, a consensus algorithm designed to improve the integrity of blockchain transactions in distributed IoT networks the design of the

ConSenseIoT algorithm is used to achieve this scheme, and the performance of the network is not affected, and less energy is consumed. The major concern on the Internet of Things ecosystem is Data protection and privacy, excessive use of IoT devices may risk the security of the network. Trustworthiness is enhanced with the use of Blockchain technology to eliminate trusted third parties when mechanisms are provided to reach consensus in a trustless participants network. The general algorithms employed in blockchain architectures ensure the integrity of the data stored in the blockchain, the resiliency of the network, and manage the security of devices. The ConSenseIoT is helped by a popular consensus algorithm which is a PoI algorithm, and this incorporates the most important characteristics needed in a secure and trusted blockchain in the IoT ecosystem. The existing solution to the problem inspired the algorithm by employing decentralized identities, and decentralized trust management. The ConSenseIoT employs, decentralized identity management assets i.e., DIDs and VCs, the outputs of a trust management mechanism and, insights from existing consensus algorithms towards an integrated scheme that puts the device's importance at the Centre of the computations. This ConSenseIoT algorithm uses a decentralized approach to accomplish the identity management of the devices by adding on the overall privacy features of the approach lastly the algorithm combines technologies for operating in a distributed manner which favors the scalability and allows the effective integration in large-scale networks.

(Zhao et al.) presented a dynamic security mechanism for lightweight IoT device's access to blockchain services therefore a design based on a blockchain SDK proxy node is proposed. The Internet of things (IoT) devices are unable to a full blockchain node or a blockchain software Development kit (SDK) client because of limited hardware resources. IoT lightweight devices will connect to blockchain services efficiently and safely to boost the blockchain applications in IoT scenarios and let the devices securely connect to blockchain services. The blockchain SDK proxy node runs the blockchain SDK client and the IoT devices need to construct and sign the blockchain transactions by sending the signed data through an Application Programming Interface (APIs) used by the proxy node. This proxy node forwards the data to the blockchain network, and a static proxy node will become the single point of performance bottleneck and failure, this is vulnerable to DDoS attacks. To improve security, a mechanism of dynamically selecting a proxy node is designed to make IoT devices access blockchain services safely and efficiently and the outcome of the scheme work was able to use the mechanism to solve the problem of single point of failure and performance bottleneck.

Zhao et al. (2021) Investigate the Blockchain interest growth in the industry and academic sector has improved the way we see and visualize transactions and keep the information, and Security and privacy

issues are at the center of an investigation in the blockchain. The work investigates the security and privacy of blockchain, firstly looking at the blockchain utility in the context of bitcoin-like online transactions, also about the security properties and presenting the additional security and privacy properties needed in blockchain applications. The work reviews security and privacy techniques for achieving security properties in a blockchain-based system which comprises hash-chained storage, mixing protocols, and anonymous signatures, among others. The outcome of the review shows that an in-depth understanding of the security and privacy of blockchain can be obtained concerning attributes, techniques systems, and concepts.

Lee and Kim (2021) work is on blockchain technology as an emerging technology used for security in defense by ensuring data processing integrity and significantly scanning system reliability from attacks of cyber threats. The research focused on the coverage of cyber defense and blockchain received by conducting research and development under the defined cyber defense. The work is done by investigating the potential concerns in blockchain usage from the recent technology reviewed and this helps in reducing the gap in blockchain for cyber defense in conclusion the work was able to highlight the involvement of government plan in promoting blockchain and to show that it is helping to play a vital role in cyber defense.

Lee and Kim (2021) investigate vehicular network (VANETs), just like every other technology is made more secure using blockchain technology, it has various characteristics that meet some of the essential security requirements like decentralization, public audit, tamper-proof nature, and transparency, among others. This survey analyses several blockchain-based security vehicular networks, which are classified into three different perspectives, namely (i) application perspective, in which the studies are classified based on application considered such as data trading/sharing, resources sharing, parking and traffic management (ii) security perspectives, where studies are classified looking into the security requirement of the network by considering the protected security attacks, also the authentication techniques and the security proofs. (iii) blockchain perspective, using the blockchain platform and consensus algorithm used. Simulation tools were used in blockchain-based vehicular networks and the work provided insight into the roles of other technologies to secure blockchain vehicular networks, such as cloud computing, fog computing, edge computing, software define network (SDN), Named Data Networking (NDN), Artificial Intelligence, 5definesg several others. The blockchain security framework uses some other technologies such as low latency, low computation, and data storage among others to meet the requirements. In conclusion, the author was able to list out the major challenges and future direction in this domain.



Choi et al. (2020) propose a novel system to monitor the data integrity of Programmable Logic Controllers by using Blockchain technologies. Considering the use of a Nuclear Power Point environment they developed a blockchain system for monitoring the data integrity of the PLCs, and this helped in overcoming the limitation of applying blockchain to the cybersecurity of the NPPs. Information Technology (IT) systems have different operational environments compared to the Nuclear Power Plant (NPPs), as the NPPs are safe from external cyber-attacks, it was later proven that isolated networks are prone to attacks from cybercriminals. For the safety of the NPPs system, the Programmable Logic Controllers (PLCs) attacked by malicious data injection attacks are deployed and these are critical to nuclear facilities just like the way they attack Stuxnet. Hence there is a need for proper monitoring of cyber-attacks on the integrity of data of the PLCs which includes the modification of deployed logic or setpoints. The Reactor Protection System (RPS) was monitored by the integrity monitoring system, using the developed blockchain, and this is used to detect cyber-attacks like false code injection attacks on PLCs and then monitor the compromising in real-time on any of the PLC's integrity. An experiment was performed on the PLCs developed system using a false data injection attack and the outcome results show that this developed system was able to monitor the modification of data in the PLCs successfully. This blockchain system can be extended to monitor the integrity of other control systems.

Pinheiro et al. (2020) discuss Cloud computing (CC), an environment provides on-demand access to computational resources which includes application storage, servers, and many more services that the user can aggregate or release. Cloud computing adoption solution is a reality in government agencies both for small, medium, and bigger companies for easy procurement and several available services, with its low cost compared to management of infrastructure and the acquisition. Customers can create cloud services in centers with distributed cloud data, process and store their data, and effectively run the applications after deployment. One of the most used services for cloud computing services is cloud file storage with security of the storage being an essential subject, most importantly the data integrity, Cloud Computing services therefore allows and follows a business model that charges the customer using the computing resources that has been contracted out by the customer and its being manage through standardized web services. This paper proposes a solution based on the use of blockchain technology to help store files in the cloud storage service (CSS), and the monitoring integrity of files in the cloud using smart contracts in blockchain Networks computational trust, and symmetric encryption. The work used a protocol that provides decentralization, confidentiality, audit availability, and secured sharing of file integrity results monitoring and avoiding the overloading of the involved services. Also, the unabridged implementation of references was used to validate the work proposal and the work shows the use of a storage infrastructure in a BN that gives assurance of security, transparency the audit performance possibility and they did the decentralization of integrity and automation check result analysis process

that does not allow the collision between the ICS and the CSS. The paper also talks about decentralization and sharing of the trust level calculation process through an SC preventing ICS attacks against the CSS reputation with the management automation of the integrity file contracts verification which allows ICS replacement without interfering in the security process. The results of the work after the validation show that the solution is feasible and faultless in detecting corrupted files and this also confirmed the sharing integrity monitoring of the results together with the significant increase of the efficiency of the proposed solution and the application of computational trust techniques.

Rodrigues and Rocha (2021) Blockchain is being used in the technological world for the transaction of cryptocurrency from one unit to another and the issue being faced includes security, integrity, and authentication among many others. The blockchain is being considered for suitability for the Efficiency and data integrity of IoT ecosystem transactions. This work analyzes the effectiveness and deployment of blockchain technology in the implementation of the IoT ecosystem database. The work assesses how the processing efficiency transactions started from the use of smart devices and the stored data integrity, they carry out this efficiency using queue theory based analytical modeling, here the minimum duration is estimated for confirmation of the transaction. Later in the work the data integrity is then measured by simulations in which case the probability of a fraudster changing the stored data is then estimated, this is done using sets of scenarios related to different application domains. The outcome of the work proves and shows that the Blockchain technology may meet the IoT efficiency requirements, aside from providing adequate data integrity.

Merugula et al. (2021) Uniquely, the Blockchain attention across all sectors, researchers, practitioners, and organizations is due to the special features such as security, reliability, decentralization, and the integrity of the data. Even with the ongoing and many other interesting features of Blockchain, little is still being recognized of the usage and benefits of the Blockchain technology. Blockchain comprises frames of cluster information, this is purely a network of structure information and contains peer-to-peer purchases. The blockchain compatriots need an encrypted crucial to approve the payment and in addition it executes a utility operation, and it functions as a financial institution in which cost exchange is highlighted. This work did a review and study on Blockchain as related to education software, it does this by looking into three major concepts, the academic apps which is formed with Blockchain, the advantages and approaches of implementing blockchain and innovation of the same in schools and, lastly the blockchain issues. The framework is well reviewed with a good outcome of all the observations, it is then analyzed, and this analysis gives insight into some aspects of learning which are gained through the innovation of blockchain. The review looks at the funding issue of the small and medium-sized enterprises (SME) which is a challenge for the upcoming nations that of the financial regions in some

developed countries and the growing economies, reserved for SMEs in current history. The work review that the development of prime business which are devoted to that of the small and medium size business is seen as a good option for the prevailing new investment, with a significant possibility in the organization and business sector. These innovations were seen not to be manipulated or tampered with and it might be an advantage to help the small market indexes and very reliable, low cost, effective method for registering goods and the buying of commodities, in conclusion the work was able to show that blockchain technology make good use of the fund payment and also exchange of equity, this is done by purchase among small and medium-sized enterprises in order to achieve exposure and exceptional motivations to get instant feedback.

Zaman and Min (2020) works deals with a novel idea of a Blockchain Consensus system for universal types of data, the mechanism is designed to allow most of the devices and entities to participate in the mechanism and do low computational validation, then a two-step validation process is introduced to this system to add extra layer of security. Blockchain systems are platform for data storage, and the increase in data allows third-party cloud storage to be extremely popular with blockchain being used to eliminate the dependency on any central power/ authority to increase the security, data retention probability, privacy and to eliminate single points of failure. Blockchain can manage growing data in the blockchain, that is the scalability, latency, and the network speed. Blockchain and its problems have an optimized tradeoff between its characteristics, and the blockchain can be used as an ideal candidate to replace the centralized cloud-based data storage. In the work a framework of the consensus mechanism was designed for the Blockchain based distributed storage, the work then analyzes the consensus mechanism with a game theory by predicting behavior or methods of the consensus participant in various situations calculated using the Nash equilibrium. The author also used queuing theory in analyzing expected congestion which will help in detecting all usual activities going on within the network and thus provide the information to the participants. The outcome of the work shows that by using a proper acceptable mechanism, the entities in the system will not launch any attack nor will they misbehave, and the queuing theory can be used by prospective users of this consensus mechanism as a supporting tool in getting some knowledge about the congestion and delay for waiting in the network.

## 2.2 Blockchain Decentralization

Blockchain Decentralization is a simple way of transferring control and decision-making from a centralized entity, such as an individual, organization, or group, such blockchains are designed in a way to makes it difficult to alter, and once the data is entered it is irreversible. For a decentralized blockchain network, no user must know or trust anyone else and in such a network, each member has a copy of the

exact same data in the form of a distributed ledger. When any member's ledger is changed /altered or corrupted in any way, most of the members in the network will know and reject the transaction.

Tang (2021) Investigates the application of blockchain in taking care of diploma fraud by investigating a blockchain-based system that falls short of meeting the requirements. Blockchain technology development is used in the cryptocurrency system and Bitcoin as one special case of distributed ledger technologies (DLTs) with a decentralized database used in computers to record data details and share the details with synchronized digital transactions. This is used to propose a solution using blockchain to facilitate and leverage basic data structure and cryptographic primitives and investigate computational complexity and demonstrate its practicability. The work was able to show the proposed solution with respect to all identified requirements and how the design can be used to enhance security and privacy.

Bhutta et al. (2021) Blockchain technology's impact on modern society is of importance and this is evident in the cryptocurrency due to its transparency and decentralization and for the sole essence of its securities capabilities, hence this work provides a comprehensive survey of the evolution of Blockchain technology with the developmental framework, the architecture, and several securities issues and also look at the analysis framework, with the classification of algorithm consensus and security risks coupled with the primitive cryptographic used in blockchain at the moment. In conclusion, the paper provided a detailed analysis for the future and made open further research provisions for researchers to investigate the challenges faced by Blockchain technology users.

Kwon et al. (2019) For traditional currencies, there are many issues such as single-point corruption and failure, and the proof-of-work mechanism is used by Bitcoin in which the nodes earn rewards when their computing resources are used. Bitcoin makes use of blockchain technology which is a public ledger used to store the transaction details and the nodes contain the history on the blockchain using blocks through a consensus protocol. Since bitcoin adopts this consensus protocol by making use of the proof-of-work (PoW) mechanism where nodes use their computational power to participate. Decentralization of digital currencies has received a good amount of time, and no business or organization controls the system but in the case of the traditional system, it is possible. Poor decentralization does not affect only PoW Bitcoin but all the cases that adopt proof-of-stake (PoS) and proof-of-stake mechanisms. This paper investigates the centralization problem in the consensus protocol. In this work the author defines  $(m, \epsilon, \delta)$ -decentralization as that in which are at least  $m$  participants is running a node, and the ratio between the total resource power of nodes run by the richest and the  $\delta$ -th percentile participants is less than or equal to  $1 + \epsilon$ . Using this the working proof that  $m$  is sufficiently big and  $\epsilon$  and  $\delta$  is 0, which means the

decentralization is full decentralization as an ideal state, it also introduces an incentive system condition for achieving good decentralization of the blockchain  $(m, \epsilon, \delta)$ - and if this condition is satisfied then the blockchain has reached a full decentralization having the probability of 1. To achieve this probability, the blockchain system must assign a Sybil cost (this is the difference between the cost of one participant running many nodes and the overall cost for multiple participants in which each is running one node). The results of the work show that it is difficult to design a system that can achieve well with good decentralization in the consensus protocol and not rely on a TTP contradicting each other. This result shows that if the gap between the rich and the poor in the real world cannot be reduced and Sybil's cost cannot be assigned without relying on a TTP, a high level of decentralization in systems will be limited in occurrence with a high probability.

Meurisch et al. (2020) Privacy invasion is related to the way user services work with actions based on the AI model to offer personalized and initiative-taking support. A continuous flow of personal data is needed for the AI algorithm which leads to issues of privacy because the user will have to share the data out of the required space. The work presents PrivAI as a design platform and decentralized privacy platform in overcoming the sharing need of user data. PrivAI is used together with the already available approaches to the personal data store and at the same time enforces the stationary of raw user data, PrivAI also investigates the resulting challenges by dividing the AI algorithm into cloud-based general model training. It also helps in loading AI models into a trusted environment for execution in which the provider's intellectual property (IP) is protected. All these were achieved by confining personal data which are stored as the solid foundation for data sovereignty and by two newly integrated mechanisms which are divisible AI algorithms and PDS-internal/external confidential processing. This shows accurate classification results and a good reasonable overhead performance for AI-based services. The results highlight the promising way in which data decentralization can be used for privacy-preserving AI services without violating the intellectual property of providers. The outcome of the work highlights the effectiveness and feasibility when comparing the performance to currently practiced approaches.

Monte et al. (2020) Public blockchain's scalability is particularly important for their success and it should be used to scale according to the number of nodes and transactions workload. The scalability of blockchain is informally conjecture and the related scalability, security, and decentralization (trilemma) stated that if there is any improvement in any of these aspects it will impact negatively on either of the other two or on both. This work describes a different blockchain architecture that measures high workload provided that an equal increment of nodes is provisioned. The work uses a design novel blockchain to distribute the burden and create a next block in May parallel executing committees that contain all nodes and avoid broadcast in all areas that are critical for scalability. The work further

discusses the scalability of their approach and how it does not affect decentralization and security, this proves that the architectural design is a solution to the blockchain scalability trilemma. The work shows that the approach does not require tradeoffs on decentralization or security.

Cao and Zhao (2021) Digital content production evolved from the expansion of the internet business and improvement in steaming media and compression technology, and this is disseminated and consumed every day at a faster rate. The digital feature, the contents all face the risk of infringement like attacks and unauthorized dissemination, or malicious tampering. Digital Right Management (DRM) is a critical technology to improve the security and flexibility of digital copyright registration and distribution. It is responsible for monitoring the entire life cycle of the registration, transfer, consumption, and use of digital content to protect the legitimate rights and interests of various stakeholders Liu et al. (2003), Subramanya and Yi (2006). This work proposes the use of DRM to solve the disadvantages of centralization with a decentralized key distribution system designed based on blockchain technology and the system data and services are maintained using centralized nodes. In the work, the design of an encryption mechanism based on zero-knowledge proof technology was used to solve the trust problem in the key distribution content by allowing the verification of the encrypted results and not exposing the secret value. The zero-knowledge-proof technology was used to prove the correctness of the encrypted key contents and not reveal it to the public, blockchain technology is used to achieve key distribution decentralization and not trust each other and prevent attackers from attacking the system. Blockchain technology is used to decentralize the key distribution and both the consumer's application and the agent's encryption are overseen by the blockchain network in which the data forged locally is difficult to verify by all other nodes and thereby will not be recorded on the chain. The damaged nodes do not affect the security and stability of the system and unwanted users who want to attack the system cannot gain access by deceiving the rightful users the system was able to use other DDRM systems to take care of the issues of key distribution to achieve complete decentralization.

Zeng et al. (2019) Blockchain technology is a groundbreaking innovation, and it can change the way humans do business and think about transactions of Bitcoin and cryptography. It can transact business from peer-to-peer with any third party being involved. Shuai et al. (2019). One of the common problems of Blockchain technology is privacy issues, this is a major problem that calls for attention to the existing centralized online social networks (OSN), and this leads to research going on in the decentralization framework for online social networks. The OSN is an important aspect of the online activities that internet users use such as web, Facebook, etc. which attract lots of users with great achievements recorded but the issue of centralized design needs to be investigated due to its control over user-generated content. Decentralized social networks enable the users of networks to have access to a better

environment in which they can have their privacy protected with secure information dissemination. The paper proposed a novel decentralized social networking architecture enhanced by blockchain technology. It uses a sharding framework to increase the scalability of the system and a blockchain system to ensure that the information within the network is secure, thereby having integrity and consistency which is a reputation-based authority control method used to improve the whole system's security. The sharding is divided into two sections, the first layer being the main chain and for each shard state, the hash function is used to calculate a correlative number, and this is further recorded in the blocks of the main chain. The second layer has several shards and each of these shards builds a sub-chain with each post of users, a hash function is used to calculate a number to record into its own sub-chain. The proposed methods were able to show that Blockchain technology power can revolutionize various areas of the economy and society.

Saha et al. (2021) Blockchain Technology is used to store data in a public ledger, and this is a growing technology which started at the turn of the 20th century when a group of researchers cooked up the idea of the blockchain to timestamp the digital documents that have been lying idle for many years and this idea was used by Satoshi Nakamoto in bitcoin later. One of the issues facing blockchain is security and this is why decentralization and transparency are used to provide wide acceptance in various sectors through different applications. The security aspect of blockchain is maintained using various cryptography techniques. The change in basic assumptions from the time of pre-quantum to post-quantum time necessitated new cryptographic developments that are big against quantum attacks and applicable in blockchain for post-quantum decentralization. This work investigates and presents a solution for post-quantum decentralization in blockchain using lattices with polynomials for identity-based encryption (IBE), then allocated signature for the consensus to make sure the efficiency and suitability in post-quantum blockchain applications is maintained. This approach was implemented based on delay, throughput, energy consumption and complexity, and the outcome of the work shows that the comparative results obtained are efficient and so that the work presented is efficient.

Lin et al. (2020) Software-as-a-service (SaaS), a subscription-based pricing model is used for monetizing the subscription and enables the payment of data streams with data usage instead of a particular price for a fixed data set, For a better vision managing budget and for data consumers to have a flexibility to subscribe and unsubscribe. The streaming data, unlike static data collections increases difficulties of dynamic data ownership and identity classification and this means trustless data infrastructure for trading is necessary for the entities to trade, ownership data validation, and data integrity even without having trust in any participant and this also include the automated subscription procedure being demanded for the sake of data monetization. The work aims to propose a highly decentralized and autonomous

subscribe model to be able to combine both the trading and data storage to give the consumer and data provider the digital right during dynamic data streaming. This work proposes the use of distributed ledger technologies (DLTs), to build a decentralized data platform for trading on top of the IoT brokered infrastructure. The work stored the data stream on the Tangle and transmitted it through MAM and automated by Ethereum smart contract design for the process, this was then compared with other works to identify a trustless data trading infrastructure, ensure scalable IoT-based data sensor confidentiality, consolidate the economic incentives in the entire ecosystem. The method can efficiently enhance the degree of transparency and scalability and the storage which was built upon the cryptographic message protocol enables the transmitting, validating, and accessing of streams over distributed ledgers without permission from authorities and the digital rights of trading participants are guarantee and enable by design. The work finally considers the workload heaviness of the low-level sensors and conducts and experiment to authenticate the data providers to delegate the MAM operations to access and then come to the conclusion that the performance of the E2EE approach employed is better than that of the MMM solutions, so a decentralized model allows the data streams trading by shifting risks with corresponding digital right of every participant deserving a guarantee, provided by the automated system.

Febrero and Pereira (2020) Blockchain, distributed database structure, cryptocurrency protocol and Bitcoin are all similar Fani et al. (2019), the blockchain is a universally acceptable system for the cryptocurrency protocol and this is not the only existing database structure or the only cryptocurrency protocol. There are several distinguishing technological components gifts and consensus mechanisms for cryptocurrency protocol and distributed ledgers, these technologies intercept and this does not make the cryptocurrency protocol different from all other available protocols and currencies it makes them available, secure, also being inclusive, transparency, integrity, authenticity, accountability, and confidentiality. Corbet et al. (2019), Biswas et al. (2017), Vigna and Casey (2015). Cryptocurrency protocol is fueled by cryptocurrency incentives, these incentives make the nodes do transactions in a peer-to-peer (P2P) network, using a unique consensus mechanism to reach an agreement on the state of cryptographically secured transactions of the distributed ledger Davidson et al. (2018), Catalini and Gans (2017), Pereira et al. (2019), works is to map cryptocurrency protocols across three major defining dimensions, these are governance decentralization, security, and scalability. They deal with the theory about the organizational and technological features which affect the three mentioned dimensions, and the features contain the validation network, the size of the network, resource expenditure, roles permissiveness, and transactions number per second. They map cryptocurrency constellations using their consensus mechanisms, also looking, at and discussing the organizational and technological features of different protocol applications conclude with their role and experience, and play with the tradeoffs among governance decentralization, security, and scalability. The work came to the outcome of the



analysis of cryptocurrency protocols builds on and expands the CAP theorem. Brewer (2000), one of the reviews works proof that a decentralized storage system cannot have consistency, availability, and partition tolerance, at the same time, this theorem applies to distributed systems at large with variation in dimensions applying to cryptocurrencies which others do not.

Jia et al. (2022) Blockchain technology deals with decentralization, immutability, confidentiality features which are used in auditing by many applications, but sometimes the immutability is limiting such application of the blockchain technology. Immutability limits the redacting of vulnerable smart contracts on the blockchain. So many available redactable solutions of blockchain will either have low efficiency or violate decentralization features and the solutions lack mechanisms for tracing the redaction history and block consistency checking. This work presents an efficient redactable blockchain that has traceability specifically in a decentralized setting, the traceability issue was solved using the design of a new structure to link the redaction history of a block to form a redaction chain and it proves that the design is compatible with the most available blockchain systems. The work is about using the decentralization chameleon hash function to tackle the trust party problem for the redactable blockchain by the assumption that all redactable action must be approved by multiple blockchain nodes, it designs a redactable structure of blockchain which takes care of all redactions of a block and encodes the redactable blocks into RSA accumulator. This redacting of a block used the threshold blockchain nodes to work in collaboration with the chameleon hash key and record the redaction request and history, then insert the redacted blocks into the RSA accumulator to check if it is redacted. It also discusses the efficient block consistency checking protocol to solve the block consistency issues which is based on the RSA accumulator and lastly, they conduct experiments to compare with some other decentralized redactable blockchain to justify our solution in practice and the outcome demonstrate that the redactable blockchain is highly effective in practice.

Pal et al. (2021) The work investigates the blockchain and analyzes the existing Public Key Infrastructure, (PKI) for blockchain and the key management of the blockchain. It went on to discuss the blockchain technology used in IoT systems and discusses key management, such as key management for Bitcoin wallet and PKI. Decentralization of a ledger or blockchain technology can eliminate third party requirements to allow the per-to-peer network transaction validation and the data stored in blockchain are in a decentralized state in the network, with the hash of the transaction stored as a ledger and are available to every user in the chain network. Decentralization of blockchain technology allowed the storage to be possible by making it difficult and tougher to change data at so many points along the chain transaction, thus, enabling higher cryptographic security as compared to all other centralized storage systems. The paper was able to come up with reliable and tremendous potential to change the

existing ideas of businesses, financial services, agricultural services, health services, e- governance services, among others.

Lehto et al. (2021) proposes the introduction of an implementation that generates and maintains the private key in an Intel Software Guard Extension (SGX) enclave using the private key in a process isolated from all other processes running on the same system and provides a method that enables the secure storage and recovery of a back-up key to an external repository and from an external repository by using an end-to-end secure connection. Traditional centralized internet services and third parties authenticate transactions of users and an important attribute of decentralized blockchain networks is the unrestricted and secured access to the user's private keys which are often threatened for several reasons. Generally, a system based on blockchain technology is prone to users losing access to their keys, either due to theft, loss or broken and one proposed application, with which this technology could be exploited, is the social wallet. The paper outlined the risks related to the current blockchain key management environments and introduced the Shamir's Secret sharing implementation-based method to implement the distributed key backup. Secure hardware (Intel SGX) was used to avoid all sorts of risks that are present in modern computational environments. The fundamental issues addressed by this Crypto Vault solution are key back-ups and key recovery such as when a device and the keys to decode it are lost or broken.

Shu et al. (2021) This work proposes a blockchain-based decentralized public auditing (BDPA) scheme in which they utilize a decentralized blockchain network in undertaking the responsibility of a centralized Third-Party Auditor (TPA) and mitigate the influence of tempting auditors and malicious blockchain miners by taking the concept of decentralized autonomous organization (DAO). The Public auditing schemes for cloud storage systems are being explored critically and widely due to the increasing importance of data integrity. TPA is introduced in public auditing systems to verify the integrity of the outsourced data on the user's behalf. To avoid malicious TPAs, several blockchain-based public verification schemes were proposed. But the existing auditing schemes rely on a centralized TPA, and they are vulnerable to tempting auditors who may align suspiciously with malicious blockchain miners to give outcome of biased auditing results. The detailed security analysis shows that BDPA can be used to preserve data integrity against those types of tempting auditors and malicious blockchain miners. They implemented each algorithm in BDPA and analyzed its performance in comparison with the existing schemes. A comprehensive performance evaluation demonstrates that BDPA is feasible and scalable by using this scheme and the work was able to prove that the security of BDPA against malicious cloud servers and the untrusted blockchain nodes is possible and the BDPA scheme has acceptable performance with scalability, availability, and better security against tempting auditors.

### 2.3 Blockchain Key Management

Public Key Infrastructure (PKI) is used in Blockchain Technology to authenticate the entities and to ensure the integrity of the blockchain, Pal et al. (2021). A challenge in the blockchain using an efficient cryptographic system is secure key management, if it is not well managed and an intruder discovers the keys by any unscrupulous means such as weak encryption, brute force, side channel attack, and physical access to the system, the intruder can have access to the blockchain without any blockage.

Ma et al. (2019) proposed a novel blockchain-based distributed key management architecture (BDKMA) and they do these by using a novel blockchain concept with cloud computing and fog computing which are introduced in satisfying well-formed audibility, decentralization, very high scalability, extensive requirements, as well as maintaining the principle of privacy to achieve a hierarchical control of the access in IoT. The fast method of the development of the Internet of Things (IoT) together with the rapid growth of essential data coming by user equipment brought about the great and strong request for hierarchical access control performed from a group communication perspective. However, the key management procedures for such to take place in the future Internet are essentially on a trusted third party, requiring the full trust of the key generation center (KGC) or central authority (CA). In the work they designed a system operation method introduced authorization assignment modes and reinforced the extensibility the group access pattern, the network is then split into different side blockchain using those sides blockchain are then properly maintained in each domain by the SAMs and the cloud is used to store the multi-blockchain to support the cross-domain interaction. The results from the evaluation performance of the architecture proposed when compared with the other existing models with various performance measures show the simulation of the multi-blockchain shapes improves system performance at a great level with excellent scalability when the size of the network increases and the rate of adjustment of dynamic transaction collection time allows the system capacity and performance to be improved when used in different types of environments.

Lou et al. (2018) proposes a Blockchain technology using a named data networking key management system, here they use the advantages of blockchain in proposing the verification methods and the key signature like partial decentralization. The Named Data Networking (NDN) is built with security requiring every of the named Data objects to be digitally signed by its producer. This project uses a key management model on an NDN testbed in order to verify the Data packet which is immune to the distribution of poisoned content However in real use, the model has two challenges to verify fake

contents, (1) the centralized architecture easily leads to a single point of failure, especially when the root key fails, it is difficult to verify the keys across sites due to the lack of trust between them, and (2) excessive overhead of certificate chain traversal when verifying the signature. The author uses a key management blockchain-based system in NDN to address the lack of mutual trust problem among sites without trust authors. With this scheme, a flat hierarchy reduces the number of authentication keys and signatures, and the hash storage way is used to replace signatures while the way of query and comparison to hash is used to perform verification of the signatures which allows the reduced computation cost when compared with the public key cryptography. All the site nodes form a permissioned blockchain for storing public key hashes to ensure authenticity and reduce the frequent communication between the blockchain and the router, likewise, the NDN public key object contents, storage, verification, and revocation are all re-designed. The outcome of the work shows that this proposed scheme can allow verification numbers to be reduced and have an extremely high efficiency.

Tian et al. (2020) propose a secure key management scheme based on blockchain (BC-EKM in DWSNs). The BC-EKM used blockchain networks to handle registration lists and cluster lists through consensus protocol. The dynamic wireless sensor network is an important means of industrial data collection which is a key area of the industrial Internet of things, IoT, in which the important characteristics of trustworthiness are secure key reliability. In achieving the goals of trustworthiness, the author used blockchain networks which consisted of H-sensor nodes in place of most work of the Base Station in the scheme of the work. Due to the dynamic, the security of key management is caused by a nontrusted base station, (BS) easily targeted. For the key management scheme distribution, galvanized Bases Station causes additional and heavy overhead on sensors, and in solving this problem a blockchain-based secure key management scheme (BC-EKM) is used. They constructed a blockchain based on a hybrid sensor network to implement key management with a design to ensure the formation of cluster algorithm and secure node movement algorithm. In their security analysis, the scheme was resilient against the pseudo-BS attack, and node compromise, and Simulation experiments showed good performance regarding the storage overhead and energy consumption. The stake blockchain is used as a trust machine to replace the functions of the Based Station and is finally used for the conduction of security analysis and ample simulation. The outcome of the work shows that the BC-EKM scheme is effective and efficient, and better suited to improve the trustworthiness of DWSNs in the IIoT Under the same condition of the PRR, the ETX of our work was reduced and this shows that the WSN had greater trustworthiness.

Ma et al. (2020) The work looks at the blockchain for VANET by investigating key management, it proposes a decentralized key management mechanism for VANET with blockchain ((DB-KMM) which

is very efficient in automatically realize the registration, update, and revocation of a user's public key. The VANET is among the prominent technologies used in improving the efficiency and safety of modern transportation systems. VANET can however present a unique range of challenges and opportunities for security and key management is used as a footstone to build a practical security framework and these ahs become a good area of research for schools and establishment. The work also presents lightweight mutual authentication and key management protocol based on bivariate polynomial and analysis is based on the security of DB-KMM in the universally composable framework and then highlights that the mechanism can prevent typical attacks such as public key tampering attacks, internal attacks, the DoS attacks, and the collusion attacks. In the end, analysis continued the performance of the scheme by conducting experiments and simulations were also conducted and the results show that DB-KMM has better performance than the existing schemes in terms of, storage, computation overhead, latency and communication.

Yin et al. (2021) addresses the secure sensitive data sharing problem concerning recipients in the blockchain Internet of things, (BIoT) and proposes a CP-DK-ABE scheme with decentralized key generation, which is suitable for sharing the sensitive data in BIoT. The author used a cryptographic method to solve and meet the requirements of decentralization and convenience by using programmable ciphertext and key management. In doing this they design a ciphertext policy which is decentralized key attribute-based encryption (CP-DK-ABE. The master secret key used is divided into full nodes as a collective form of threshold secret sharing, used together with a decentralized multiparty computational protocol to generate a private key for the users in an interactive method. In the work the attribute subkeys related to the private key can be reconstructed with a fragment from each full node to obtain the cooperative management of the attribute key from all the full nodes. Using the blockchain script system, five new opcodes were used to represent ciphertext in the programmable format to provide flexible capability in representing the logical relationship of the access control policy among attribute sub ciphers in the CP-DK-ABE by the scripting language. The processes of encryption and decryption are implemented entirely by the script interpreter on the blockchain node and improve the convenience of programming in BIoT devices and this shows that the proposed scheme is key private and semantically protected for limited corrupted nodes that are full in the decision linear and bilinear Diffie-Hellman idea, respectively. In conclusion it was shown that the script driven ciphertext can reduce the difficulty of programming BioT devices and our key generation algorithm shows that protecting the secret key held by the full nodes is semantically secure and our CP-DK-ABE scheme is semantically secured under the assumption of the DBDH.

Panda et al. (2021) proposes a novel approach for distributed authentication and key management in exploiting the advantages of cloud computing, fog computing and Blockchain technology, used to achieve a secure and efficient architecture for IoT use cases. Several layers of blockchain were used to increase the scalability of the system, speeding up the validation process. The Ethereum platform was also used in developing the blockchain network, the exponential growth in the number of connected devices as well as the data produced from these devices call for a secure and efficient access control mechanism that can ensure the privacy of both users and data. Several of the key management mechanisms involved are dependent on a trusted third party such as a registration center or key generation center for the generation of the management keys. The article also investigates the issues of trusting third party which has its problem and so results in a centralized architecture, this was done by designing a blockchain-based distributed IoT architecture that makes use of hashing of chains to secure key management. This proposed method used the key characteristics of blockchain technology like immutability, traceability, openness, and fault tolerance in ensuring that the data privacy in IoT scenario is maintained and then gives the communication a secure environment. Thirdly the scheme proposes secure and efficient key generation and mutual authentication management between the different communication parts, using a one-way chain technique hashing for a set of public and private key pairs to the IoT devices. The pair of keys are then used to verify each other at the same time. This scheme was thoroughly evaluated and so it confirmed the high efficiency and scalability of the scheme. Also, the security analysis demonstrates the scheme's compliance with the security requirements of IoT use cases. In conclusion the experiment analysis was able to confirm the superiority of its performance in the proposed scheme compared to the existing conventional mechanisms.

Yu et al. (2023) work proposes a distributed management scheme, where the master and slave key generated at the center respectively generates part of the user's private key, and users generates their own private key locally, therefore it avoids the key escrow problem. Identity-based cryptography algorithm, SM9 requires a trusted third-party key generation center (KGC) to generate the user's private key. It brings about the risks and problems of key escrow and single point failure. The work also proposes a distributed identity-based cryptography key management scheme. The participants in the scheme generate a partial identity private key and then transfer it to the user. The user then locally generates its identity private key. The identity status data generated is then uploaded into the blockchain and this helps to prevent the key escrowing problem and solve the single point failure together with the trust problem, thereby the system availability and security are improved, This proposed scheme has advantages in terms of bandwidth and efficiency requirements.

Lei et al. (2017) propose a novel key management scheme for key transfer among SMs in heterogeneous VCS networks. It proposes a framework for providing secure key management within the heterogeneous network by introducing Information technology to the transportation infrastructures, maintaining take care of the road and maintain safety and traffic efficiency. Security is the actual concern in vehicular communication systems (VCSs) and using the secure group broadcasts with secure key management schemes, considered as a critical technique for network security can help to address the problem. Security managers (SMs) have a major function of capturing the vehicle departure information, encapsulating the block for transport keys, and executing the rekeying to vehicles within the same security domain. The work is divided into two different frameworks. The first part is a novel network topology based on a decentralized blockchain structure proposed to simplify the distributed key management in heterogeneous VCS domains. The second part of the framework makes use of the dynamic transaction collection period to reduce the key transfer time cost further during the vehicle handover, this transaction uses a mathematical model to make SMs to be able to decide how to use different transaction collection periods. The blockchain structure allows key transfer securely within the decentralized SM network, therefore we developed an incredibly good flexible transaction collection period selection system to shrink the key transfer time of the blockchain scheme. Privacy issues were also taken into consideration, with the investigation of a system that provides both privacy and security. Rigorous and continuous simulation and analysis highlighted the efficiency and effectiveness of this proposed framework where the blockchain structure performs a lot better when looked at from the perspective of key transfer time and the structure with a central manager and the dynamic scheme permits the SMs to be able to fit into various traffic levels.

Kirupanithi and Antonidoss (2021) proposed a system that states that user can manage their own data forming a self-sovereign identity management system. In every situation, the network operator manages and generates the user identities and their corresponding keys to be accessible over the network where the user's personal information is stored in the centralized servers. Storing in the centralized system causes the users to lose the privacy of his or her data and this is a big problem and confusion for users on how to prevent the loss of their sensitive data to the public without compromising. This scheme allows the users to generate their own public and private keys, the blockchain and chameleon are then used to remove all illegitimate data from gaining access to the blockchain. A third party then authorized the system to authenticate the user's request on blockchain and to have a self-sovereign identity with their public keys as validation access. The work was concluded by showing that the evaluation results have reduced the overheads in transmission delay of the total number of storages, encryption of data and packets and the user information is completely managed by the user leading to a user-centric system,

minimizing the leakages of data, and maintaining privacy. By adopting a session key, it can avoid registration and the blockchain is able to record the identities and the public key to provide genuine authentication. Revocation lists are no longer needed but instead a redactable blockchain is used which allows the operators to revoke user access dynamically.

Meng et al. (2021) propose a distributed key management scheme for MEC-enabled vehicular network. In a critical technology of network security, attention has been drawn to key management in mobile edge computing, (MEC)-enabled vehicular networks. But the traditional centralized key management methods are prone to failure in a single point and therefore in this scheme, the use of permissioned blockchain to keep the key and present a new transaction format with the update, revocation and key registration included. The high mobility of the vehicle makes us design an authentication protocol which is lightweight and mutual to ensure that the vehicle can access MEC servers safely and quickly. The peak of the scheme was able to offer an efficient key update and revocation based on blockchain technology and the lightweight mutual authentication protocol helps to achieve important security properties. The simulation analysis carried out shows that the scheme is a great improvement over the existing certificates-based PKI schemes of the delay and communication overhead. Lastly, simulation results show that the proposed scheme can achieve a lower authentication delay and higher security with less communication overhead, compared with traditional key management.

Lehto et al. (2021) propose a distributed key management scheme for MEC-enabled vehicular network. In a critical technology of network security, attention has been drawn to key management in mobile edge computing, (MEC)-enabled vehicular networks. But the traditional centralized key management methods are prone to failure in a single point and therefore in this scheme, the use of permissioned blockchain to keep the key and present a new transaction format with the update, revocation and key registration included. The high mobility of the vehicle makes us design an authentication protocol which is lightweight and mutual to ensure that the vehicle can access MEC servers safely and quickly. The peak of the scheme was able to offer an efficient key update and revocation based on blockchain technology and the lightweight mutual authentication protocol helps to achieve important security properties. The simulation analysis conducted shows that the scheme is a great improvement over the existing certificates-based PKI schemes of the delay and communication overhead. Lastly, simulation results show that the proposed scheme can achieve a lower authentication delay and higher security with less communication overhead, compared with traditional key management.

Chen et al. (2021) proposed a blockchain-based key management scheme for managing secure keys and establishing secure group channels in fog-based IoT systems. In the proposed scheme, key management is used for the improved DConBE, a new PoW mechanism called DPPoW, and the TAA scheme as the



key building blocks. Several benefits are associated with the fog computing development such as analyzing and computing data from the internet of things, (IoT) there is reduction of bandwidth, storage overhead and computational at the fog nodes of the cloud servers and the quality of experience due to latency is improved for the user. For additional security requirements, secure keys are needed to establish secure channels between the distributed fog nodes and in order to facilitate fog nodes in taken care of the secure keys and establishing secure group channels, a new authentication mechanism resources based on Proof of Work (PoW) is deployed in the fog system facilities resources authentication to evaluate the capability of fog device's computing power before the permission of the device in entering the system. The outcome of these schemes (simulations and secure analysis) shows the utility of our system and shows proof that it achieves data recoverability, non-repudiation, conditional anonymity, and resource authentication. The outcome of the simulations done shows the efficiency of the scheme.

Sharma (2019) discussed securities problems and the challenges in blockchain technology, like scalability, privacy, wasted resources, data malleability, usability, and bootstrapping. The paper works on elaborate and detail review of the integration process and present working mechanism of the blockchain together with the changes of nature of value. Blockchain is a method that allows transactions of data, being evaluated using groups of untrustworthy actors, it can be referred completely and allow access to all the transaction taking place within the system and thus gives a safe, transparent, auditable, dispersed, and absolute record. Blockchain can either be private or public and it is receiving great attention from all aspects of life, be it researches, organizations, schools etc. as it brings forth magical solutions to the classical centralized architecture problems. It is used for maintenance of integrity, and it is a type of distributed ledger for decentralization of transaction among many participant and end users and on the other hand IoT revolutionize the facilitation of connection of all end user devices over the internet and then share the services and applications for improvement of daily living standards. This centralized IoT has several benefits and comes with lots of challenges. The work uses the security requirement for the Internet of Thing (IoT) Routing protocol for low power and lossy networks (RPL), then adapts the provided framework which is required by different classes of applications. RPL security field information means the security level and the cryptographic process used to deliver the required security are three modes in the existing RPL specification, the unsecured which means there is no security applied to the routing message in this mode, preinstalled mode make use of a preconfigured symmetric key together with existing RPL, which gives support to the authentication, confidentiality, data integrity used for the routing protocol, and the authenticated mode which is best for devices that operates as a router. The outcome highlights the advantages of various talents of blockchain technology in several programs which include, music industry, healthcare, cybersecurity, public service and Voting process and this leads to the integration of blockchain as next level of development.

Pereira et al. (2019) propose a certificateless public verification scheme against procrastinating auditors, such as CPVPA. The CPVPA used on-chain currencies, where each verification performed by the auditor is integrated into a transaction on the blockchain of on-chain currencies. With public verification techniques, a user can employ a third-party auditor to verify the data integrity and then these are vulnerable to procrastination auditors who may not perform their verification quickly. When the transaction has been recorded in the blockchain system, the user then verifies what time the verification takes place, this is done by looking at what time the transaction is generated. Constructing the CPVPA on a well-established and a blockchain that is well used instead of newly created ones. The public verification schemes are then constructed on public key infrastructure (PKI) and suffer from certificate management. The work target at design a secure public verification of data integrity to be used in cloud storage systems, and with a threat model where they consider three different challenges, the semi-trusted server, the misbehaved auditors, and, the malicious users, after evaluating the performance using the proposed scheme in terms of communication overhead and computation overhead, the experiment is then conducted on a computer with window 10 system where the code is implemented by using C language and MIRACL Library with evaluation of security level of 80 bits, which means that the pairing is based on the MNT curve,6 its base field size is 159 bits and its embedding degree is 6. The outcome of the security analysis was able to demonstrate with CPVPA we can get the strongest security when compared with existing schemes.

(Lee & Jeong, 2021) present the use of a Biometric Authentication System, BDAS in blockchain technology and this provides a distributed and decentralized mechanism for processing the authentication of biometrics of users and makes it auditable in managing biometric information and does not rely on any central authentication module. Using BDAS allows every person to independently manage the template fragment and do the authentication procedures without having a general central point.

Imam et al. (2021) present using Ethereum blockchain-based technology for a decentralized web application for digital document verification in P2P cloud storage to improve the verification of the process and make it more transparent and easier to audit. It uses methods like cryptography (private/public key), digital signatures, online storage methods, etc. in verifying uploaded documents for organizations or authorities faster and more conveniently by assigning hash values to each user's document. The results show an efficient and accurate verification outcome.

Lin et al. (2019) propose the use of a GS and a MAC in authenticating a requestor without information being leaked on any user with the use of a home gateway with perfect forward secrecy at the same time.

Any user can be traced effectively if they are found to be carrying out wrongdoings on the system. A secure mutual authentication system was constructed and applied to the smart homes, with the integration of blockchain, message authentication code, and group signature for auditing the various users, and group members with their home gateway and access history. The work was able to prove that the security and privacy requirements, anonymity, traceability, and confidentiality, were satisfied.

Nguyen et al. (2020) proposed some blockchain-based application development principles in solving the issues of certificate forgery by the application of blockchain technology to deal with social problems in general as well as certificate management in Vietnam, they used Hyperledger Fabric as a blockchain platform deployed on the Amazon EC2 cloud to build a step by step VECefblock having a well-designed overall architecture together with business processes, data mapping structure and implementing the decentralized application that can meet the specific Vietnamese requirements. This experiment also shows the feasibility of our proposal, thus promoting the essential security against certificate forgery in Vietnam.

Cai et al. (2020) present a blockchain assisted system for secure authentication in Solid and for implementation of fine-grained access control policies. It achieves a secure authentication and fine-grained access control by introducing a trust access authentication system with blockchain equipped with several security properties and authentication functions to integrate threshold RSA signatures in a permissioned blockchain system. Utilizing a smart contract to control transaction flows and manage access control policies automatically to enhance the resilience and robustness of authentication system, the results shows that the proposed trust access authentication system enhances security, scales well, and is efficient and economically feasible.

## CHAPTER 3

## BLOCKCHAIN INTEGRITY, SECURITY ISSUES AND SOLUTIONS

## 3.1 Introduction

The Technology of Blockchain is the emerging technology with rapid distribution over a recent period of technological advancement and this has gone viral indicating what a revolution of technology can be. It is a distributed secure way of allocating databases. A Blockchain as the name implies is a chain of numerous blocks joined together via cryptography for the transaction of data and transferring of information from one user to another.



Figure 3.1: Blocks of Chains connected.

The block header + block data with every block has a unique hash to prevent changing the data once it is recorded. A unique Hash is used to link the block Cryptographically and numerous pieces of information from one transaction to another transaction are all trying to maintain the correct record while information is being added to the chain. Important aspects of blockchain technology are Decentralization, Cryptography, transparency, and security.

Blockchain is a linear type of data structure that is made up of blocks in a chain-like manner, this simply means combinations of blocks connected as a chain in which transaction takes place in each block consisting of transactions by batches and the longest chain will become the valid chain. Blockchain is used to solve the problem of money transfer, and the relationship between Bitcoin and blockchain shows that they are not the same as Bitcoin is a digital coin, while blockchain is the technology that enables the movement of Bitcoin from one individual to another. Hence, we have a different definition of blockchain such as a digital ledger that contains immutable records distributed among the partners on the network and this eases the process of keeping records in a digital format across the network. Bitcoin aims to solve the problem of fiat currencies with the help of blockchain technology. Blockchain is a distributed database or list of records that store records, and data of transactions in secured, decentralized, and chronological orders. It ensures the privacy of the users is maintained and data cannot be altered. Records of data are trusted without the need for a trusted third party. Blockchain was designed to be secured and to be difficult to attack and compromise by making sure each of the blocks or data is digitally signed

with a “hash.” It is imperative to note that for blockchain three elements are essential and these are (i) Decentralization, (ii) Security, and (iii) Scalability. But the situation achieving all three optimally and simultaneously is almost impossible. From all indications, it is obvious that blockchain is not so secure and so many attacks can occur in the transaction within the chain. In this paper, I investigated the issues of blockchain Integrity and the several ways by which blockchain can help in alleviating these issues with user satisfaction.

### 3.1.1 Benefits of Blockchain

- It is very secure using cryptography.
- It is not controlled by a central authority.
- Everyone on the network has access to the transaction.
- All copies of the data are visible and copied to everyone involved in the chain of the transaction to ensure the data remains unchanged.

### 3.1.2 Types of Blockchain

- The Public blockchain opens and allows any user to join the chain while ensuring anonymity of the participant.
- The Private blockchain depends on identity for confirming the membership and access privileges.

### 3.1.3 Blockchain Security Issues

- Exploited code.
- Missing keys.
- Hacking Employee system.

### 3.1.4 Blockchain Attacks

- 51% of Attacks: This form of attack is when an individual or organization, i.e., a malicious attacker collects more than half of the hash rate and takes access to the entire system; this can be dangerous and harmful to the network. Attackers will change the mode of order of transactions, thereby preventing the transaction from being confirmed. These types of attacks can be prevented by Improving the mining pool monitoring, the hash rate can be increased and made higher, and also avoid using proof-of-work (PoW) consensus procedures, Manan [48].
- Routing Attacks: This is used to partition the network into two, in which the attacks intercept data transfer traffic. This form of attack is preventable by the following processes, Implementation of

secure routing protocols using certificates, the data encryption usage, and regular change and modification of password (strong password).

- **Blockchain endpoint vulnerability:** This is a situation where an attacker can access any form of data belonging to a user of the network through an attack on the person's personal computer so that he can get keys to unlock secured passwords. Blockchain endpoint vulnerability attacks can be prevented by avoiding saving blockchain keys on your computer or mobile phone as text files, making sure antivirus software is downloaded and installed properly on the system and making sure the system is reviewed from time to time.
- **Vendor Risks:** Vendors sometimes have weak security control on their systems, flawed code, and even personnel vulnerabilities that can easily expose their client's blockchain credentials to unauthorized users. This is particularly a case when using smart contracts since the organization's policies and operations can be housed as a smart contract on a blockchain in which any vulnerabilities of such will cause major damage.
- **Transaction privacy leakages:** Transaction contains sensitive information about their issues in some blockchain such as the Internet of things or mobile crowdsourcing, transaction privacy leakages can cause critical issues. Indirect privacy leakages through the disclosure of transaction contents, namely the analysis of the transaction graph could uncover the correlation between different transaction addresses. Transaction leakages problem can be solved by implementing a mixing service and upon activation, the service will allow several users to make transactions simultaneously with multiple inputs and outputs and because of this, the transaction inputs will not be able to map to their corresponding outputs.
- **Phishing attacks:** Generally used by hackers to gain access to customer's details by sending emails to users with links to scams and obtain the credentials of a user. The email requests information about user credentials through hyperlinks and when hackers get these credentials and sensitive information of a user, the user, as well as the blockchain network, are open to subsequent attacks. Phishing Attacks can be solved by educating wallet owners and key stakeholders of a network about countermeasures to avoid phishing.

## 3.2 Background

The first Blockchain was created in 1982, by 'David Chum' while in 2009, 'Satoshi Nakamoto' launched the first Bitcoin blockchain source code into SourceForge. The major difference in their invention is the addition of the Bitcoin proof-of-work consensus mechanism for validating data blocks and mining coins. KRIPTOMAT [49]. Blockchains are typically databases that record transactions on user's computers all over the world instead of storing information on a central server that is easily accessed by all users. It is a peer-to-peer architecture that allows non-central authority to hold a master copy of the data, therefore the blockchain is a distributed database and allows the data to be stored in multiple locations. One general problem with blockchain technology is the issue of Integrity. Every user wants to have a secure mode of transacting business and information must be protected and secure. In Blockchain technology, this is one important issue that we looked at in this research work. We will look at various integrity issues of blockchain technology and proffer solutions to make the technology more comfortable for the users.

### 3.2.1 Blockchain Integrity

This is one of the principles of cybersecurity, it is about ensuring the accuracy of a message such that when it is read it is the same as when it was first written. This can be seen from the way information is passed from one person to another, it does not come out the same way it was initially spoken. Most current systems are not designed to protect the integrity of the data from the moment of creation until the point of use. Protect its Confidentiality? Yes. Protect its Availability? Yes, again. The more we depend on data to drive processes of increasing complexity, the more Integrity supplants Confidentiality and Availability as the paramount goal of cybersecurity. Data integrity is the maintenance of, and the assurance of the accuracy and consistency of data over its entire life cycle, and is a critical aspect to the design, implementation, and usage of any system which stores, processes, or retrieves data." It is at times used as a proxy term for data quality.

### 3.2.2 Types of Integrity

3.2.2.1 Commission: Creating a message that did not exist. The main tool used by integrity commissions is investigation. Investigations are used to meet the objectives of promoting integrity, and investigating, exposing, and deterring corruption.

3.2.2.2 Omission: Deleting messages so that they never existed.

3.2.2.3 Manipulation: Changing messages, creating brand new data, or completely deleting data. This is often difficult to spot, therefore we need to guard against most. This can be protected by using a signature or a hash function. This takes all the data and puts it through a mathematical process to create a Unique identifier so that even if a single bit of the original message changes, the signature changes wildly and becomes obvious that the original message has been changed.

The working of blockchain with integrity can be highlighted with the following scenarios and transfer concepts. A normal transfer between Customer A and Customer B through a third party will only allow a transfer between A and B, but without passing through the third party.

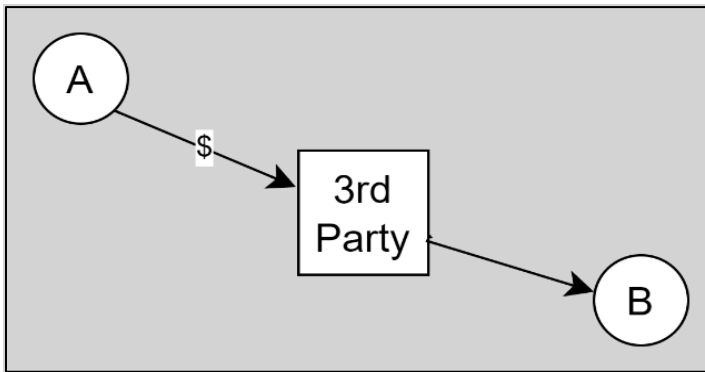


Figure 3.2: Simple chain transaction from user A to user B.

### 3.2.3 The Transfer Concept

1. Using an open ledger: This is known as the chain of transactions otherwise called blockchain.

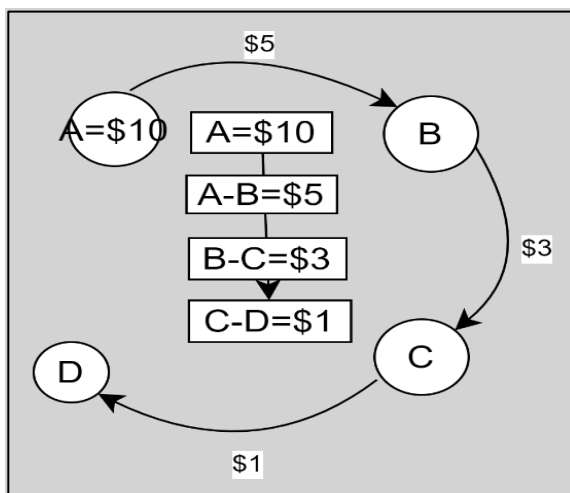


Figure 3.3: Transaction among many users in the network being notified.



2. In a distributed ledger: Everyone can have a copy of the transaction. Therefore, there is no need for the general transaction blocks.

Table 3.1: Different Blockchains with transaction in a distributed Ledger.

BLOCK A	BLOCK B	BLOCK C	BLOCK D
A=\$10	A=\$10	A=\$10	A=\$10
A-B=\$5	A-B=\$5	A-B=\$5	A-B=\$5
B-C=\$3	B-C=\$3	B-C=\$3	B-C=\$3
C-D=\$1	C-D=\$1	C-D=\$1	C-D=\$1

3. Synchronizing the ledger: All transactions made must be visible and same to all participants involved.

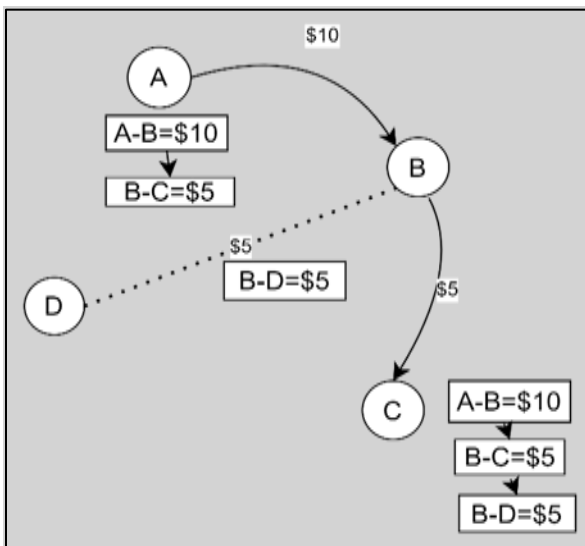


Figure 3.4: Synchronization of transactions in a ledger.

In this transaction B can make a transfer to D using a miner, in this situation, there is a need to decide who receives the transaction first, from B between C and D. this is where the use of a miner is essential as the miner is expected to perform two operations,

- i. The miner needs to validate the new transaction if B has the funds available to carry out both transactions.

- ii. The miner must find what is termed a key that will enable the miner to be informed of the previous transaction to log a new transaction and this is done by randomly finding the key.

### 3.3 Blockchain Integrity Issues

Data integrity is achieved within blockchain applications with three main requirements, data origin integrity, oracle integrity and digital-twin integrity and this form the components of blockchain integrity. FORUM [50]. Blockchain technology will maintain data integrity by ensuring that all transactions are verified using multiple nodes on the network, it uses cryptographic hashing to ensure data integrity without compromising or modification. Blockchains or distributed ledger technologies. Allows the blocks to be structured and each block contains a transaction or bundle of transactions while every new block is joined to the previous blocks in a cryptographic chain such as making it impossible to tamper with.

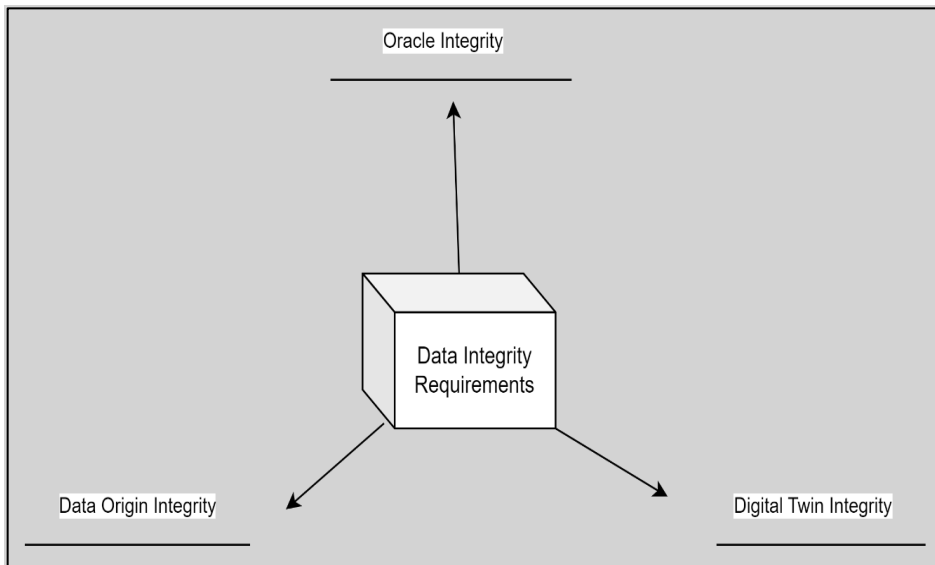


Figure 3.5: Components of Integrity.

### 3.4 Method

In the work we design a simple Blockchain, with several transactions made and a look at the integrity from the hash value generated by the output. Since blockchain is a group of blocks connected cryptographically, all the transaction must be original with integrity when it is being read by the other user of the network and by whoever it is intended for. The Blockchain was built to make transactions from Williams to Anna by sending 3BTC across and the transaction was called out with a generation

of hash value which is specific to the transaction from the sender to the user and only the confirmation of the specific hash value by Anna can authenticate the integrity of the transaction. Several other transactions from Jeff to Greg, Jeff to Anna, Greg to Williams, Anna to Greg and Anna to Rick were equally made in the network, and all the transactions generate specific hash value to verify the integrity. It should be noted that any change in the transaction by anyone, most probable an unwanted user such as a hacker/ attacker will have a significant effect and changes in the generated hash value, and this will tamper with the integrity of the transaction and when such occurs everyone within the network will not access the transaction and it will be rejected.

```

1  import hashlib
2
3
4  class Blockchain:
5
6      def __init__(self, previous_block_hash, transaction_list):
7          self.previous_block_hash = previous_block_hash
8          self.transaction_list = transaction_list
9
10         self.block_data = "_".join(transaction_list) + "_" + previous_block_hash
11         self.block_hash = hashlib.sha256(self.block_data.encode()).hexdigest()
12
13
14     t1 = "Williams send 3 BTC to Anna"
15     t2 = "Jeff send 4 BTC to Greg"
16     t3 = "Jeff send 5 BTC to Anna"
17     t4 = "Greg send 4 BTC to William"
18     t5 = "Anna send 2 BTC to Greg"
19     t6 = "Anna send 2 BTC to Rick"

```

Figure 3.6: Building blockchain with Python showing the transaction to be made.

```

20
21     initial_block = Blockchain("Initial String", [t1, t2])
22
23     print(initial_block.block_data)
24     print(initial_block.block_hash)
25
26     second_block = Blockchain(initial_block.block_hash, [t3, t4])
27
28     print(second_block.block_data)
29     print(second_block.block_hash)
30
31     third_block = Blockchain(second_block.block_hash, [t5, t6])
32
33     print(third_block.block_data)
34     print(third_block.block_hash)
35

```

Figure 3.7: Printing of transactions in a blockchain across the users.

```

main X
C:\Users\olale\miniconda_3\python.exe C:/Users/olale/python0lalekanBlockchain/main.py
Williams send 3 BTC to Anna_Jeff send 4 BTC to Greg_Initial String
d0c5f98411127650773d0238702279aaf38b3bcff8b1456984abfdcd0f6bf78
Jeff send 5 BTC to Anna_Greg send 4 BTC to William_d0c5f98411127650773d0238702279aaf38b3bcff8b1456984abfdcd0f6bf78
9bc0e94d8f1b3363dade6eabdfbcf8df0af8ee7fd2b0b5dca6ce5827b27f7645
Anna send 2 BTC to Greg_Anna send 2 BTC to Rick_9bc0e94d8f1b3363dade6eabdfbcf8df0af8ee7fd2b0b5dca6ce5827b27f7645
c25c4606e6deed3dedfb42a571d8fe479e4ac5b41bcbf1b8e566ab48a3ab67d5
Process finished with exit code 0

```

Figure 3.8: Hash value generated showing various transaction values.

Table 3.2: Interpretation of the code and generated hash values.

Lines	Interpretations
1	Importing the hash algorithm from the library for the blocks.
4	Class of blockchain
6	Definition of the previous blocks such as the genesis which is the first block
7	Hashing of the value of the previous block
8	The transaction list is generated for all the transactions
10	Creating blocks after the initial blocks all through the list of transaction
11	Code for hash for every transaction with sha256
14	T1: transaction from William to Anna
15	T2: transaction from Jeff to Greg
16	T3: transaction from Jeff to Anna
17	T4: transaction from Greg to William
18	T5: transaction from Anna to Greg
19	T6: transaction from Anna to Rick
21-34	Transactions are made with a generated hash value for each transaction as it is made. The outcome in the Figure 3.8

### 3.5 Results and Conclusion

Maintaining a blockchain with integrity was obtained in this work, with the generation of the hash value for the various transactions and this led to verification of the integrity of the transaction in the blockchain, any little change in these transactions will result in a change in the generated hash value, the transaction from T1 to T2; T3 To T4; T5 to T6, all generated different hash values specific to the

transaction and this hash values is also received by the other users on the network for easier verification of the integrity of the transaction, when these are matched, then the receiver can verify that the transaction has not been hijacked or modified by an unauthorized person and so the transaction can be accepted and completed. If by any chance a little alteration was done in the transaction either by the genuine user or the hacker, the hash values will change, and this will show the other authorizer user to be careful verification will fail and the transactions will be rejected.

In conclusion, this work verifies the integrity of blockchain transaction and notes that securities issues in the blockchain is minimized with the integrity verification, it goes a long way in helping blockchain transaction and help the organization and individuals within a blockchain network. Since for every transaction change there is equally a change and new generated hash value.

## CHAPTER 4

### BLOCKCHAIN DECENTRALIZATION, SECURITY ISSUES AND SOLUTIONS

#### 4.1 Introduction

Decentralization of Blockchain is when the chain is broken down into several pieces and installed in many locations so that it can be accessed easily by all the users and make inputs and contributions along the transaction, but the main user who puts up the transaction can take it down. In blockchain, decentralization is permitted for every member participating across the distributed network and this makes sure that there is no single point of failure, likewise no single member will influence the changes in the transaction IBM [51]. Decentralization gives the users of blockchain full control over the credentials or personal information shared with every user of the blockchain and this is done by verifying their identity. It is an effective identifier that enables the verification and protection of users' credentials and personal information. In simple terms Decentralization of blockchain is the process of breaking down the power that central authority has and then distributing it across the common masses Team [52].

Majorly blockchain Implementations are now decentralized and distributed and this is referred to as the system of information or data and decision-making transfer from a central mode comprised of individuals, organizations, or groups to a more distributed network. (basically, this is the distribution of authority, responsibility, and accountability to the various levels of management). The decentralization essence is basically to reduce the power concentration in a single user, so no single user is to have authority or control in a transaction over and above all other users, and this allows the users to have a good level of trust and confidence in all participants within the network AWS [53].

Blockchain used the decentralized blockchain to improve cybersecurity by using the decentralized storage solution, as data is being stored in a decentralized manner, there will not be a single point of attack (i.e., no single user can change the transaction alone without the other user's input) for the hackers rather blockchain technology enables the decentralization through the participation of members across a distributed network. Decentralized blockchain uses encryption to secure data either by a symmetric or asymmetric key.

##### 4.1.1 Types of Decentralization in Blockchain

Decentralization can be categorized into three main sectors, these are, the fully centralized blockchain, which is controlled and managed by a central authority, the semi-decentralized system that is controlled and managed by multiple authorities and the fully decentralized system with no middlemen

or central authorities to manage or administer the network. Further categories of decentralizations include Physical decentralization which deals with the geographical distribution of blockchain servers across the entire globe to ensure no single entity or user has the monopoly control of the network, thereby preventing the loss of data or information with any loss of physical server within the network. The transactional decentralization helps to improve the efficiency and transparency of B2B networks are made the more secured and consensus-based environments for executing, verifying, and recording transactions. Political decentralization is another type of decentralization which is more of a regulatory system that checks how many people, users or organizations have control over the network and not the server Patrizio [54].

Table 4.1: Scale of Decentralization.

Fully Centralized	Semi decentralized	Fully Decentralized
The central intermediaries are in control of the transactions	At this point, the intermediaries are competing with each other.	No intermediaries are involved at this level of blockchain technology.

#### 4.1.2 Benefits of Decentralization

Decentralization has many benefits over centralized blockchain technology, and these include such as:

- (i) **Trustless Environment:** in this environment there is no need to know your client, since the transaction cannot be tampered with and in case anyone tries to get access to the transaction, most of the network members will reject the transaction if the ledger is altered or corrupted in any way.
- (ii) **Data Accuracy improvement:** Data can be lost or manipulated each time it is transferred, but in a decentralized blockchain, every entity/user has access to real-time transfer and shared view of the data, and which prevent the data from being changed or manipulated.
- (iii) **Reduced Downtime:** failure in the blockchain is reduced since there is no single point of central authority, it is a good way to continue transactions even when one source is unavailable or if there is a system bottleneck.
- (iv) **Transparency:** Blockchain decentralization makes transactions easily available to all, therefore every user can have access to the transaction and have control over the information and who is allowed to see it.

- (v) Minimization of weakness: Decentralization helps to minimize weakness in systems, this point of weakness could help to prevent failures or inefficiency of services due to bottlenecks, periodic outages, corruption, and lack of sufficient incentives for good services.
- (vi) Immutability: Every user must confirm the transaction in a decentralized network; therefore, the data cannot be altered by any single user, which makes it impossible for the integrity of the decentralized blockchain as there must be approval by each node in the network.

#### 4.1.3 Blockchain Decentralization downsides

- (i) Discipline: lack of discipline on the part of any user of the blockchain will result in the network suffering or lapses since all users must be involved in the transaction.
- (ii) Clarity: Lack of clarity can lead to a stop in the transaction in blockchain decentralization since every member has to be clear in their transaction in the network.
- (iii) Consensus: No single decision from any single user, it must be consensus from every user and this cause delay and can be messy at times.
- (iv) Cost: Blockchain decentralization system can be more expensive because of the need for more systems and users to run it successfully.

## 4.2 Background

Decentralized blockchain was started by a person named, Satoshi Nakamoto in 2008, in which he successfully used Hashcash to improve the design method to timestamp blocks without requiring them to be signed by a trusted user and then introduce a parameter that is difficult in stabilizing the rate at which blocks are added to the chain [55]. Due to several issues arising from the transaction within a blockchain network, the idea was proposed to build a blockchain technology network with architectural considerations for centralization, distribution, and decentralization. The major reason for creating this technology is to prevent a few individuals or organizations or entity from being in control of transactions that belong to all. The banking sector for example thinks of a way out to put all the flow in and out of currency from the central bank into a single user's hand and hence the design of a decentralized system which is unalterable once data has entered, so it makes it impossible to change or reverse the transaction. The only thing that can be done in case of an error is to start another transaction all over and discard the transaction, so this is a security measure in preventing an unauthorized person from changing details or any part of the transaction [54].



Comparing Centralized and Decentralized blockchain systems proves that decentralization is more beneficial and preferable for successful transactions in a big Organization as compared to smaller establishments.

Table 4.2: Comparison between the Centralized system and Decentralized system of Blockchain.

Attributes	Centralized system	Decentralized System
Flow of Information	Flow is in a vertical system and to and for within the network	Here the information is in an open and free system and there are multiple routes of transaction.
Decision making	The decision lies with the top management down to the lower-level cadre, it is by hierarchical	Multiple participants are making decisions, and it is a faster and more democratic system of decision.
Control	Control is at the central entity	This is basically by the software code that connects every entity.
Pros	It is a simple decision-making system and less expensive with more control for the top management	There is transparency, immutability and every member are involved in the transaction with no single point of failure.
Cons	Have a single point of failure which is the person in control of the system coupled with trust issues and data can easily get lost or manipulated	More expensive hardware involved, user anonymity.
Example	Small size organization	Large organization (Ethereum, Bitcoin)

### 4.3 Methods

There are two methods of decentralization we investigated in this paper and securities issues affecting

decentralization is investigated with concrete solutions.

- a. Disintermediation System: this is when the intermediaries are removed from the transaction within the network, such an example is in the transaction involving transferring money from your account to another user account and this can be done by transferring through the blockchain technology by simply requesting for the address of the other account owner. In this way the middleman is eliminated, and the transaction is completed successfully.
- b. Context driven/ Competition System: Here there is competition among several middlemen who tried to outsmart each other in gaining control of the transaction and hence dictate the running of the system within the network.

Security issues in blockchain decentralization are a major setback for the technology like in every other technology this has been a source of concern for the user of the blockchain technology. In a decentralized system security is usually provided by the private key and the challenge is how can we ensure that an asset or token associated with the private key is protected and not rendered useless due to the bug or negligence of the code. Here we design a simple smart contract to analyze the simple transaction. The smart contract is designed with Remix IDE.

```

1  pragma solidity ^0.5.10;
2
3  contract Ola {
4      address owner;
5      uint    fortune;
6      bool    deceased;
7
8      constructor() payable public { 224130 gas 162200 gas
9          owner = msg.sender; // msg sender represents address that is being called
10         fortune = msg.value; // msg value tells us how much ether is being sent
11         deceased = false;
12     }
13
14     // create modifier so the only person who can call the contract is the owner
15     modifier onlyOwner {
16         require(msg.sender == owner);
17         _;
18     }
19
20     // create modifier so that we only allocate funds if friend's gramps deceased
21

```

Figure 4.1: Creating a decentralization chain transaction.

```

21
22     modifier mustBeDeceased {
23         require(deceased == true);
24     };
25 }
26
27 // list of family wallets
28 address payable[] familyWallets;
29
30 //mapp through inheritance
31 mapping(address => uint) inheritance;
32
33 //set inheritance for each address
34
35 function setInheritance(address payable wallet, uint amount) public {  undefined gas
36     familyWallets.push(wallet);
37     inheritance[wallet] = amount;
38 }
39
40 // pay each family member based on their wallet address

```

Figure 4.2: Decentralization of Blockchain transaction.

```

41
42 function payout() private mustBeDeceased {  infinite gas
43     for(uint i=0; i<familyWallets.length; i++) {
44         familyWallets[i].transfer(inheritance[familyWallets[i]]);
45         // transferring the funds from contract address to receiver address
46     }
47 }
48
49 // oracle switch simulation
50 function hasdeceased() public onlyOwner {  infinite gas
51     deceased = true;
52     payout();
53 }
54 }
55

```

Figure 4.3: Payout code for the blockchain decentralization.

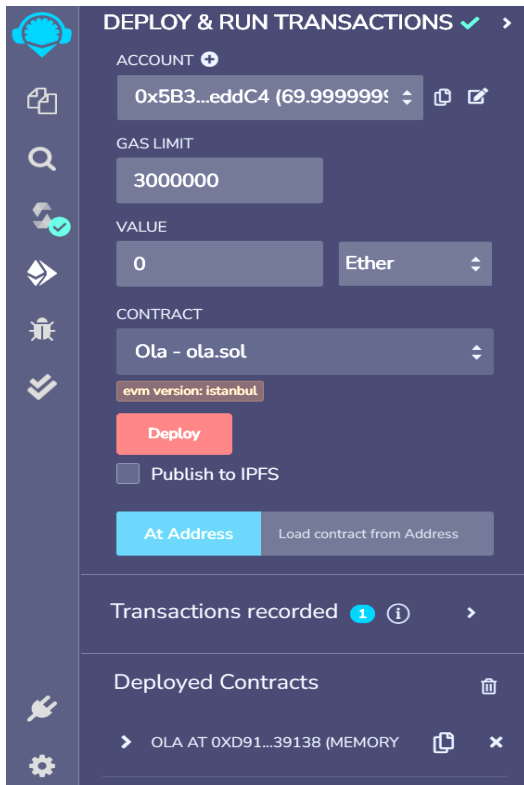


Figure 4.4: Final deployment of the transaction into the contract.

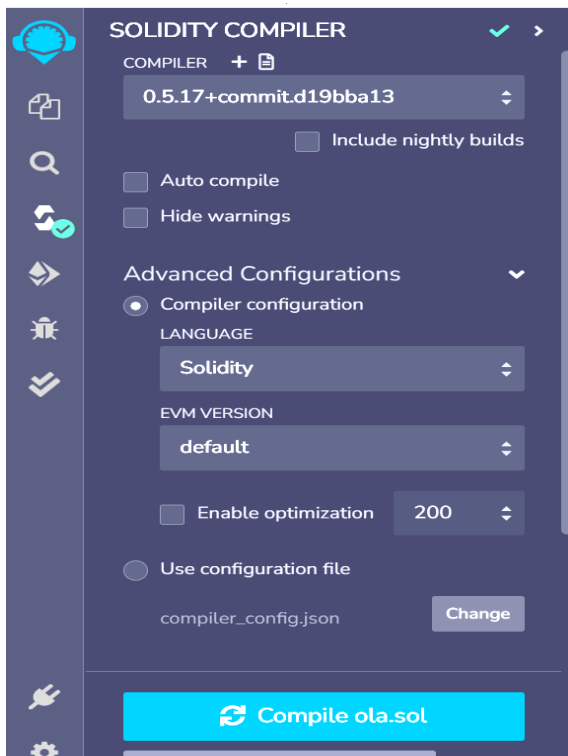


Figure 4.5: Compilation and solidification of the final transaction with each user being able to read.

#### 4.4 Results

Decentralization enables every member of the transaction to be able to have access to the transaction and view how the will is being allocated to each person. From the building of our work, decentralization makes it possible for the will from the dead parent to be distributed among the family members, with each member having detailed access to the transaction as it is being done within the network.

#### 4.5 Conclusion

In conclusion from our work, we were able to infer that decentralization serves a good purpose in securing the transaction in the blockchain and making it available to all authorized users to have access to the real time transaction within the network.

CHAPTER 5

BLOCKCHAIN KEY MANAGEMENT ISSUES AND SOLUTION

5.1 Introduction

Key management is the process of putting certain standards in place to ensure the security of cryptographic keys in an organization. This explains the usefulness of key management in blockchain technology. It deals with the creation, exchange, storage, deletion and refreshing of keys. Examples of key management are public key infrastructure (PKI) used in the secured socket Layer (SSL) and the Transport Layer Security, (TLS). The key management was introduced to solve the problem of security encryption in the blockchain. Encryption is a mathematical formula used to protect data and used key in hiding data. It works by using a code to protect input data and sending the data as a ciphertext to the other user of the network. The encryption algorithm has a mathematical formula which combines with the key in changing plaintext into ciphertext and at the same time helps in carrying out the reverse order by changing ciphertext into plaintext. The mathematical model can be written as:

For each  $k = (e, n) \in K$ , the encryption function is  $E_k = P_e, n$ ..... i  
 For each  $k = (e, n) \in K$ , the corresponding private key is  $(d, n)$  ..... ii  
 where  $ed \equiv 1 \pmod{\phi(n)}$ ..... iii  
 and the decryption function is  $D_k = P_d, n$  Joel Brawley [56]

Key management is generally agreed to form the basis of all data security. When data is encrypted and decrypted through the use of encryption keys this infers that the loss or compromise of any encryption key would be able to invalidate the data security system measures put in place. Keys are also used to ensure the secure transfer of data across an Internet connection Consulting [57].

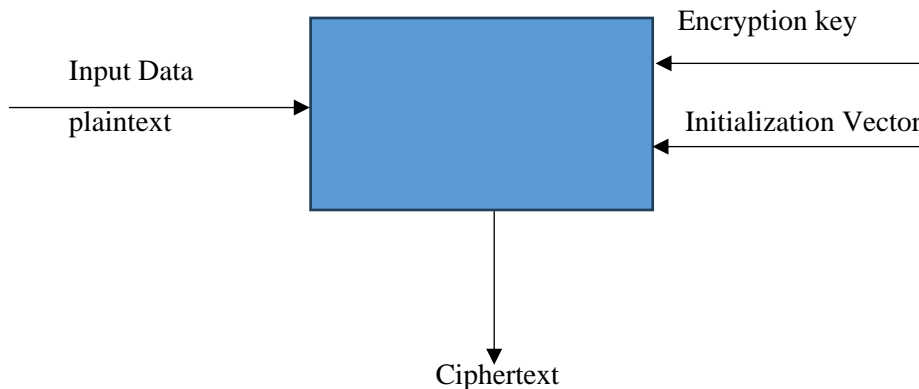


Figure 5.1: Simple frame of the encryption process in the network.

Encryption keys are divided into symmetric and asymmetric keys, and these are used to manage the security in blockchain technology. The standard algorithm used for encryption or decryption is the Advanced Encryption Standard (AES), with 128, 192 and 256-bit keys for advanced demanding purposes. There is also the Data Encryption Standard (DES) and IDEA in which users of the system who share a common secret key can communicate with each other safely over an unsecured source.

- a. **Symmetric Keys:** This is a secret key that can encrypt and decrypt the data being transferred and must be secretly transmitted to the user that will decrypt the information. These are not used for multiple purposes, and they are the most common type of key type for data at rest.
- b. **Asymmetric keys:** these consist of the private key and the public keys everybody can have access to public keys but only the authorized entity will have access to the private key, since the data encrypted with the public key will only be decrypted with the private key which is only given to the authorized person to have access to the information.

There are so many benefits of Key management in blockchain technology, and this is also applicable to Blockchain technology. These are listed below in this work [58].

- I. Operation Overhaul is reduced: In blockchain using key management helps in reducing the overhaul of the operation.
- II. Reduces the cost with automation:
- III. Human Error risk which can be dangerous to the loss of key and allow the blockchain to be attacked or hacked is reduced.
- IV. Automated key Update and distribution to an endpoint.
- V. Provides tamper-evident records for proof of compliance.
- VI. High availability and scalability.

## 5.2 Background

To prevent the problems of losing data or falling into the wrong hands and be manipulated or changed completely brought about the idea of using encryption of the transaction and hence the use of private key to manage the encryption from one point to another. Encryption and key management combine to prevent the data from being lost, hence key management becomes crucial and must be engaged. Good key management will be able to control and have access to the keys, check keys in and out, log access to keys, and be able to back up keys and the keys can expire. Key management encryption enables sensitive information to be protected by encrypting it and the encryption key is used to access the

information. Encryption key management is the collection of policies and processes that protect, store, organize and backup encryption keys and in this paper, we investigate the issues in key management of blockchain and how encryption key can be used to solve the intended issues.

#### 5.2.1. Key management issues and solutions

Several solutions have been proposed for the issues of key management in blockchain and this is to help alleviate the security issues that happen during transactions.

- The use of a multi-signature wallet: in this way more than one private will be required to sign a transaction to give additional security instances to the transaction. This has proved to be beneficial to blockchain technology, it helps to limit the issues of loss or theft of private keys by the user of the blockchain. When more than one key is used during a transaction, that gives more security since the hacker/attacker will need to obtain all the private keys before they can have access to the transaction, and this is a big mountain to climb for the attacker. The more data acquired, the more encryption keys you need.
- Hardware wallet: Physical devices stored as private key that are securely offline and away from any internet connected devices, to make them secure and safe from attack from malware infection, such example includes USB key, smart cards, and dedicated devices.
- Paper wallet: Paper documents containing both the public and private keys of a cryptocurrency address. It is cold storage as it is not connected to the internet therefore, they are less vulnerable to attack. Users have to secure their wallets properly to prevent loss and unauthorized users from gaining access to them.
- Key Management services: This helps to eliminate the storing of private keys in a local device, rather allows keys to be stored on a remote server that can be accessed by the authorized users only and so reduce the risk of it falling into the hands of bad people, it used encryption and access control in protecting the keys. It can integrate with blockchain platforms to secure transactions that involve cryptographic operations and allows the delegation of key management to third parties by the original owners.
- Social Recovery: This recovery requires a high level of trust in the selected individual.
- Key Sharding: The private key is broken into several pieces and stored in different locations, like hard drives, clouds, and other people to prevent the loss or theft of the entire key. Cryptographic algorithms are used to break the private keys into multiple and smaller fragments called shares and each of these is encrypted and stored in a different location.



- Decentralized Identity System: This can be used by users to store and manage their identity in a decentralized manner, it allows users to prove their identity while sharing their personal information without relying on centralized identity providers or third-part services. It eliminates the storing of private keys as the identity of the users in the decentralized network and offers increased privacy and security because users have control over their personal information and are not reliant on centralized identity providers.

### 5.3 Method

In this paper, we investigated the private key issues in Blockchain, since private key plays a critical role in securing user's digital assets and ensuring the authenticity of transactions. Private keys are used to sign and authenticate transactions and without them, access to funds stored on the blockchain would be impossible. The issues of key management in the blockchain are.

- Private keys can be lost: There is no known way of recovering digital assets when a private key is lost, and this may cause a permanent loss of funds and resources.
- Private keys can be stolen; when a private key is stolen it will give the thief access to digital assets, including Cryptocurrencies. Cybercriminals may use various methods to steal private keys such as phishing attacks, malware attacks and social engineering.
- Insecure Storage of private keys: This is another way of security issues in blockchain and it can result in compromise on the digital assets, therefore private keys must be well stored securely and an unauthorized person cannot get access to them because if they get access to it, it will cause breach of security, private keys are stored as plaintext or on a device that is connected to the internet making them vulnerable to cyber-attacks.
- Human Error: managing private keys is prone to errors from humans, individuals may forget their private keys or accidentally delete them and may even expose them to the public or unauthorized persons which will give access to the hacker from gaining access to the private data.

Cryptography was used in this work, in which we converted data into a particular form so that only those intended for can have access and view the information and any unauthorized person cannot have access to the information.

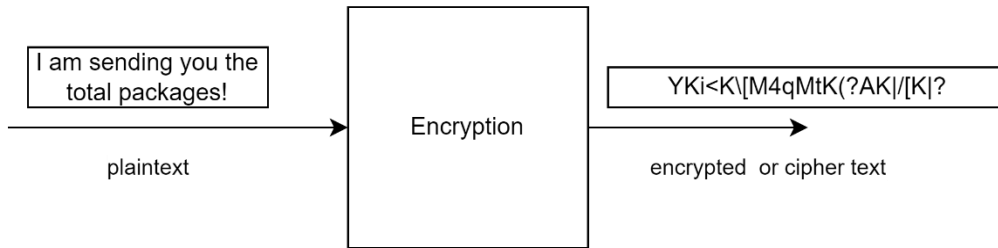


Figure 5.2: Encryption of plaintext message to be converted into a cipher or encrypted text.

The essence of these encryptions is to convert plaintext (readable message by anyone) into ciphertext (unreadable by anyone) for the intended user who will have the means of decoding the messages. The intended user can then use his or her key to decrypt the messages and make it readable.

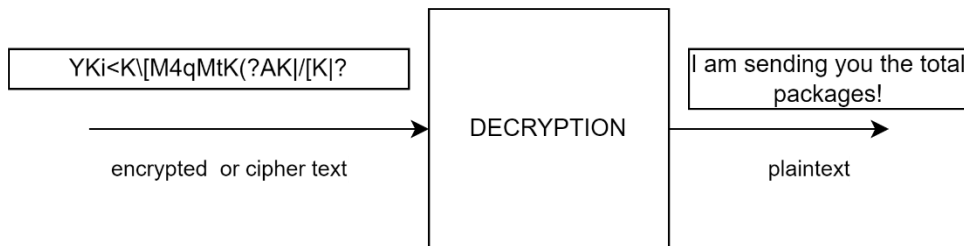
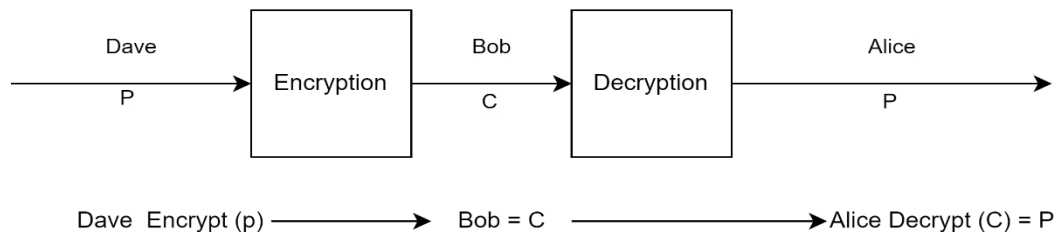


Figure 5.3: Decryption of the encrypted message from ciphertext into plaintext.

The essence of decryption is to convert unreadable messages into readable messages and make the message secure and safe for the intended user to read without hacking from the attacker.

This can easily be summarized as Dave sending an encrypted message to Alice, but Bob is involved, only Alice will be authorized to get access to decrypt the message even though Bob can see the message, he will be unable to read message because he does not have the authority to read the message.



P = plaintext, C = ciphertext,

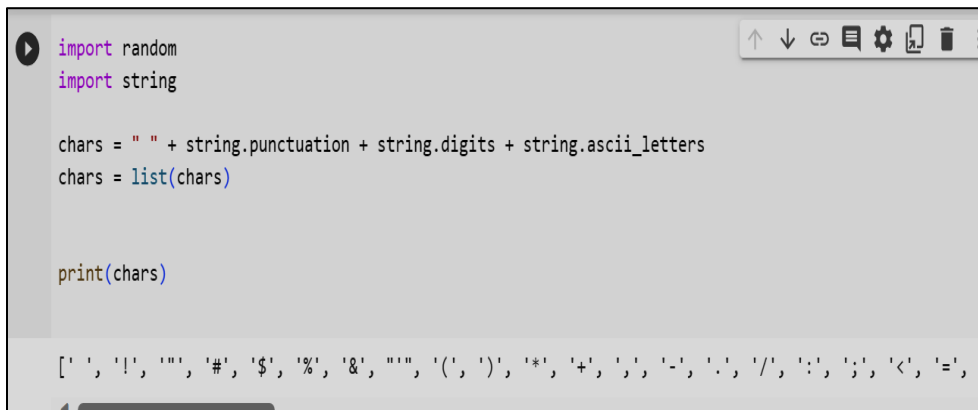
Figure 5.4: Process of encryption and decryption of data.

The creation of messages or transactions within the blockchain using key management of symmetric and asymmetric keys is an important security issue carried out to help prevent attacks within the network of the blockchain. In this work, we designed a blockchain with the message “I am sending you the total packages” which was encrypted using the hash function (cryptography). After the original message was encrypted, a private key was sent to the receiver to be able to decrypt the messages after successfully and securely transferring the message from one user to the recipient of the message protecting the intrusion into the message within our network.

A private key was used to encrypt messages in the blockchain, and the results are highlighted in the section below.

#### 5.4 Results

The output detailed in our Figures 9.5 through Figure 9.10, shows the processes and outcome in the design of our blockchain network, where a plaintext message: “I am sending you the total packages” is sent to another user and this message is encrypted to give an output known as unreadable messages (ciphertext). This was done starting with the generation of keys for every character of our messages and these keys are used to decide the encryption of the messages. From our work it was noticed in Figure 5.11, that for every time the transaction is made the keys change for each character, so as many times as the transaction is done there will be an equal and corresponding change in the generated output in the key. This was able to monitor the intrusion into the transaction by an unauthorized person. Figures 5.12 and Figure 5.13 highlight the decryption and encryption process and the final readable messages received and decrypted from the unreadable messages.



```

import random
import string

chars = " " + string.punctuation + string.digits + string.ascii_letters
chars = list(chars)

print(chars)

[' ', '!', '!', '!', '#', '$', '%', '&', '"', '(', ')', '*', '+', ',', '-', '.', '/', ':', ';', '<', '=', '

```

Figure 5.5: Generation of the printing of character string.

```

import random
import string

chars = " " + string.punctuation + string.digits + string.ascii_letters
chars = list(chars)
key = chars.copy()

print(chars)
print(key)

[' ', '!', '"', '#', '$', '%', '&', "'", '(', ')', '*', '+', ',', '-', '.', '/', ':', ';', '<', '=', '>',
[' ', '!', '"', '#', '$', '%', '&', "'", '(', ')', '*', '+', ',', '-', '.', '/', ':', ';', '<', '=', '>']

```

Figure 5.6: Generation of the character and key strings.

```

import random
import string

chars = " " + string.punctuation + string.digits + string.ascii_letters
chars = list(chars)
key = chars.copy()

random.shuffle(key)

print(f"chars: {chars}")
print(f"key : {key}")

```

Figure 5.7: Shuffling code for the characters and the key.

```

import random
import string

chars = " " + string.punctuation + string.digits + string.ascii_letters
chars = list(chars)
key = chars.copy()

random.shuffle(key)

print(f"chars: {chars}")
print(f"key : {key}")

#ENCRYPT
plain_text = input("write a message to encrypt: ")
cipher_text = ""

chars: [' ', '!', '"', '#', '$', '%', '&', "'", '(', ')', '*', '+', ',', '-', '.', '/', ':', ';', '<', '=', '>', '?', '@', '[', '\\', ']', '^', '_']
key : ['\n', 'N', 'Y', 'j', '|', 'Q', 'a', 'k', '3', '_', 'O', 'h', 'C', '=', '(', ' ', 'D', 'S', 'P', 'M', 'f', '?', 'w', '>', ',', 'U', 'W']
write a message to encrypt: 

```

Figure 5.8: Encrypting message with cryptographic for transaction.

```

1 import random
2 import string
3
4 chars = " " + string.punctuation + string.digits + string.ascii_letters
5 chars = list(chars)
6 key = chars.copy()
7
8 random.shuffle(key)
9
10 print(f"chars: {chars}")
11 print(f"key : {key}")
12
13 #ENCRYPT
14 plain_text = input("write a message to encrypt: ")
15 cipher_text = ""
16
17 for letter in plain_text:
18     index = chars.index(letter)
19     cipher_text += key[index]
20
21 print(f"original message: {plain_text}")
22 print(f"encrypted message: {cipher_text}")

```

Figure. 5.9: Printing of Encrypted messages in plaintext.

```

chars: [' ', '!', '!', '!', '#', '$', '%', '&', "'", '(', ')', '*', '+', ',', '-', '.', ':', '/', ';', '<', '=', '>', '?', '@', '[', '\\', ']', '^',
key : ['N', '"', '!', '@', 'P', ']', '?', 'B', '7', '>', 'H', 'b', 'D', 'M', 'i', 'z', '[', 'Q', '4', 'R', '-', 'E', '!', '!', '!', 't', '}', '#',
write a message to encrypt: I am sending you the total packages!
original message: I am sending you the total packages!
encrypted message: JN{XN%5dwhd-NIq1N^k5N^q^{:Nn{eZ{~5%

```

Figure 5.10: Plaintext input (encrypted message) output as ciphertext.

```

encrypted message: |F1}Fc^0
original message: I am sending you the total packages!
encrypted message: |F1}Fc^0=
original message: I am sending you the total packages!
encrypted message: |F1}Fc^0=a
original message: I am sending you the total packages!
encrypted message: |F1}Fc^0=a0
original message: I am sending you the total packages!
encrypted message: |F1}Fc^0=a0.
original message: I am sending you the total packages!
encrypted message: |F1}Fc^0=a0.F
original message: I am sending you the total packages!
encrypted message: |F1}Fc^0=a0.F;
original message: I am sending you the total packages!
encrypted message: |F1}Fc^0=a0.F;i
original message: I am sending you the total packages!
encrypted message: |F1}Fc^0=a0.F;i2
original message: I am sending you the total packages!
encrypted message: |F1}Fc^0=a0.F;i2F

```

Figure 5.11: Different ciphertext generated for every time the transaction is run.

```

22 print(f"encrypted message: {cipher_text}")
23
24 #DECRYPT
25 cipher_text = input("Write a message to be encryp: ")
26 plain_text = ""
27
28 for letter in cipher_text:
29     index = key.index(letter)
30     plain_text += chars[index]
31
32 print(f"encrypted message: {cipher_text}")
33 print(f"original message : {plain_text}")

```

Figure 5.12: Decryption of ciphertext into plaintext message.

```

chars: [' ', '!', '"', '#', '$', '%', '&', "'", '(', ')', '*', '+', ',', '-', '.', ':', ';', '<', '=', '>', '?', '@', '[', '\\', ']', '^',
key : ['K', 'k', 'F', 'f', 'p', 'j', 'e', '7', 'B', 'O', 'I', 'i', 'w', 'R', 'H', 'j', 'G', 'W', 'T', 'S', 'N', 'L',
Write a message to be encrypt: I am sending you the total packages!
original message: I am sending you the total packages!
encrypted message: YKi<K\[M4qMtk(?AK)/[K]?i]KIi+Uit[\k
Write a message to be encrypt: YKi<K\[M4qMtk(?AK)/[K]?i]KIi+Uit[\k
encrypted message: YKi<K\[M4qMtk(?AK)/[K]?i]KIi+Uit[\k
original message : I am sending you the total packages!

```

Figure 5.13: Encrypted and Decrypted messages output.

## 5.5 Conclusion

The key management principle in a blockchain server to secure and prevent unauthorized access into the transaction and this prevent the issue so hacker gaining access to personal information of the users, the only person authorized to have access are the intended users for whom the messages are meant. With this outcome we can say categorically that key management is secured and can safely deliver the blockchain from any form of attack.

## CHAPTER 6

### DECENTRALIZED IDENTITY SYSTEM, DIDs

#### 6.1 Introduction

After investigation and research into the Integrity, decentralization, and key management in solving the security issues in blockchain, we went further to investigate the Decentralized Identity systems, (DIDs), this is a new method being used in blockchain security to minimize the attack from unwanted sources. Decentralized Identity allows individuals to take full control over their credentials or personal information which is shared with the establishment or organization or with another individual within the blockchain network. The use of DIDs makes use of a Unique Global Identifier, UGI which allows all the entities on the network to communicate among themselves using machine readable, self-sovereign blockchain as the anchor. The use of DIDs allows for effective identifiers as it allows transactions to be done effortlessly without the fear of being hijacked by attackers or unwanted persons and it does this in a decentralized ecosystem by serving a traceable, tamper-evident, and unique source of verifying all the data about every entity involved. This protects all user's credentials and personal information by using a third party to verify the details. The benefits of DIDs are a good means of controlling access to the network and hence prevent attacks into the personal information of the user, good at maintaining the security of the transaction in any system including blockchain transactions, a unique identifier can maintain and protect the privacy of every entity on the network and, the ease of use of the DIDs helps in easy transactions being carried out successfully in the blockchain.

#### 6.2 Background

Due to so many atrocities taking place in blockchain transactions and any other system, the introduction of a Unique identifier is needed to maintain the privacy and security of personal details and hence help to protect the lives of individuals, organizations, and companies. The introduction of a Global Unique Identifier, GUI, helps in carrying out verifications of credentials of individuals and organizations using a third-party verifier.

##### 6.2.1 Global Unique Identifier

The GUI is used to monitor a secure transaction rather than using several entities to carry out the transaction verifications from one user to another up to the last user on the network. In this transaction

system, all the individuals or entities involved will have control over their data/information and will not be controlled by a single user. The power of GUI enables users to control their digital identity without the involvement of a third party.

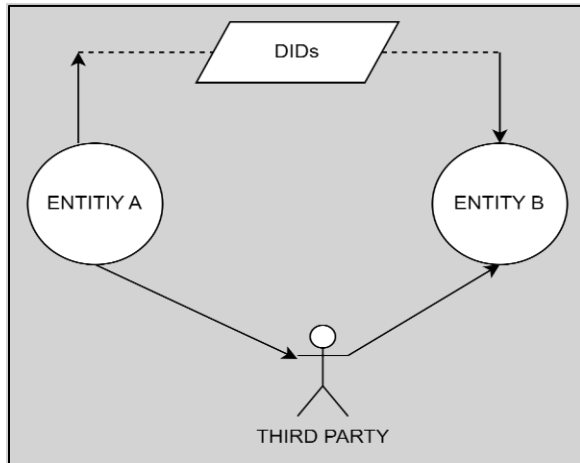


Figure 6.1: Decentralized Identity model.

The Decentralized Identity System works by eliminating third parties when verifying the credentials of a holder of the digital identity. In the Decentralized system in a blockchain, the DIDs are embedded in verifiable credentials, (VCs) created with an entity in a decentralized ecosystem and issued to the holder. The verifier can carry out the verification of the credentials of the holder using cryptography to check the connection between the holder and issuer and it can do so without the central system or the third party.

### 6.3 Method

In our research, we use DIDs to verify the credentials of an individual in Blockchain with digital identity and we take the following steps in carrying out work; We are using a cryptography key in the ID.me to derive the Identity of the user, Identity is shifted to the network model from a provider and all entities on the network get equal control of the verification.

We used ID.me to identify and verifying the credentials of a user seeking employment from an organization with a photo ID issued by the government and with our DIDs the credentials is sent to the verifier, who verifies the credentials as that of the holder.



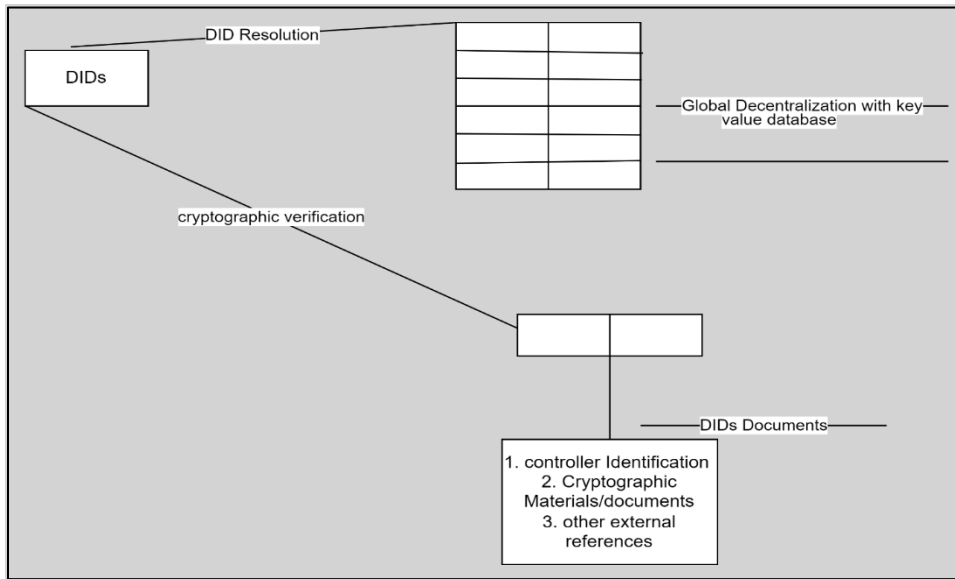


Figure 6.2: Model of the Verification credentials with DIDs.

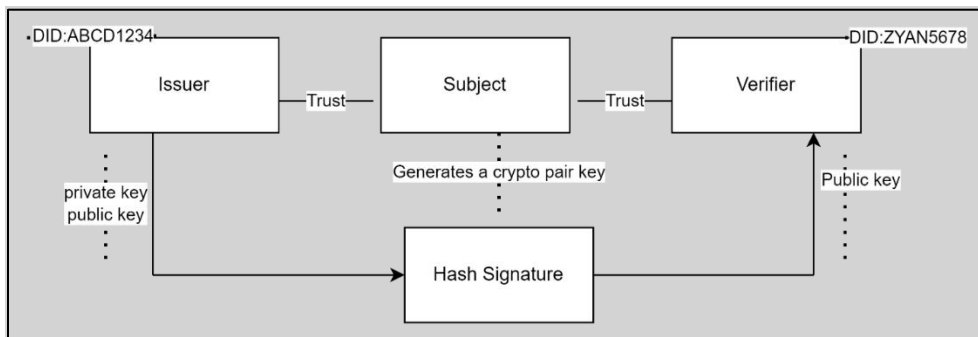


Figure 6.3: Credential Verification with DIDs.

## 6.4 Results

The credentials are verified with a DIDs resolution for every user of the blockchain network by sending the credentials issued by the issuer to the holders of the credentials and each user digital ID is used as the registration document for every user within the network, and a pair of keys is registered. i.e the public key and a private key, the verifier then used the verified credential VC as the key. A unique identifier is allocated for each user who participates in the transaction on the blockchain.

## Create an ID.me account

If you already have an ID.me account, do not create a new one. [Sign in to your existing account.](#)

\* Indicates a required field

**Email \***

**Password \***

**Confirm Password \***

**Remember me**  
For your security, select only on your devices.


I accept the ID.me [Terms of Service](#) and [Privacy Policy](#) \*

[Create account](#)

OR

Figure 6.4: Creating ID.me account for Credentials Verification.

## CONFIRM YOUR EMAIL ADDRESS



We sent an email to [olalekanadaramola72@gmail.com](mailto:olalekanadaramola72@gmail.com).

### Click the link in our email

Check your inbox for an email from [hello@id.me](mailto:hello@id.me) and click the link inside to confirm your email address.

If you do not receive an email within 10 minutes, check your spam folder and verify it hasn't been blocked.

[Why do I need to confirm my email?](#)

[Resend my verification](#)

OR

### Enter the 6-digit code from the email

**Confirmation Code**

[Continue](#)

Figure 6.5: Setting of email for account.

Figure 6.6: Account page creation.

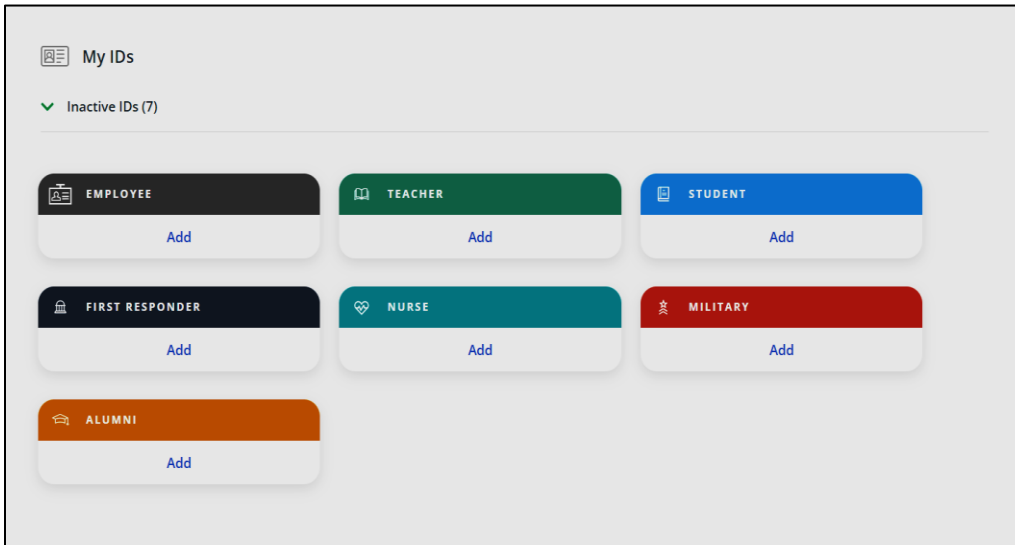


Figure 6.7: ID.me with user's categories.

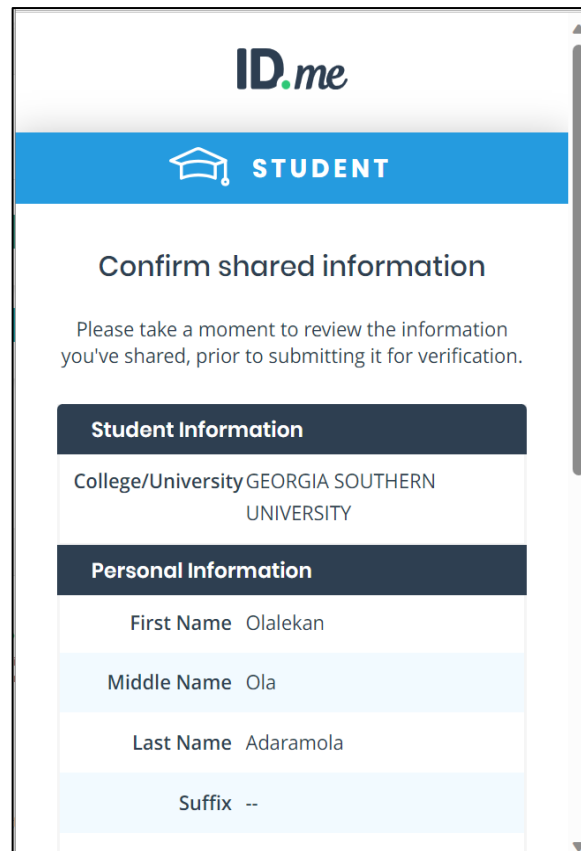
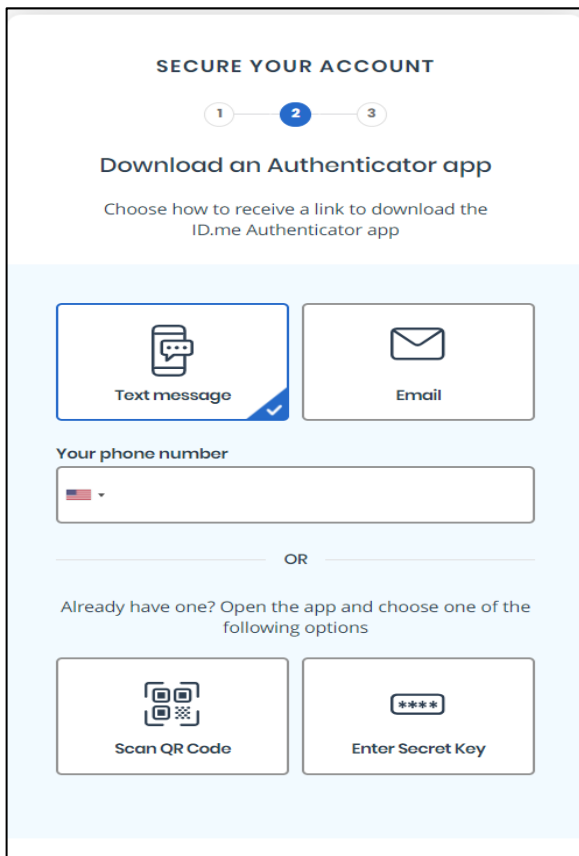


Figure 6.8: Authentication Security creation. Figure 6.9: Account verification Information page.

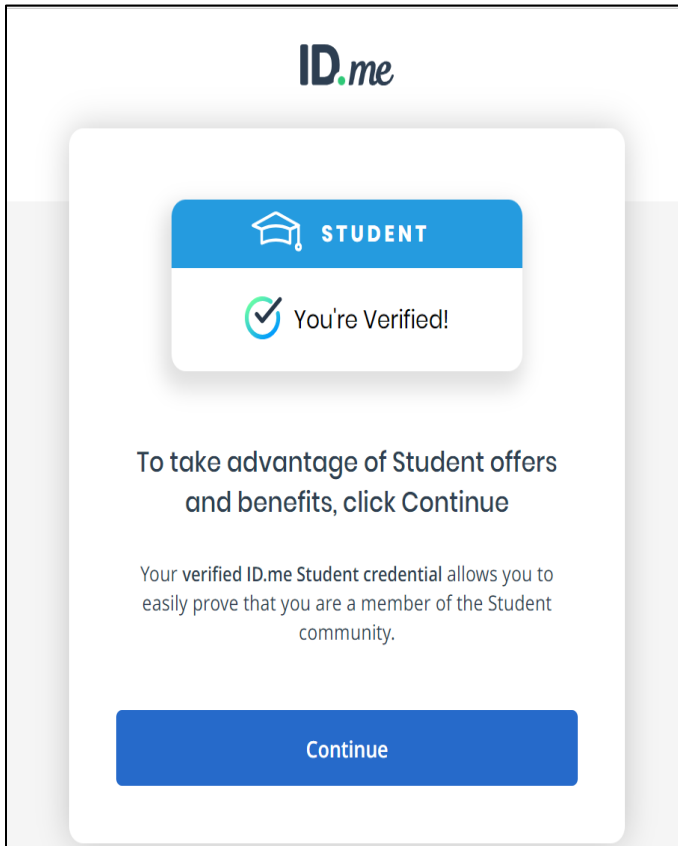


Figure 6.10: Credentials Verification completed.

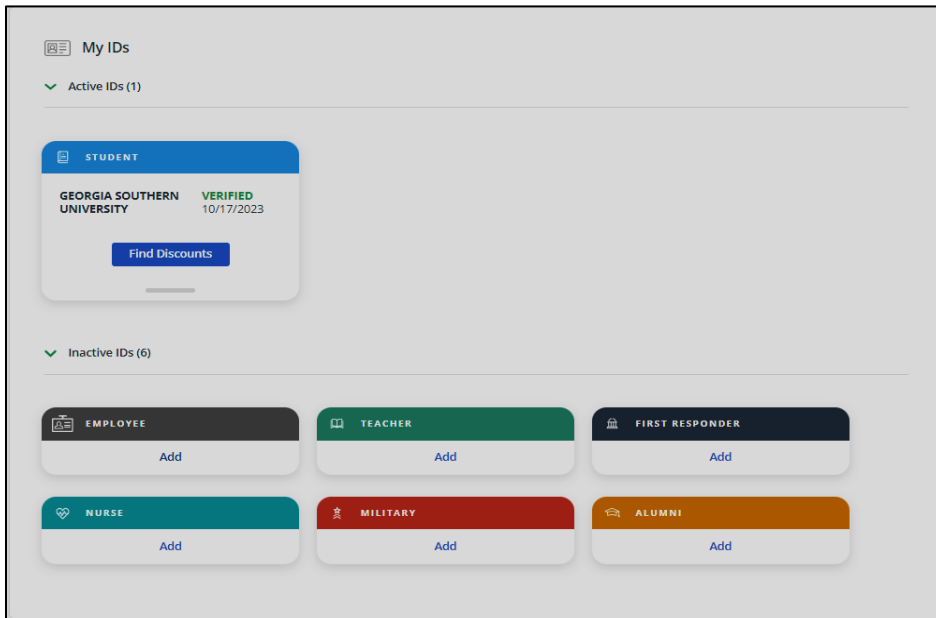


Figure 6.11: Confirmed Verification for Users.

The subject uses a dedicated app to generate a crypto key, (public and private) and save this in a specific place to keep it secure from falling into the wrong hands when the credential is finally verified the keys are used to make transactions on the blockchain with a DID that is also associated with the public key. In this process the Unique identifier through the verification of the user credential with a hash signature and crypto keys by both the issuer and the verifier will give the subject (user) a pass to make secure transactions on the blockchain and this will apply to all users of the network, so each user credentials and identity are first verified using the Decentralized Identity System (DIDs). Therefore, the security of the blockchain will be prevented and the privacy of all the members of the network will be preserved and secure their information.

Although several works have been done on the authentication verification of users in the blockchain such as using MySecure ID in which they do the Multi-factor authentication (MFA) to carry out the identification of users, the work failed to take care of the slow pace at which authentication is being carried out and it does not take into consideration of other verification factors such as occupation and age of every user involved in the blockchain. We also investigated the coinbase[64] and blockchain.com app.[65] for the verification process involved in gaining access to the blockchain and we have to improve on the entities used for verification, including the use of an easy method of signing in which is the email and password alone, Figure 6.12 and Figure 6.13 below show this. The use of the ID.me app gives an added security in which the verified credentials are saved on the app, making use of RSA signatories/hashees to put the verified credentials on the blockchain, such that when the user tries to log into the blockchain account, the saved credentials will pull up the person and allow them to have access to the account.

ID.me verifies the user's email, job, and date of birth together with all the information being verified by MySecure.ID, in coinbase and blockchain.com. this authentication using ID.me gives the blockchain a more secure act over the existing methods with ID.me readily available and able to maintain the integrity and privacy of all users.

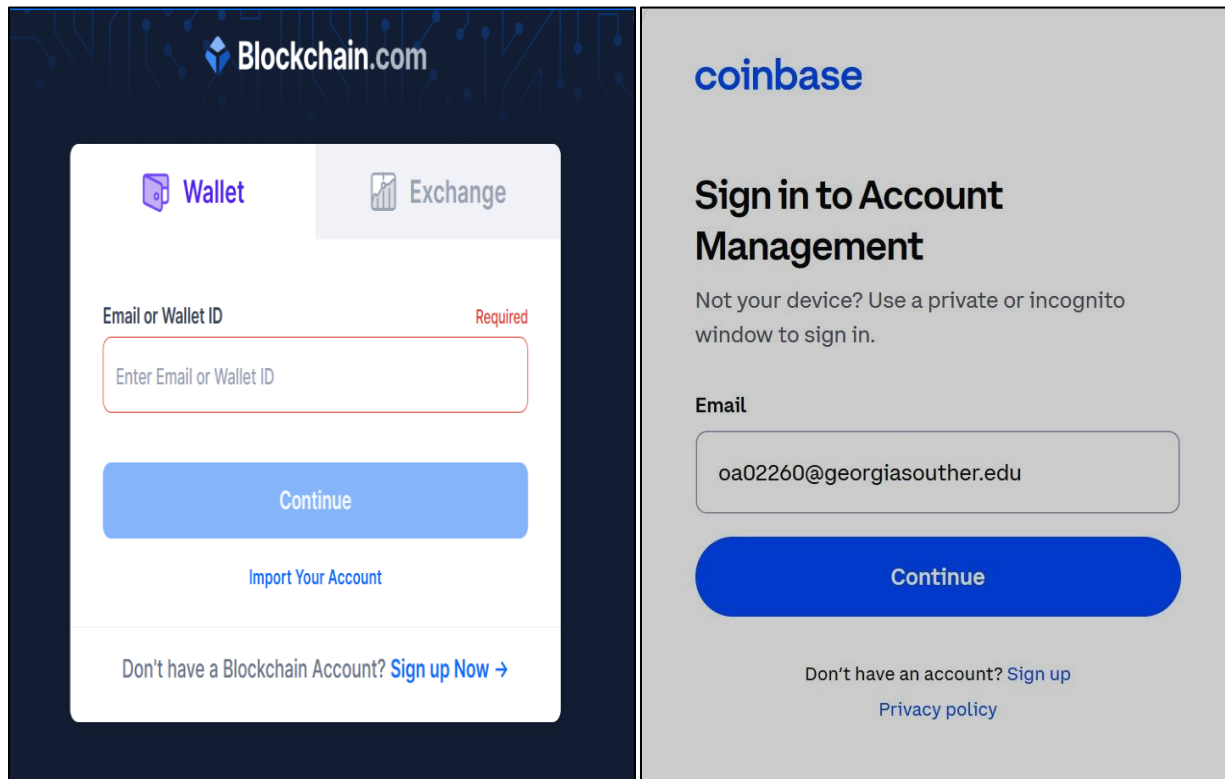


Figure 6.12: Comparison of Different authentication apps on the blockchain.

Comparing our work, using ID.me with MySecure.ID authentication gives a completely improved and different approach listed below.

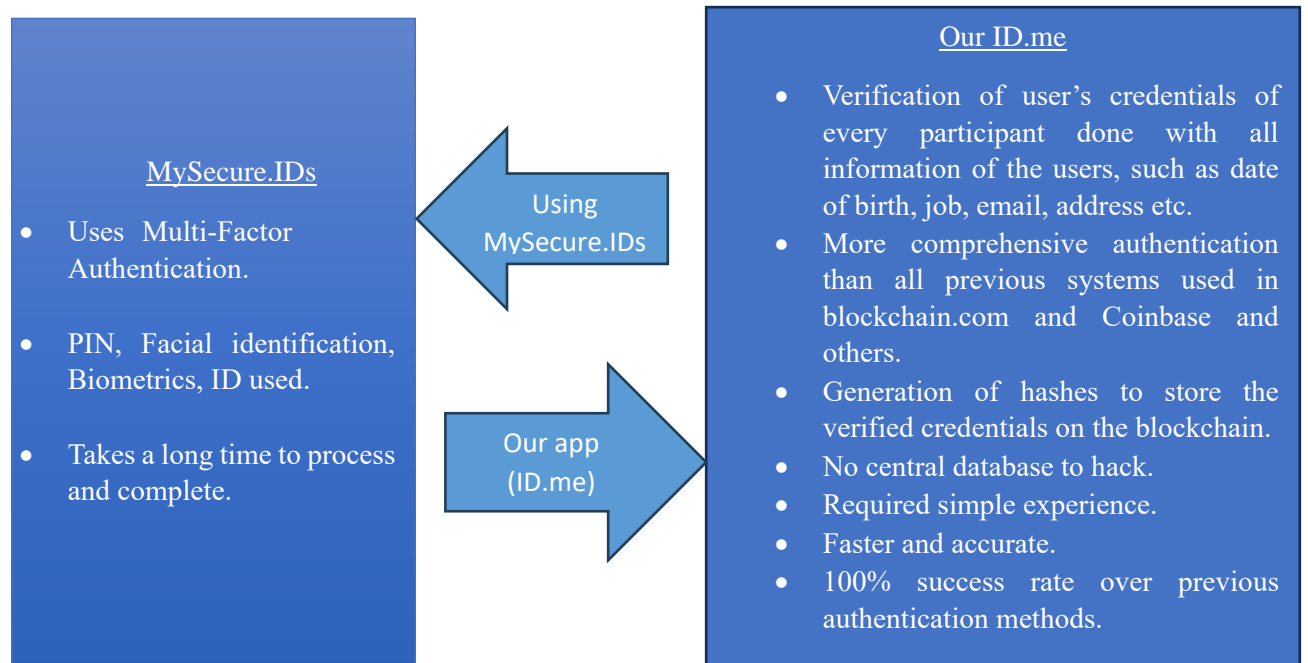


Figure 6.13: Comparison of MySecure.IDs with Our ID.me used in the blockchain.

Our ID.me with the blockchain account never adds cards to your wallet or shares your information with anyone and all the cards used must meet specific criteria before being allowed to be added to the wallet. This is an improvement over all other methods that have been used for authentication in blockchain. Our ID.me is a great improvement in managing the security in the blockchain by making sure of total verification of all identities of every user, when compared with other methods in existence this proves to be a more reliable, easy to use, and faster means of accessing the blockchain with accuracy and privacy of users put at the forefront of our work. This app is recommended for use by all organizations and users of blockchain in general.

## 6.5 Conclusion

Decentralized Identity Systems (DIDs) prove to be a reliable method of eliminating identity fraud in a blockchain transaction with the help of verification of credentials. From this work we were able to see that if employed in the blockchain transaction, it will first have to identify any user in the network and verify the authenticity of such user before allowing them to have access to any transaction. Why the use of ID.me is common knowledge that accurate and perfect identification is needed to be able to maintain the entities on blockchain technology and after reviews of previous work done on the blockchain, the problem persists such as keeping track of user's identities, and time of completion to sign in to the blockchain. This was visible in the Coinbase and blockchain.com shown above even using multi-factor Authentication in some of them, the time taken to complete the signing-in was slower than our method of using ID.me which is faster and accurate. From MySecure ID, using MFA with pin, facial, biometrics, and ID verification, a lot are still lacking in securing the blockchain due to the slow time in verification and it is equally possible to manipulate all the requirement, whereas our proposed method using ID.me will verify all credentials pertaining to every entity entering the blockchain, these include, the date of birth, job, email, address and every other verification done by the use of MySecure ID.

## CHAPTER 7

### DISCUSSIONS

In our work, the integrity was highlighted and with any little change in the parameters in the transaction gives a different hash value displayed this causes integrity to be affected and the transaction will be nullified and rejected as not the right transaction from the original messages. Also, decentralization, the process taken was to decentralize the distribution of the family will to all the family members in such a way that all members will be able to have control and access to the transaction at the same time. Thirdly, using key management in checking for the securities of the blockchain, we were able to encrypt a plaintext message with a ciphertext and the ciphertext changes with every new input and this makes the transaction well protected and secured from any alteration from unwanted/ unauthorized users (hacker/attacker), the output(cyphertext) is then decrypted using the same key from the encryption to get the plaintext (original message) back. The new work in this work uses Decentralized Identity System, (DIDs) in carrying out credential verification for all users in the blockchain network, and in so doing, the identity of all those that are allowed to transact business in the blockchain network are first verified before they can be allowed to access the network transaction. A unique identifier is included, and the user must provide a digital ID from the issuer who will then use a crypto key generated to encrypt the documents and send to the verifier for proper verification, the verifier on the other hand then uses a corresponding public key in decrypting the messages sent from the issuer and carry out a proper verification. The process of DIDs is effective in that it protects the credentials and records of all users, and it maintains the security states of the transaction, with privacy.

## CHAPTER 8

### CONCLUSION

Generally, Blockchain technology has security challenges just as much as every other technology, and being a new technology, a lot of effort is being made to maintain security and safely guide the transaction being carried out by users in a network without the problem of being hack into and stealing their information and hard-earned income. There is every need to ensure it is more secure and safe for users. Our outcome in this paper, shows that maintaining the integrity of transactions is very essential to avoid the transaction from being rejected, decentralization of blockchain transactions is also very needed to provide all users with control of their money and information and give access to trust from and across all the chain. This makes transaction done with good intention and believe in each other within the network and the use of cryptographic in key management helps in limiting the stealing of data that



belongs to another user, this eliminates the attack on blockchain since it requires the use of private and public keys in encrypting and decrypting messages and only the authorized person will be able to get access to the keys, but care must be taken to protect the key very well. And lastly, the Use of a Global unique Identifier in Decentralized Identity System (DIDs) play a very important role in protecting the problem that arises in blockchain transaction, by first carrying out a credentials verification of the intended user this means that any users whose credentials do not match the Id presented will be denied access into the transaction within the network and hence stop the attack or stealing of others information. After comparing our work of using ID.me to authenticate users of blockchain with all work that have been carried out on authentication in blockchain, we can infer that our work has a uniqueness in that provides an easy way to verify users' identity and still maintain the security, privacy, and integrity of the blockchain. It is a good means of controlling access to the network and hence preventing attacks on the personal information of the user. More work and implementation still need to be done on the securities issues of blockchain transactions especially with the use of DIDs which is the future of maintaining global security in blockchain technology.

## REFERENCES

- AWS, (2023). *What is Decentralization in Blockchain?* [https://aws.amazon.com/blockchain/decentralization-in-blockchain/#:~:text=In%20blockchain%2C%20decentralization%20refers%20to,thereof\)%20to%20a%20distributed%20network](https://aws.amazon.com/blockchain/decentralization-in-blockchain/#:~:text=In%20blockchain%2C%20decentralization%20refers%20to,thereof)%20to%20a%20distributed%20network).
- Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., Song, H., Alshamari, M., & Cao, Y. (2021). A survey on blockchain technology: Evolution, architecture and security. *IEEE access*, 9, 61048-61073.
- Biswas, K., Muthukkumarasamy, V., & Tan, W. L. (2017). Blockchain based wine supply chain traceability system. Future Technologies Conference (FTC) 2017,
- Blockchain.com. (2023). *Wallet*. <https://login.blockchain.com/en/#/login?product=wallet>
- Brewer, E. A. (2000). Towards robust distributed systems. PODC,
- Cai, T., Yang, Z., Chen, W., Zheng, Z., & Yu, Y. (2020). A blockchain-assisted trust access authentication system for solid. *IEEE access*, 8, 71605-71616.
- Cao, Z., & Zhao, L. (2021). A design of key distribution mechanism in decentralized digital rights management based on blockchain and zero-knowledge proof. 2021 The 3rd International Conference on Blockchain Technology,
- Catalini, C., & Gans, J. (2017). *Some Simple Economics of the Blockchain*. Rotman School of Management.
- Chen, T., Zhang, L., Choo, K.-K. R., Zhang, R., & Meng, X. (2021). Blockchain-based key management scheme in fog-enabled IoT systems. *IEEE Internet of Things Journal*, 8(13), 10766-10778.
- Choi, M. K., Yeun, C. Y., & Seong, P. H. (2020). A novel monitoring system for the data integrity of reactor protection system using blockchain technology. *IEEE access*, 8, 118732-118740.
- Coinbase.com. (2023). *Coinbase*. [https://login.coinbase.com/signin?login\\_challenge=e0e912c82fc4442ab67063ceda24526f](https://login.coinbase.com/signin?login_challenge=e0e912c82fc4442ab67063ceda24526f)
- Consulting, E. (2023). *What is Key management? How does Key Management work?* <https://www.encryptionconsulting.com/education-center/what-is-key-management/#:~:text=Key%20management%20forms%20the%20basis,data%20across%20an%20Internet%20connection>.
- Corbet, S., Lucey, B., Urquhart, A., & Yarovaya, L. (2019). Cryptocurrencies as a financial asset: A systematic analysis. *International Review of Financial Analysis*, 62, 182-199.
- Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics*, 14(4), 639-658.
- Fani, K., Ferreira, M., & de Vroomen, C. (2019). An exploration of state-of-the-Art blockchain scalability approaches. In.

- Febrero, P., & Pereira, J. (2020). Cryptocurrency constellations across the three-dimensional space: Governance decentralization, security, and scalability. *IEEE Transactions on Engineering Management*, 69(6), 3127-3138.
- FORUM, W. E. (2023). *Data Integrity*. <https://widgets.weforum.org/blockchain-toolkit/data-integrity/index.html>
- IBM. (2023). *What is blockchain security?* <https://www.ibm.com/topics/blockchain-security>
- Imam, I. T., Arafat, Y., Alam, K. S., & Shahriyar, S. A. (2021). DOC-BLOCK: A blockchain based authentication system for digital documents. 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV),
- Jia, M., Chen, J., He, K., Du, R., Zheng, L., Lai, M., Wang, D., & Liu, F. (2022). Redactable Blockchain From Decentralized Chameleon Hash Functions. *IEEE Transactions on Information Forensics and Security*, 17, 2771-2783.
- Joel Brawley, S. G. (1999). *Mathematical Models in Public-Key Cryptology*. [http://www.math.clemons.edu/~sgao/papers/crypto\\_mod.pdf](http://www.math.clemons.edu/~sgao/papers/crypto_mod.pdf)
- Kirupanithi, D. N., & Antonidoss, A. (2021). Self-sovereign identity management system on blockchain based applications using chameleon hash. 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC),
- KRIPTOMAT. (2023). *A Brief History of Blockchain Technology That Everyone Should Read*. <https://kriptomat.io/blockchain/history-of-blockchain/#:~:text=Nakamoto%20uploaded%20blockchain%20source%20code,with%20the%20associated%20cryptocurrency%2C%20Bitcoin.>
- Kwon, Y., Liu, J., Kim, M., Song, D., & Kim, Y. (2019). Impossibility of full decentralization in permissionless blockchains. Proceedings of the 1st ACM Conference on Advances in Financial Technologies,
- Lee, S., & Kim, S. (2021). Blockchain as a cyber defense: opportunities, applications, and challenges. *IEEE access*, 10, 2602-2618.
- Lee, Y. K., & Jeong, J. (2021). Securing biometric authentication system using blockchain. *ICT express*, 7(3), 322-326.
- Lehto, N., Halunen, K., Latvala, O.-M., Karinsalo, A., & Salonen, J. (2021). CryptoVault-A Secure Hardware Wallet for Decentralized Key Management. 2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS),
- Lei, A., Cruickshank, H., Cao, Y., Asuquo, P., Ogah, C. P. A., & Sun, Z. (2017). Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet of Things Journal*, 4(6), 1832-1843.

- Lin, C.-H. V., Huang, C.-C. J., Yuan, Y.-H., & Yuan, Z.-s. S. (2020). A fully decentralized infrastructure for subscription-based IoT data trading. 2020 IEEE International Conference on Blockchain (Blockchain),
- Lin, C., He, D., Kumar, N., Huang, X., Vijayakumar, P., & Choo, K.-K. R. (2019). HomeChain: A blockchain-based secure mutual authentication system for smart homes. *IEEE Internet of Things Journal*, 7(2), 818-829.
- Liu, Q., Safavi-Naini, R., & Sheppard, N. P. (2003). Digital rights management for content distribution. *Conferences in Research and Practice in Information Technology Series*,
- Lou, J., Zhang, Q., Qi, Z., & Lei, K. (2018). A blockchain-based key management scheme for named data networking. 2018 1st IEEE international conference on hot information-centric networking (HotICN),
- Ma, M., Shi, G., & Li, F. (2019). Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario. *IEEE access*, 7, 34045-34059.
- Ma, Z., Zhang, J., Guo, Y., Liu, Y., Liu, X., & He, W. (2020). An efficient decentralized key management mechanism for VANET with blockchain. *IEEE Transactions on Vehicular Technology*, 69(6), 5836-5849.
- Manan, S. (2022). *5 blockchain security issues and how to prevent them*. <https://www.fastcompany.com/90722111/5-blockchain-security-issues-and-how-to-prevent-them>
- Meng, C., Zhang, H., Ji, H., & Li, X. (2021). Mutual Authentication and Distributed Key Management with Permissioned Blockchain in MEC-Enabled Vehicular Networks. 2021 7th IEEE International Conference on Network Intelligence and Digital Content (IC-NIDC),
- Merugula, S., Dinesh, G., Kathiravan, M., Das, G., Nandankar, P., & Karanam, S. R. (2021). Study of blockchain technology in empowering the SME. 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS),
- Meurisch, C., Bayrak, B., & Mühlhäuser, M. (2020). Privacy-preserving AI services through data decentralization. *Proceedings of The Web Conference 2020*,
- Monte, G. D., Pennino, D., & Pizzonia, M. (2020). Scaling blockchains without giving up decentralization and security: A solution to the blockchain scalability trilemma. *Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems*,
- Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press.
- Nguyen, B. M., Dao, T.-C., & Do, B.-L. (2020). Towards a blockchain-based certificate authentication system in Vietnam. *PeerJ Computer Science*, 6, e266.

- Niavis, H., & Loupos, K. (2022). Consenseiot: A consensus algorithm for secure and scalable blockchain in the iot context. *Proceedings of the 17th International Conference on Availability, Reliability and Security*,
- Paduraru, C., Cristea, R., & Stefanescu, A. (2022). Enhancing the security of gaming transactions using blockchain technology. *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*,
- Pal, O., Alam, B., Thakur, V., & Singh, S. (2021). Key management for blockchain technology. *ICT express*, 7(1), 76-80.
- Panda, S. S., Jena, D., Mohanta, B. K., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2021). Authentication and key management in distributed iot using blockchain technology. *IEEE Internet of Things Journal*, 8(16), 12947-12954.
- Patrizio, A. (2023). *What is Decentralization in Blockchain?* <https://www.techtarget.com/searchcio/definition/blockchain-decentralization>
- Pereira, J., Tavalaei, M. M., & Ozalp, H. (2019). Blockchain-based platforms: Decentralized infrastructures and its boundary conditions. *Technological Forecasting and Social Change*, 146, 94-102.
- Pinheiro, A., Canedo, E. D., De Sousa, R. T., & Albuquerque, R. D. O. (2020). Monitoring file integrity using blockchain and smart contracts. *IEEE access*, 8, 198548-198579.
- Rodrigues, C. K. D. S., & Rocha, V. (2021). Towards blockchain for suitable efficiency and data integrity of IoT ecosystem transactions. *IEEE Latin America Transactions*, 19(7), 1199-1206.
- Saha, P. (2023). *Decrypt The Importance Of Key Management In Cryptography For Your Organization*. <https://www.encryptionconsulting.com/the-importance-of-key-management-in-cryptography/>
- Saha, R., Kumar, G., Devgun, T., Buchanan, W., Thomas, R., Alazab, M., Kim, T.-H., & Rodrigues, J. (2021). A blockchain framework in post-quantum decentralization. *IEEE Transactions on Services Computing*.
- Sharma, M. (2019). Blockchain for Cybersecurity: Working Mechanism, Application areas and Security Challenges. 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT),
- Shu, J., Zou, X., Jia, X., Zhang, W., & Xie, R. (2021). Blockchain-based decentralized public auditing for cloud storage. *IEEE Transactions on Cloud Computing*, 10(4), 2366-2380.
- Shuai, Z., Yong, Y., Xiao-Chun, N., & Fei-Yue, W. (2019). Scaling blockchain towards bitcoin: key technologies, constraints and related issues. *Acta Automatica Sinica*, 45(6), 1015-1030.
- Subramanya, S., & Yi, B. K. (2006). Digital rights management. *IEEE potentials*, 25(2), 31-34.
- Tang, Q. (2021). Towards Using Blockchain Technology to Prevent Diploma Fraud. *IEEE access*, 9, 168678-168688.

- Team, S. C. (2023). *A Guide to Advantages and Disadvantages of Decentralization for 2023*. <https://sharedeum.org/blog/advantage-and-disadvantages-of-decentralization/>
- Tian, Y., Wang, Z., Xiong, J., & Ma, J. (2020). A blockchain-based secure key management scheme with trustworthiness in DWSNs. *IEEE Transactions on Industrial Informatics*, 16(9), 6193-6202.
- Vigna, P., & Casey, M. J. (2015). *Cryptocurrency: how Bitcoin and digital money are challenging the global economic order*. Bodley Head.
- Wang, Q., He, L., Zhu, X., Huang, Y., & Li, Z. (2021). Privacy protection of blockchain security development status. 2021 4th International Conference on Information Systems and Computer Aided Education,
- Yin, H., Chen, E., Zhu, Y., Zhao, C., Feng, R., & Yau, S. S. (2021). Attribute-based private data sharing with script-driven programmable ciphertext and decentralized key management in blockchain Internet of Things. *IEEE Internet of Things Journal*, 9(13), 10625-10639.
- Yu, Y., Li, Z., Tu, Y., Yuan, Y., Li, Y., & Pang, Z. (2023). Blockchain-based Distributed Identity Cryptography Key Management. 2023 15th International Conference on Computer Research and Development (ICCRD),
- Zaman, M. U., & Min, M. (2020). Decentrally-Consented-Server-Based Blockchain System for Universal Types of Data. 2020 International Symposium on Networks, Computers and Communications (ISNCC),
- Zeng, S., Yuan, Y., & Wang, F.-Y. (2019). A decentralized social networking architecture enhanced by blockchain. 2019 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI),
- Zhao, J., Liu, J., Lin, L., Liang, L., Wang, H., & Xiang, S. (2021). Dynamic Security Mechanism for Lightweight IoT Devices Access to Blockchain Services. Proceedings of the 2021 4th International Conference on Blockchain Technology and Applications,

## APPENDIX A

**INTEGRITY CODE**

```
import hashlib

class Blockchain:

    def __init__(self, previous_block_hash, transaction_list):

        self.previous_block_hash = previous_block_hash

        self.transaction_list = transaction_list

        self.block_data = "_".join(transaction_list) + "_" + previous_block_hash

        self.block_hash = hashlib.sha256(self.block_data.encode()).hexdigest()

t1 = "Williams send 3 BTC to Anna"
t2 = "Jeff send 4 BTC to Greg"
t3 = "Jeff send 5 BTC to Anna"
t4 = "Greg send 4 BTC to William"
t5 = "Anna send 2 BTC to Greg"
t6 = "Anna send 2 BTC to Rick"

initial_block = Blockchain("Initial String", [t1, t2])
print(initial_block.block_data)
print(initial_block.block_hash)

second_block = Blockchain(initial_block.block_hash, [t3, t4])
print(second_block.block_data)
print(second_block.block_hash)

third_block = Blockchain(second_block.block_hash, [t5, t6])
print(third_block.block_data)
print(third_block.block_hash)
```

**DECENTRALIZATION CODE**

```
pragma solidity ^0.5.10;

contract Ola {
    address owner;
    uint fortune;
    bool deceased;

    constructor() payable public {
        owner = msg.sender; // msg sender represents address that is being called
        fortune = msg.value; // msg value tells us how much ether is being sent
        deceased = false;
    }

    // create modifier so the only person who can coll the contract is the owner
    modifier onlyOwner {
        require(msg.sender == owner);
        _;
    }

    // create modifier so that we only allocate funds if friend's gramps deceased

    modifier mustBeDeceased {
        require(deceased == true);
        _;
    }

    // list of family wallets
    address payable[] familyWallets;
}

pragma solidity ^0.5.10;
```



```
contract Ola {
    address owner;
    uint    fortune;
    bool    deceased;

    constructor() payable public {
        owner = msg.sender; // msg sender represents address that is being called
        fortune = msg.value; // msg value tells us how much ether is being sent
        deceased = false;
    }

    // create modifier so the only person who can coll the contract is the owner
    modifier onlyOwner {
        require(msg.sender == owner);
        _;
    }

    // create modifier so that we only allocate funds if friend's gramps deceased

    modifier mustBeDeceased {
        require(deceased == true);
        _;
    }

    // list of family wallets
    address payable[] familyWallets;

    //mapp through inheritance
    mapping(address => uint) inheritance;
```

```

//set inheritance for each address

function setInheritance(address payable wallet, uint amount) public {
    familyWallet.push(wallet);
    inheritance[wallet] = amount;
}

// pay each family member based on their wallet address

function payout() private mustBeDeceased {
    for(uint i=0; i<familyWallets.length; i++) {
        familyWallets[i].transfer(inheritance[familyWallets[i]]);
        // transferring the funds from contract address to receiver address
    }
}

// oracle switch simulation

function hasdeceased() public onlyOwner {
    deceased = true;
    payout();
}
}

```

### **KEY MANAGEMENT CODE**

```

import random
import string

chars = " " + string.punctuation + string.digits + string.ascii_letters
chars = list(chars)

```

```
key = chars.copy()
random.shuffle(key)
print(f"chars: {chars}")
print(f"key : {key}")

#ENCRPT
plain_text = input("Write a message to be encrypt: ")
cipher_text = ""
for letter in plain_text:
    index = chars.index(letter)
    cipher_text += key[index]

print(f"original message: {plain_text}")
print(f"encrypted message: {cipher_text}")

#DECRYPT
cipher_text = input("Write a message to be encrypt: ")
plain_text = ""

for letter in cipher_text:
    index = key.index(letter)
    plain_text += chars[index]
print(f"encrypted message: {cipher_text}")
print(f"original message : {plain_text}")
```

