

Securing Banking Systems with Blockchain Integration

Rama Krishna Kambhampaty - B00168197

Discipline of Cybersecurity,
School of Informatics and Cybersecurity,
Technological University Dublin

Submitted to Technological University Dublin in partial fulfilment of the
requirements for the degree of

Master of Science in Applied Cyber Security

Supervisor:
Muhammad Arshad

September 2024

| | | |
|---|--|---|
|  | <h1>Declaration Form</h1> <p>TO BE COMPLETED IN FULL</p> |  |
|---|--|---|

| | |
|---------------------------|--|
| Student ID | B00168197 |
| Student Name | Rama Krishna Kambhampaty |
| Assessment Title | Securing Banking Systems with Blockchain Integration |
| Module Code | H6029 |
| Module Title | MSC Research Project |
| Module Coordinator | Stephen O'Shaughnessy |
| Supervisor | Muhammad Arshad |

A SIGNED AND SCANNED COPY OF THIS FORM MUST ACCOMPANY ALL SUBMISSIONS FOR ASSESSMENT WITHIN THE BODY OF THE DOCUMENT.

STUDENTS SHOULD KEEP A COPY OF ALL WORK SUBMITTED.

Plagiarism: the unacknowledged inclusion of another person's writings, ideas or works, in any formally presented work (including essays, examinations, projects, laboratory reports or presentations). The penalties associated with plagiarism are designed to impose sanctions that reflect the seriousness of the University's commitment to academic integrity. Ensure that you have read and understand the University's Plagiarism Policy and Procedures.

Declaration of Authorship

I declare that the work contained in this submission is my own work and has not beentaken from the work of others. Any sources cited have been acknowledged within thetext of this submission. I have read and understood the policy regarding plagiarism in the Technical University of Dublin – Blanchardstown campus.

Signed.....



..... Date ...30/08/2024.....

Acknowledgements

I would like to take this opportunity to thank everyone who supported me while completing the masters and in particular during the completion of this research project. Your guidance and advice were invaluable throughout.

I would like to extend my thanks to my supervisor, Dr. Muhammad Arshad, whose support and feedback over the past weeks assisted greatly in making efforts towards the completion of this research. Your advice and reassurance was much appreciated throughout.

I would also like to thank my friends for their never ending support. Your advice and encouragement will never be forgotten.

Finally, I would like to thank my family. Mom, Dad I can't thank you enough for your wise counsel and constant support.

Abstract

This thesis demonstrates the provision of a secure blockchain system supported by AES, Ethereum digital signatures and a solid technology stack including Flask, React and MongoDB. It uses AES encryption with Base64 to encrypt the transaction data to maintain the data confidentiality and also for efficient encoding. The integration of Ethereum is done through integration of MetaMask for signing of the transactions and verifying them that increases the general security of the blockchain. The backend, using Flask and the frontend which is built using React is responsible for a good and an interactive UI of the application particularly in the creation of transactions and the Blockchain visualization, it also comes with a nice integration with the backend to enhance the user experience. As for the future work further developments of the methods of the key management, the increase in the throughput and efficiency of transactions employing the methods of sharding and other layer two solutions as well as the use of other blockchain networks are going to be considered. The study also acknowledges the successful implementation of AES encryption and Ethereum signing in building the secure blockchain platform for future advancements and improvements that may be expected in the decentralized technology industry.

Keywords: Blockchain, AES Encryption, Base64 Encoding, Ethereum Integration, MetaMask

Contents

| | |
|---|------------|
| List of Tables | vi |
| List of Figures | vii |
| 1 Introduction | 1 |
| 1.1 Background | 1 |
| 1.2 Motivation | 1 |
| 1.3 Scope of this Project | 2 |
| 1.4 Research Questions, Aims and Objectives | 3 |
| 2 Literature Review | 6 |
| 2.1 Blockchain Applications in Banking | 6 |
| 2.2 Implementation of Wallet Systems with Blockchain Technology | 16 |
| 3 Methodology | 26 |
| 3.1 Introduction | 26 |
| 3.2 System Development | 27 |
| 3.2.1 Overview | 27 |
| 3.2.2 Backend Development | 29 |
| 3.2.3 Frontend Development | 30 |
| 3.3 AES Encryption Implementation | 31 |
| 3.3.1 Ethereum Integration | 32 |
| 3.4 Data Collection | 35 |
| 3.5 Development Environment | 37 |
| 3.6 Blockchain Implementation | 39 |
| 4 Results and Discussions | 41 |
| 4.1 User Authentication Interface | 41 |
| 4.2 Blockchain App Dashboard | 42 |

CONTENTS

| | | |
|----------|--|-----------|
| 4.3 | Blockchain Structure and Transactions | 44 |
| 4.4 | Blockchain New Transactions | 45 |
| 4.5 | Mine Page | 47 |
| 4.6 | Performance Analysis | 48 |
| 4.6.1 | AES with Base64 Encoding | 48 |
| 4.6.2 | RSA Encryption | 49 |
| 4.6.3 | Comparative Analysis of AES with Base64 Encoding and RSA En- cryption | 50 |
| 4.7 | System Functionality | 52 |
| 4.8 | Discussion | 53 |
| 5 | Conclusion Future Works | 54 |
| 5.1 | Main Findings | 54 |
| 5.2 | Contributions | 55 |
| 5.3 | Limitations and Further Research | 56 |
| 5.4 | Conclusion | 57 |
| | References | 59 |
| A | Python Code | 61 |
| A.1 | Blockchain Class Implementation with AES Encryption and Ethereum Trans- action Verification | 61 |
| A.2 | Python Flask for Blockchain Operations and User Authentication | 62 |
| A.3 | Flask Application Setup with MongoDB and Ethereum Web3 Integration | 63 |

List of Tables

| | | |
|------------|---|----|
| Table 2.1: | Summary of Key Studies on Blockchain in Banking and Financial Services | 14 |
| Table 2.2: | Research Studies on Blockchain-Based Payment Systems and Wallets | 23 |
| Table 4.1: | Comparative Analysis of Proposed Method vs. RSA Encryption in Blockchain Systems vs. SHA-256 without tokens | 51 |

List of Figures

| | | |
|-------------|--|----|
| Figure 2.1: | Applications of Blockchain | 7 |
| Figure 2.2: | Services of Blockchain in Finance | 10 |
| Figure 2.3: | Interaction between sender and receiver | 17 |
| Figure 3.1: | Backend and Frontend architecture | 31 |
| Figure 3.2: | Ethereum Integration Architecture | 35 |
| Figure 3.3: | Proposed System Architecture | 40 |
| Figure 4.1: | login page | 42 |
| Figure 4.2: | Blockchain App Dashboard | 44 |
| Figure 4.3: | Blockchain History Page | 45 |
| Figure 4.4: | Blockchain New Transactions | 46 |
| Figure 4.5: | Mine Page | 48 |
| Figure A.1: | Blockchain Class Implementation with AES Encryption and Ethereum Transaction Verification | 61 |
| Figure A.2: | Flask Blueprint for Blockchain Operations and User Authentication | 62 |
| Figure A.3: | Flask Application Setup with MongoDB and Ethereum Web3 In- tegration | 63 |

Chapter 1

Introduction

1.1 Background

The background to this project lies in the continued weakness with respect to security of conventional banking systems, slow transaction handling, and doubts over open and secure access to banking services. Such concerns shed light on the areas of development that aim at improving the level of security, effectiveness as well as usability of functions within the field of finance. Blockchain technology can be regarded as the solution of these challenges. Blockchain is a decentralized and secure technology which provides a capability of smooth and trustworthy transactions through use of cryptographic principles and smart contracts [16]. Introducing blockchain technology presents an opportunity to enhance banking via implementation on Ethereum [22], Solana and so on, through their capability to reduce costs, time plus eliminate risks connected with frauds or data hacks. In addition, with the evolution of the blockchain technology beyond the use in cryptocurrencies into other financial applications, the idea behind blockchain This background creates the basis for identifying approaches to the implementation of block-chain, as well as its influence on the development of financial services, increasing the operational capacity of organizations, and creating the future state of the banking industry.

1.2 Motivation

Blockchain technology when incorporated in banking systems is a revolution in making and processing banking transactions and ensuring security. Currently, the conventional approaches that are used in banking systems experience a number of shortcomings or

critical issues such as; cases of fraud, slow clearance of banking transactions and most importantly, issues of compliance to the law. These problems indicate the importance of more secure, effective and clear systems. These are tracks that blockchain technology with its digital ledger is not only capable of handling but also can do so in an effective way. I found that using blocked chain, it is also possible to reduce the fraud factor as middlemen are avoidable, and data cannot be tampered with easily. Furthermore, due to its decentralised nature, blockchain has more extensive audibility and regulatory imminent with a record of all the account owns tamper proof. This project is inspired by the possibility of the blockchain in changing the face of banking system. By adopting blockchain in the conventional banking structures, it is possible to advance the measures of security, operation, and trust among the users. Thus, with the help of Ethereum or Solana platforms functioning, we plan to create a reliable banking system that includes, in particular, a blockchain-based secure digital asset wallet. In addition, the frontend and backend together with the utilization of Flask and Django enhances a friendly user interface for a mining platform and enable interconnectivity between blockchain networks and banking databases. Using fake money means that the performance of the system will be closely assessed to upgrade the quality and security, and efficiency once the actual coins will be used. The rationale for this project is to realise the dream of a banking environment that provides adequate support not only for the contemporary world's requirements but also for what the world will become in the future. Here, through analysing and applying the blockchain technology, is to offer solutions to the challenges faced by financial organizations in order to improve their services, cut costs of their operations and thus to help make the financial system safer and more transparent. Indeed, it is a relatively new concept that is capable of revolutionizing the way that banking is conducted, to the great advantage of both the banking companies and their clients.

1.3 Scope of this Project

This project is limited to the blend of the new age technology which is blockchain with the existing systems in the banking industry with an aim of improving security, efficiency of the process and experience of the user. This initiative includes the creation of a complete banking system where front-end and backend will be designed and coded in Python using the Django and Flask frameworks. One of the core competencies when it comes to the project is to design and integrate a blockchain wallet, using the solutions offered by, for example, Ethereum or Solana. This wallet will then be used to store and transfer digital

assets to and from various platforms in banking hence it has to have very high security and be interoperable with the existing blockchain. Further, the development of secure transaction channels and incorporation of smart contract capabilities to enhance the financial operation automation and security is also in the project. Connecting to blockchain networks will be done using Python libraries with emphasis made on the use of Polygon and Ethereum as these are effective networks. In these control tests dummy real coins will be used to analyse the function and safety of the system in its totality under different test conditions. Planned optimization strategies will be geared towards optimising the speed of the transactions, their cost and scalability of the system. In addition, the study will incorporate a security and privacy evaluation of the envisaged blockchain addition on the safety of transactions and protection of data in banking procedures. This involves assessing cryptographic protocols and consensus mechanisms with a view of finding out their strengths and weaknesses. Further, performance benchmarking and test will be conducted and scalability test to determine the capability of the system to accommodate large transaction that is characteristic of banking systems. Last but not the least, the result of the project will also aim at identifying the value proposition of blockchain adoption across the banking value chain both in terms of cost optimization and cycle time reduction among others as well as the level of customer satisfaction with overall banking services in order to provide a clear road map to stakeholders on how to leverage on the technology to optimize financial services delivery. This four-pronged approach seeks to foster formation of safe, sound, and transparent banking system that can cater for the changing needs of the banking sub-sector.

1.4 Research Questions, Aims and Objectives

The following research questions of this project are to address these important issues of applying blockchain technology to banking systems. These questions, therefore, seeks to meet the research questions that touches on the main issues and possibilities relating to the application of blockchain in financial market, with reference to Ethereum and Solana as platforms that enable secure and decentralized monetary exchange.

- 1 In what ways is blockchain technology suitable to be incorporated in the current banking systems to improve on it's security by reducing on cases of frauds and data breach?
- 2 What are the technical pitfalls and opportunities in the area of wallet implementation

using the blockchain principles for the purpose of safe storage and fast exchange of digital assets?

- 3 How does the integration of the blockchain in the banking system affect transaction Security and integrity, and general performance?
- 4 What risks and threats can there be associated with the adoption of the blockchain in the banking industry, with reference to the technological enhancements and general adoption of the best practices?

That is why the identification of the following research questions will help to reveal the broader prospects of blockchain in banking systems: The findings will help to extend the contribution to the development of the financial technology, providing specific advice to use in complexities and opportunities of the blockchain for increasing security, effectiveness and trust of users in financial operations.

In this project, it is the intended goal to upgrade the security and performance of banking systems via the use of block chain technology. As a result of limited investment in IT and shortcomings in IT infrastructure, incumbent banking industries continue to experience several persisting issues that are security threats, slow transaction turnaround, and low disclosure. Such problems call for new approaches that may address the need for improved security, more efficiency, and better customers' experience. The following challenges will be solved effectively through this project where blockchain is incorporated to be a decentralized and permanent database. The main aim is to incorporate blockchain into the banking system using a scalable environment through Ethereum and Solana explained for their reliability in dealing with secure transactions and integration with smart contracts. Major features of the project cover establishing a blockchain wallet that will safely store digital resources, improving the security of transactions using cryptographic means, and utilizing frontend hierarchies that are Flask and Django, being the optimal for using in Python. In the backend, most of the development will involve synchronization and management of data and it would be designed to work harmoniously with the blockchain network of banking systems. By making use of placebo coins and fair assessment as among the major objectives of the project, this undertaking endeavors to determine the viability of the application of blockchain in enhancing security, minimizing on cost of transaction and boosting efficiency in the banking systems. Therefore the goal of this research will be to provide the essential knowledge and guidelines for the industry members to create conditions necessary to make banking operations more safe, open, and efficient for the global economy.

The research questions of this project are as follows They pertain to the implementation of blockchain technology in banking systems, incorporating all aspects of security, efficiency, and user experience into the project. The objectives are designed to focus on major technical and operational issues connected with the application of blockchain in the existing financial systems.

- 1 For this, we have to investigate the role of deploying blockchain for improved security in the banking systems in this, we have to dissect the area of Ethereum and Solana, to determine ways of reducing or eradicating the risks posed by fraudulent and data breaches in banking systems.
- 2 Develop the blockchain wallet solution for efficient and safe management of digital assets together with the execution of transactions in the banking sector.
- 3 Exploit dummy coins to perform numerous tests to determine the strength, security and efficiency of the complete system under different conditions.
- 4 Analyze the level of positive changes in the banking sector due to the implementation of blockchain solutions.

Through the accomplishment of these research objectives, this project will be able to make the following significant findings; These are answers to the research questions which will enhances understanding of how blockchain can practically be implemented in banking systems. The results will not only contribute to the development of academic literature but will also be helpful to professionals from the various industries intending to improve the security, effectiveness, and transparency of financial transactions using blockchain technologies.

Chapter 2

Literature Review

2.1 Blockchain Applications in Banking

In the literature review part, the current works regarding the Blockchain Applications in Banking will be discussed with emphasize on its revolutionary aspect and limitations for further improvement of security and performance. Further, it will look into issues such as the advancement, use and utilization of Wallet Systems using the Blockchain Technology and some of the factors that must be put into consideration when Wallet Systems are being incorporated into the Financial Services. Thus, the first study which is provided by [2] demonstrates how with the help of Blockchain technology, there is a possibility to revolutionize banking activities and recommends further research of this approach in the sphere of banking. The authors complete the work with the introduction of an extensive literature and methodological analysis that concerns Blockchain in the context of financial services. Their method entails assessing the various ways in which Blockchain works in regulating its functionalities with the primary emphasis on its decentralised and immutable ledgers. They discuss the potential of signing transaction digitally, with no concerns on security and interpretation issues, intermediators not being required. However, the paper recognizes that there are various challenges associated with Blockchain especially on issues to do with scalability, legal frameworks and integration with the conventional banking systems. Nevertheless, the study reveals positive findings on how Blockchain has the potential of making transaction easier, more transparent and eliminate risks which are associated with a central authority such as a bank. Discussed in (Chowdhury et al., 2021) through case and theoretical analysis, Blockchain can positively affect the financial process, decrease the cost of the transaction, and enhance the total performance in banking

environment. Hence, the framework’s discovery further reaffirms significant improvements provided by Blockchain and presents it as a further solution to the existing problems in banking security, as well as the organizational structure of work.

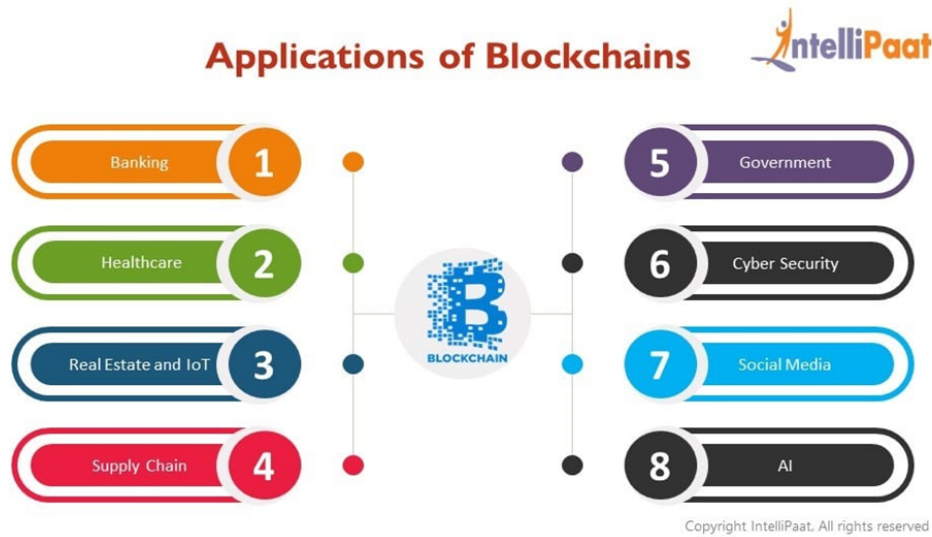


Figure 2.1: Applications of Blockchain

In the study which is offered by [7], blockchain technology is considered as a disruptive tool that could significantly alter traditional business models of various industries – particularly, banking and finance sectors – and the ways of conducting transactions. To start with, Fontana et al. undertook a qualitative set of systematic bibliometric critical analyses by reviewing 76 articles from 2016 to 2020. Conducting thematic analysis, the paper acknowledges the main research areas, describes five major benefits related to the application of Blockchain in the context of business, and reveals three critical issues regarding to the concept of Blockchain in banking and finance. The advantages that they post are increased security, higher transparency, fees involved in the transaction which can be rejuvenated and new business models. Challenges outlined include; scalability concerns, uncertainty in regulation, and compatibility problems with systems that exist. However, the study shows some positive results and affirm that the Blockchain application can bring positive results by increasing the efficiency of processes, preventing fraudulent actions, and providing people with confident transaction results. The study therefore recommends more studies to be conducted to fill the existing gaps and expand on the identified opportunities to provide valuable direction for future, theoretical and empirical, research in the field and appropriate practical applications in the industry. Also, [7] discusses the limitations of the

study and the direction of the further research, presenting their paper as a reference point for bankers and researchers wishing to embrace Blockchain's positive changes to banking and finance industries.

The study [20] carries Blockchain technology as a revolutionary disruptive technology in digital technology that is changing business models around the world and has received a lot of attention in various industries in India. It seeks to explain the working and structural features of Blockchain with a focus on decentralised application methodology. This paper provides an overview of some Blockchain characteristics and advantages as well as analyses the opportunities of its implementation in banking transactions with the help of use case assessments and fit analyses. Security aspects of Blockchain are also looked into to reinforce its application in exchange of data and values. However, as the final point of the paper, the author recognises the barriers in the form of policies that banking institutions face to embrace this great potential which, akin to the commercial Internet, is on the rise. Such issues include accomplishment of further elaboration of regulatory standards and development of cooperation with the regulatory bodies acting in the field of Blockchain- based solutions, as well as integration of regulatory considerations into Blockchain developments. The research ends by suggesting that regulators should become involved early in policies, and help with the furthering of understanding and evaluating the propensity for risk regarding Blockchain technology. According to the proposed approach, the banks should look for opportunities for such solutions, evaluate the possibility of implementing them, engage in the proof of concept test, and align with the regulators for compliance and integration. Therefore, in addressing these items of consideration, the paper seeks to assist the banking firms in harnessing Blockchain potentials in handling existing business challenges besides advancing efficiency in operations and in compliance with the law; and managing risks.

Moreover, as for the blockchain technology in financial services there is study by [12] that reveals the effect of the technology on bringing authenticity, security and risk management. It focuses on how organizations continue to incorporate blockchain technology with buying and selling and contracting and trade and other operational systems for smart contracts, better productivity, and new revenue streams. Blockchain's possibilities of creating an unalterable record book is cited for offering opportunities in the clearing and settlement processes thus optimizing functions for institutions involved in finance. Blockchain-based IDs are also considered as an opportunity for banks to improve the security of its customer databases and optimise the process of verifying identities. The paper suggests that more attention should be paid to predicting trends in applying blockchain technology

for finance and creating the necessary features for efficient further use of those trends. Nevertheless, there are some concerns; these are the regulatory issues, the improvement of the use and structure of blockchain technology that hinders its expansion of use and also, integration of the new system into the existing system. At the same time, however, the proposed use of blockchain raises a number of challenges that are nonetheless seen to elucidate asset ownership and financial obligations in order to enhance productivity and efficiency of accountants. The paper presents the research findings on the subject of blockchain's application in financial service along with various tools and strategies and the featured services in the bloc-based financial solutions. As a result, it discusses the critical uses of blockchain, especially concentrating on the role of innovative applications of that technology in the financial services industry, including the enhancement of credit reporting security; the desire to achieve a faster and cheaper execution of digital securities; the enhanced market opportunities accompanied with the minimized counterparty risk by customizable financial instruments. The paper calls for using the distinctive features of blockchain by standardized protocol-shared procedures for improving cooperation and data exchange among the business networks to increase the effectiveness and credibility of financial operations and services.

The role of Blockchain as the enabling agent for change in this banking industry as pointed by study [10] but also responsible for the surge in the volume of big data in the banking systems. It reveals an important research and development deficiency in the area of blockchain-based big data applications in banking, which presents a huge challenge to the utilisation and further development of this technology for banking innovation. Therefore, to help in filling the gap and encourage more focus by academicians, researchers and bank executives, this study provides a clear literature and theoretical review on the application and effect of blockchain on banking from the banker's perspective of view. The methodology comprises synthesising relevant literature to argue about the possible advantages of blockchain in improving security, relaying and processes inside banking institutions. The paper still recognizes other barriers like regulatory oversights, integration complications that stem from embracement of blockchain using existing systems, and the essential demand for appropriate data analytics skills that can transform blockchain-generated big data in banking fully. As stated in the study, the successor big data analytics of banking data will be derived from blockchain wherein on advanced filtering particularly signal extraction will be of critical essence. Despite acknowledging the fact that some of the banks across the globe have undertaken the use of blockchain in a limited way, this paper raises concern on the need to undertake research and development on the var-



Figure 2.2: Services of Blockchain in Finance

ious ways of using blockchain in banking to overcome the existing hurdles to widespread adoption. This way they provide an overview of blockchain discussion on banking, give an outlook on how it can change data processing and operations in banking and try to inspire cooperation that will further the development of the value enhancing applications of blockchain in banking.

In particular, the study [14] was concerned with the analysis of the banking industry to assess the opportunities of using the blockchain technology but also the arising problems. The research utilized the literature review approach, and the articles were obtained from the following recognized scientific databases were ABI Inform, Academic Search Elite, Emerald, Sage Premier, ScienceDirect, Springer Open, and Google Scholar. By applying the use of the PRISMA guidelines, six scholarly articles were used in the study after applying the inclusion and exclusion criteria. The data were categorized into five main areas: including cross-border payments, goods exports and imports financing, capital markets,

accounting and tax and anti-money laundering and other compliance procedures. The current study indicates that blockchain has the potential of transforming these banking sectors into efficient and effective sectors. More specifically, it will transform a range of value-added services such as cross border payments which are faster and cheaper, trade finance which shortens the time to execute trades, capital market operations and financial reporting and compliance through a secure open source ledger. Also, with blockchain, the ‘Know Your Customer’ (KYC) procedures are less complicated and safer. Nonetheless, the study also conducted a great threat analysis and distinguished considerable difficulties that might complicate the implementation of blockchain in banking. These are regulatory constraints, technological restraints, and the requirement for standardization of affair across the industry. The study revealed that blockchain has the ability to revolutionize the banking industry but without proper implementation of solutions to the emerged challenges the opportunity is unable to unleash. Therefore, the presented method underscores the importance of the balanced vision concerning the possibilities of using the blockchain technology and the challenges that have to be addressed for the successful application of this approach in the environment of the banking sector.

The central research question of the work [5] asks about the potential difference in the number of publications on the topic of blockchain technology, specifically, its use in central banks, by practitioners and academics. Employing Systematic Mapping Study methodology, the paper reviews the research to classify the peer-reviewed articles and papers regarding DLT applications in central banking tasks and activities. This is in order to map the research potential, in terms of saturation and trends and to identify failure and bad practices, in terms of the concentrations of the scientific workforce in specialisms. The study focuses on the application areas like CBDC, Regulatory Compliance and Payment Clearing and Settlement Systems (PCS) application areas that elicit great interest from researchers. On the same note, it records its non-involvement in the Assets Transfer/Ownership and Audit Trail. Thus, the study shows that the subject of the blockchain and the central bank is still largely emerging and is mainly initiated by the business world rather than academia. This can be an implication that the industry has scaled deeper and broader in the exploration of blockchain than the academia. The paper also identifies several challenges in the adoption of blockchain technology for the central banks which include; Trust, Performance, scalability, Interoperability, Integration and standardisation.

The streamer [3] shows how the blockchain technology has been implemented to solve actual business problem within the Italian Banking industry with a particular reference to an exploratory case study of Interbank Spunta project spearheaded by ABI Lab, the

research and innovation center of the Italian Banking Association. The nature of the Interbank Spunta project is to make improvement in the interbank processes where blockchain will be applied to the interbank processes in an effort to improve the visibility, as well as accelerate the execution time for the transfer of checks and money, and also the transfer of funds directly within the application. The research also places emphasis on emerging woes among bankers and some of these include issues to do with innovation and change in technology and the need to incorporate the new technology. The areas where the application of blockchain in banking according to the study may include the following; efficient interbank reconciliation, better record keeping and increased security in the transactions area. Although these propositions are designed to shape future research, their purpose is also to urge bank managers to adopt novel financial technologies for increasing value across multiple lines of business. These are some of the insights that could be derived from the present analysis which suggest that, while there are numerous advantages of blockchain as an enabling technology – more efficiency, and more transparency, among others, there are also considerable issues that one must acknowledge – from the regulatory horizon, to technological presuppositions, to the requirement for the entire banking community to embrace this new technology. The case study conclusion is indeed that blockchain is awaiting to revolutionize the banking processes to a huge extent, while the challenges delineated herein can be managed to ensure the successful application of blockchain if only more studies, researches and efforts in increasing innovation, and cooperation of the members in banking industry. Thus, the study contributes to the understanding of applying blockchain in banking activity and highlights the necessity of implementing new technologies as the tool for development and improvement of the sector.

The study [8] focuses on examining and quantifying business value addition believed to be attained by business organizations in the banking industry, arising from blockchain technology adoption, and on determining confirmable factors in the measurement of the perceived business values. The research deals with important issues that are associated with security, values and standards in banking operations. A sample of 291 respondents was collected, including blockchain consultants, marketing gurus and CEOs or business heads of the banking and financial institutes who are involved in advising or consulting in implementing Blockchain technology or using it in their business activities. For assessment of internal consistency reliability, the Confirmatory Factor Analysis (CFA) was used for testing the proposed measurement instrument. The analysis was useful for the validation of the instrument which produced five constructs that are highly reliable, valid and uni-dimensional. To be noted, this study suggests that despite blockchain technology is in its

infancy, the recent developments could affect the outcomes. The developed instrument helps decision-makers have the basic instrument that will enable them to evaluate the effectiveness of blockchain technology before adopting it into his existing system. Comparatively, this tool is most useful for its applications and its formulation of a method for assessing the effects of blockchain on the banking. It also discussed some of the issues that may be experienced in the implementation of the system including the need to achieve total security, standardization and instability of technology. The results underline the extensive opportunity of blockchain in improving banking activities where problems outlined above are solved. The study emphasizes the scientific and social impact of the work done by highlighting not only the research contribution to the academic advancement of the discussion on blockchain and banking triumphs, but also societal contributions to the advisance of practical guidance that can be offered by this research to leading executives and practitioners who intend to pursue adoption of blockchain.

Last but not the least, [6] discussing about non performing assets problem in Indian banking sectors recommends to leverage blockchain technology in the way that minimize the problem of moral hazard and adverse selection problems arising out of information asymmetry. The issues of credit have remained a concern in Indian banks suggesting that there is more need to reconsider and redefine the reporting and regulatory frameworks. The study shows that protocols of the blockchain technology decrease the uncertainty and contribute to credit risk evaluation reduced on enormous data and efficient generation of red flags limiting regulatory gaps. The proposed approach involves coming up with a comprehensive roadmap on how Regulation will be applied in credit decisions as well as having a better regulatory framework with the help of regulatory technology which is commonly referred to as RegTech. This can integrate the information that is already scattered within the banking system in order to enhance quality information for the lenders whereby; data driven finance enable efficient funding for credit risk and better tracking of loans. The major challenges categorised are therefore: risk of operational disruptions, which requires a solution in the form of risk management that anticipates disruption; and digitalised banking regulation, which requires enhancement through the adoption of effective regulatory frameworks. The study finds that integration of blockchain and RegTech can take the industry towards the improvement of the regulatory and reporting frameworks, prudent credit risk capital charge and efficiency of the banking system.

Table 2.1: Summary of Key Studies on Blockchain in Banking and Financial Services

| Study | Focus Area | Proposed Approach | Challenges Identified | Key Results |
|------------------------|--|---|---|--|
| (Javaid et al., 2022) | Blockchain in Financial Services | Review of blockchain's impact, tools, strategies, and applications in financial services. Focus on smart contracts, IDs, and digital securities | Scalability, regulatory challenges, interoperability | Showcases blockchain's potential to improve security, efficiency, and transparency in financial services, calls for more research to overcome adoption challenges. |
| (Cucari et al., 2022) | Blockchain in Italian banking (Interbank Spunta project) | Exploratory case study of ABI Lab's Interbank Spunta project | Integration with existing systems, adaptation to new technology | Blockchain can enhance data transparency, execution speed, and transaction security in interbank processes; significant potential but needs addressing integration challenges. |
| (Garg et al., 2021) | Measuring perceived benefits of blockchain in banking | Survey of 291 respondents; Confirmatory Factor Analysis (CFA) | Ensuring security, maintaining consistent standards, adapting to technological advancements | Validated instrument to measure blockchain benefits; high reliability and validity; practical tool for decision-makers in banking. |
| Continued on next page | | | | |

Table 2.1 – continued from previous page

| Study | Focus Area | Proposed Approach | Challenges Identified | Key Results |
|----------------------------------|--|--|--|---|
| (Chowdhury et al., 2021) | Blockchain in Banking | Review-based analysis of blockchain's application in secure banking systems, with an emphasis on its mechanisms and potential benefits | Scalability, regulatory compliance, interoperability | Demonstrates blockchain's ability to streamline transactions, enhance transparency, and mitigate risks, providing a comprehensive foundation for future research. |
| (Gan et al., 2021) | Blockchain in Finance | Bibliometric review of 76 articles (2016-2020), thematic analysis to identify hot topics, benefits, and challenges | Scalability issues, regulatory uncertainties, interoperability with existing systems | Identifies five key benefits and three major challenges, provides a foundation for future research, emphasizing blockchain's transformative potential in finance. |
| (Dashottar and Srivastava, 2021) | Addressing non-performing assets in Indian banking | Framework for blockchain in credit decisions and regulatory technology (RegTech) | Information asymmetry, robust institutional reforms, predicting disruptions | Blockchain and RegTech can improve data quality for lenders, leading to more informed credit decisions and optimized credit risk capital. |

2.2 Implementation of Wallet Systems with Blockchain Technology

The term “digital wallets’ has been given a new turn given the new found technology that is the blockchain technology. By review of the literature, this paper aims to survey previous research on wallet systems which are implemented based on blockchain technology, their usage, security measure, and the issues facing and prospects for advances in such systems. According to the type, there are two categories of Digital Wallets and they are Traditional Digital Wallets and Blockchain-based Digital Wallets. Recognising the need to cut payment, clearing and settlement cycles to avoid operational costs and risks in the financial sector, [21] has put forward a new architecture to link e-wallets of various banks and financial institutions through blockchain. A peer-to-peer network based on a swarm for this integration is proposed; it constitutes the foundational layer of the DLT for the Indian financial system. This architecture is effective in that it relieves the CBS of banks and in turn the servers at the data centers of high loads. One of the strategies that creates a big problem when practiced is coordinating and embarking on transactions that are smooth and involving several banks and many related financial institutions. The proposed solution eliminates this by establishing a sound and secure architecture to foster communication and transactions between separate sides of banking organizations. Based on such findings, an integration implies not only efficiency in managing the transaction but also improved security and effects contrary to those of traditional banking systems’ latency. The architecture optimises more operation efficiency and reduce financial risk by adopting the attribute of blockchain that is distributed random, make transparency and decrease the scale of fraudulent actions. As this total solution approaches the issue, it presents the parameters that will enable the development of some set standard that can produce e-wallet systems that can be readily integrated into the coalition or network to advance towards more coherent and efficient momentum in the financial shot. In this way, this approach provides India’s financial segment with huge potential for transactions and optimisation of subsequent financial processing, which will place emphasis on the further advancement of related SDGS.

[11] has put forward an electronic payment architecture known as Pure Wallet (PW), which creatively employs the Blockchain cryptocurrency for offline payments. The architecture works in a fashion that can be described in three stages. First and foremost, an Internet connection is needed to exchange a cryptocurrency for a token via a token manager starting a transaction which requires the information of the token. After that,

several offline purchases are performed using electronic devices for example the mobile phones through Near Field Communication (NFC). In this process, the sender converts the financial value into the token and through NFC sends it to the receiver's device. The last stage is when the receiver makes an attempt to exchange the received token back into the cryptocurrency by transmitting the required transaction details to the token manager only if he or she has access to the Internet. This makes financial transactions possible, possibly when an internet connection is not available, a drawback seen in most classic Blockchain integrations. It utilizes smart contracts on the Ethereum Blockchain to ensure that transactions that take place are both safe and valid. One of the major issues arising from such an approach is how to deal with the offline transactions where issues of security come to play and how to handle token conversion when connectivity is restored. The effects observed and obtained during the implementation verify feasibility of the offline transactions through Blockchain technology without any means of the Internet connection as necessary. Nevertheless, there are several questions that need to be answered for higher performant FA 2 tokens contracts and are outlined for further investigation., namely: Picking Blockchain for its implementation not only expands the application of cryptocurrency but also solves the missing link in the list of transaction functionalities enhancing the efficiency of the financial services in a limited or no Internet connection environment. Therefore, the proposed architecture is a leap towards a better solution in the field of electronic payments with more future proof financial transaction solutions.

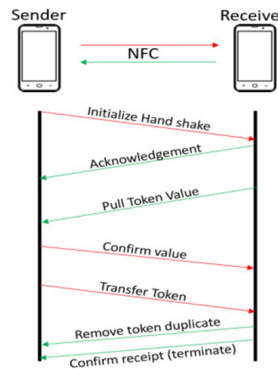


Figure 2.3: Interaction between sender and receiver

[13] raises broad guidelines on the incorporation of universal wallets and predicts that this can be a very effective advancement to the blockchain applications. In this paper, I propose the first substrate for handling universal wallets which are broader in function as compared to other conventional cryptocurrency wallets. The approach involves classifica-

tion of digital goods and the functions enabled by universal wallet and reflection on the existing and more elaborate study and research on the ways and appropriateness of universal and digital and crypto wallet in digital identity, self-sovereign identity management and other more classic and contemporary use of digital and crypto wallets. Interestingly, while wallets and blockchain are significant components of the digital environment, there is limited research from the information-systems tradition on these phenomena. Most of the current research is linked to the concept of crypto wallets, which, however, only give users a narrow range of opportunities, much narrower than universal ones. Based on the evidence generated in the course of the study, it becomes possible to identify the need to address the issue of wallet interactions with other assets, including cryptocurrencies and NFTs as well as study various implementations. Thus, the proposed taxonomy should be encouraging to see how concept of universal wallets can build better solutions for the more effective contemporary problem solving and at the same time share considerations concerning possible side effects. Moreover, the paper also includes the need for ‘smart,’ autonomous interactions of the wallets with their surroundings, which remains vital for safety and success of the given interaction with the user. In view of the development of AI and robust technologies, there is a need to study how these robust technologies will independently employ these wallets. Further, coupling with the IoT solution, Smart City, ID cards, universal wallets portray the importance of having policies, the regulation framework and self-enforcing governance. This study shows that the use of UWs could revolutionise digital encounters, and promote self-served and self-driven services. They could potentially unlock fresh forms of transactions and co-ownership – for example through NFTs. But at the same time, this becomes a question of privacy or surveillance. This generated taxonomy offers a conceptual framework of various uses and directions of the development of universal wallets to be further explored, including significant advices for IT, legal, economics, and socio-cybernetic fields.

In turn, another work of [4] focuses on the highly relevant problem of protecting digital currency purses, developing a lightweight purse on the basis of the blockchain and using Trustzone technology. Understanding the weaknesses of both the hardware and software wallet where while the former is highly secure but not easily portable and the latter is easily portable but not very secure this paper presents portable wallets that are secure yet easily portable. The current traditional wallets entail synchronization with blockchain and this is something that most of the mobile devices are incapable to handle due to memory limitations. To overcome this, mobile devices can employ Simplified Payment Verification (SPV) but with the currently available methods; the transaction verification process has

no adequate security. That is why the proposed approach involves using Trustzone to design and develop a secure execution environment (SEE) that would protect SPV. This design makes it more portable than hardware wallets, and more secure than the software wallets at the same time. The main issue solved is the impossibility of the Rich OS state affecting the wallet owner and the possession of the private key with the help of damaging the code and stealing the wallet address. In the same manner, by integrating these sensitive components and performing the transaction verification inside the SEE, the solution avoids the external threats of invasion and modification. Also, the approach merely encrypts local block headers hence they are indiscernible from the Rich OS and hence more secure. In the current experimentation of this method, the following were used: RASPBERRY PI 3 MODEL B development board. The result proves that this kind of design for secure lightweight wallet does not have much inflow on the system performance but greatly improved the security aspect. It manages to shield the wallet from sundry invasions and guarantee the sanctity of transaction authentication. It brings about an enhancement that offers better protection to the existing wallet solutions and also brings about convenience through a portable and practical way of handling and managing digital currencies. This study underscores the possibilities offered by Trustzone technology to improve mobile secured digital wallet and the possibility of the development of mobile payment system security.

[19] introduces a new concept of digital backup of the HW wallets addressing a major concern of safe and easy-to-implement backup and recovery. Honest hardware wallets are regarded as the most secure in terms of safeguarding private keys, yet, in case of loss or damage, they afford no means of a credible backup, other than writing mnemonics. This paper also captures some of the risks that are associated with this approach including for instance the paper may be lost or stolen thereby enabling the hackers to regain the keys. This was to overcome the above by using side-channel human visual verification through the display screen of the HW wallet. This novel approach enables the protected move of the root of the private keys from one hardware wallet to another with the aid of the untrusted terminal such as smartphone. In our approach, the security of the back up operation is improved since the private keys are not made a target to risks arising from other compromised devices. Particularly, the information transfer process is displayed on the hardware wallet's display so that the privacies of the relevant keys remain preserved. Upon the end of this process, users get two hardware wallets containing the same private keys, where one is the main wallet, and the other is backup. The primary issue solving this approach addresses is the presence of a reliable and easily accessible backup solution

while resistant to standard threats like mnemonic key phrase loss or theft. The backups are protected in this manner, as the results indicate, but the use of hardware wallets is not hampered. Users can be assured that a backup wallet is an exact replica of the original wallet that they can easily access in a bid to lessen the possibility of being locked out of the digital currency. Such a scheme greatly improves the general security and dependability of HW wallets, offering a practical approach to a key problem in the handling of crypto private keys.

[15] used an examination of the effects of development in digital payment on public spending therefore the method used in this study was a descriptive one to give a background to the events and succession of events regarding digital payments and how they shape consumer behaviour. This method has been enriched with strong theoretical frameworks from both, international and domestic sources. Digital payments referring to payment systems that use the Internet facilities as middlemen were analyzed with a view of making comparison and check the impact of making transactions. Among the issues that were notable in the course of this study, prospective and constant innovation and development in the growth of the digital payment technologies and their uses in demographic segments posed one of the major difficulties. Furthermore, the level of digital literacy was also high variable as well as the availability of internet services making the results of public spending more biased. However, the findings of the study were as follows: There is evidence that the use of digital payments shifts the government consumption from the retail sector which includes the sale of goods through physical store to that via online platforms or what is commonly referred to as e-commerce. Greater flexibility that emanates from the use of the digital payment systems was cited as capabilities that led to this change. DDD and proactive engagement research revealed that, many peoples' transactional behaviours reported being facilitated by digital payment enhancing daily transactions via e-money. This has not only adapted the purchasing behavior of the consumers but also enlarged the horizon in exercising E-commerce, thereby implying enhanced visibility of the Digital Payment solutions in the society and their upgrading as a mere routine.

[1] suggested a disaggregate study of the use of Bitcoin and other crypto currencies for online purchases with an intent of establishing a starting point for the research on the challenges that has slowed the generality of acceptance of these digital monies. The method used included the study of the current state of affairs regarding the use of cryptocurrencies adopting technological, economical and legal factors affecting their application in e-commerce. This research arose from the following research question: why has the opinion of cryptocurrencies as technologies that provide completely transparent, fast

and secure transactions not replaced conventional means of payment like digital wallets, banking cards, bank transfers, and cash on delivery? Among the main issues in question, the highest variability of cryptocurrencies has been identified as problematic since it prevents those currencies from stabilizing as media of exchange. Other challenges include problems in performance deterioration including transaction time and energy user of the systems. Further, there are legal issues and risks which are a challenge since legal frameworks differ across countries affecting the ease with which cryptocurrencies can fit in existing platforms. However, this study established that there is a rising trend in the adoption and acceptance of cryptocurrencies, primarily occasioned by the possibility of offering a new approach to online payments. But this interest has not yet lead to adoption, or widespread adoption, anyway, and the reasons are obvious given the barriers mentioned above. Accordingly, the identified trends called for improved respect for infrastructures, efficient legislation, regulation as well as the general public susceptibility to the promulgation of cryptocurrencies. In conclusion it is noted that there is a great potential in the use of cryptocurrencies but there is still a lot of work to be done to overcome the existing challenges to their wider adoption. The study provides premises for subsequent studies to look into workable solutions that would increase adoption of cryptocurrencies that will seamlessly fit into the function of digital currencies, hence achieving the intended function of cryptocurrencies.

[9] suggested the use of private blockchain to mitigate on processing and costs of payment card transactions. The approach envisaged the swapping of the conventional multiple ledger, third party reliant transaction type with a single, immutable distributed ledger based on private Blockchain technology. This blockchain system employs a linked list created with hash pointers to securely and efficiently store encrypted transactions with the aid of a decentralized and distributed ledger made comprehensible to all involved parties in the transaction. One of the major issues of concern in this proposition was on how to exercise a secure convergence of private Blockchain Technology in a financial system that involves cardholders, merchants, issuing banks, merchant banks and third party processors. Furthermore, it was not easy to persuade people to accept this new system, because they have done verifications in the existing method up to now. Nevertheless, the outcome of the study was also that private blockchain technology can reduce the fee for transactions by 95 percent because it does not involve third parties for validation. The former can raise the overall transaction value for the merchants as it lowers the fees involved. Furthermore, security of transactions in block-chain makes them almost irreversible and more reliable in relation to the payments making the process more trustworthy and less

prone to frauds. The study also noted that efficiency of the solution would enable organizations to make the transactions faster and cheaper in case private blockchains would be implemented properly.

[17] suggested that the use of an innovation known as a Blockchain-based mobile payment system can be used to enhance higher education student fee payment system in Zambia. Cross sectional study is used in the approach to establish factors that encourage use of e-Wallets by students. Hostels were purposively identified by the first author and PARTICIPANTS WERE SELECTED BY SYSTEMATIC RANDOM SAMPLING. Close questions questionnaires which were completed by the researcher were used to collect data and data analysis was done using SPSS and Excel. The study focused on seven predictor variables: Perceived ease of use, perceived usefulness, perceived cost, perceived risk, social norm, gender, age and perceived ease of risk. Based on the Likelihood Ratio Test, a 5percent significance level showed that perceived ease of use and gender were predictor variables that impacted on the adoption of e-wallets. Hence, the designers and developers of the e-wallet products were encouraged to develop applications that are easy to use and that captured gender preference by the users. In order to explain how it was developed, certain Unified Modelling Language (UML) diagrams were employed in order to depict the primary player or actor, role-players and actions, and classes. The prototype was implemented under an object-oriented paradigm, and consisted of an e-wallet mobile application, coupled with a RESTful API on the back end, based on blockchain. It was selected for the use of cryptography along with decentralized database that provides a tamper-proof and transparent database that can not be altered. The outcomes of the test also showed that through the suggested system, students can pay different fees with the convenience of the safety of the payment during the Covid 19 outbreak. It has a potential of reducing congestion of crowds and lengthy queues at financial institutions and higher learning institutions, the payment system being more efficient and secure.

[18] presented the design and implementation of a secure blockchain payment system for fee payment for higher learning institutions in developing countries in order to tackle problems arising from the current fee payment methods. As for the approach utilized in the payment system, the emphasis was made on the scheme based on elliptic curve public-key encryption and digital signatures. Choosing the object-oriented form of software development, system is designed as an e-wallet mobile application united with a RESTful API, and blockchain technology is the basis for the API. This has come up with this unique system that will enable students to overcome the long queues as well as overcrowding that is encountered at financial institutions when paying fees through remotes. Also, the

e-wallet may be employed in other purchases of goods and services that are provided within the institution as well as other associated merchants. In creating this system, however, one of the major concerns was the issue of the security and stability the system to warrant user confidence to use for financial transactions. However, the implementation of the blockchain in the current financial architecture of the institutions for higher learning posed a great challenge in planning and implementation. Nonetheless, the findings of the study showed that the proposed blockchain-based payment system aligns equally to the recognized performance hindrances and offers a safer way of payment especially during the Covid-19 period. This makes the system safe and dispersed so that there is small probability of fraud and thus user trust in the system is highly improved. Besides enabling payments to be made from the comfort of one's home, the proposed solution is also consistent with the current health measures that discourage contact payments as a way of tackling the spread of Covid-19.

Table 2.2: Research Studies on Blockchain-Based Payment Systems and Wallets

| Study | Focus Area | Proposed Approach | Challenges Identified | Key Results |
|------------------------|--|---|---|--|
| (Moonde, 2023) | Blockchain-based mobile payment system for higher education institutions in Zambia | Cross-sectional study with stratified random sampling and closed-ended questionnaires analyzed using SPSS and Excel | Secure and seamless integration, overcoming public resistance | Found that perceived ease of use and gender significantly influence adoption; prototype system showed potential for remote fee payments, enhancing safety during Covid-19. |
| Continued on next page | | | | |

Table 2.2 – continued from previous page

| Study | Focus Area | Proposed Approach | Challenges Identified | Key Results |
|----------------------------|--|--|---|--|
| (Moonde and Phiri, 2022) | Blockchain-based payment system for higher learning institutions in developing countries | Used elliptic curve public-key encryption and signature scheme; object-oriented software development methodology | Ensuring security and reliability, integrating blockchain into existing systems | Demonstrated the proposed system's ability to address inefficiencies, offer secure transactions, and facilitate remote payments, aligning with Covid-19 health guidelines. |
| (Jorgensen and Beck, 2022) | Universal wallets taxonomy | Developing a taxonomy to classify functionalities and applications of universal wallets | Limited understanding of interactions between wallets and digital assets | Potential for transformative impact in digital transactions and shared ownership models through NFTs. |
| (Igboanusi et al., 2021) | Universal wallets | Designing a taxonomy for universal wallets, exploring their capabilities beyond crypto wallets. | Lack of extensive research on wallets and blockchain. Focus mainly on crypto wallets. | Calls for more research on digital identities, self-sovereign identity management, and broader applications of universal wallets beyond crypto assets. |
| Continued on next page | | | | |

Table 2.2 – continued from previous page

| Study | Focus Area | Proposed Approach | Challenges Identified | Key Results |
|-------------------------|---|--|---|---|
| (Bezovski et al., 2021) | Impact of digital payment development on public spending patterns | Descriptive method supported by theoretical frameworks to detail events and trends related to digital payments | Capturing rapid evolution of technologies, varying levels of digital literacy and internet access | Found digital payments significantly alter public spending habits, shifting from offline to online shopping |

Chapter 3

Methodology

3.1 Introduction

In the methodology chapter draws out the systematic approach used in the setup and execution of the blockchain system, which defines the key technologies as well as the design concepts and procedure frameworks that were used to develop a strong and secure system. The focus of this chapter is to introduce the systematic approach for the development of the blockchain system, in its aspects of functional and security qualities enhanced by the use of the modern IT technologies and methodologies. Python Flask is selected at the core of the development process because of its good performance of web requests while providing a solid and sustainable framework for backend system. This backend which is at the heart of the blockchain system performs critical functions such as block chain management, transaction management or the interaction with Ethereum with the aid of Web3. py library. Flask was chosen because it is easy to handle server-side programming while being highly modular, allowing the different aspects of the project such as operations and transactions and cryptography to be handled independently. In essence, the structure of the blockchain is classes and these classes are equipped to create a block, validate the transactions as well as the mechanisms of proof of work. As for transactions, those are encrypted with AES and the cipher data encoded with Base64 gives additional security for the data's storage. MongoDB was chosen as the database because it is schema-less to adapt complex data structures in blockchain as well as it handle large records well. RESTful APIs when combined with Flask enables the frontend and the backend to interact; this includes the mining of blocks, creation of transactions, and even the retrieval of chains. In the frontend, React was used for rendering as it has excellent rendering capability

for user interface for managing the transaction and engaging with the block chain. The integration from the frontend layer with MetaMask, an Ethereum wallet extension, allows a safe signing of transactions while keeping users' private keys safe and maintain higher levels of security in the system. The frontend also uses different React hooks and the asynchronous API calls in order to create real-time data updates and the responsive UI. Web 3, integration of Ethereum with it. py, extends the system's features through allowing operation with the Ethereum blockchain; for example, the signing of transactions, the checking of balances, the verification of transaction information. Its integration is crucial to taking advantage of Ethereum decentralized finance ecosystem, security of the transactions taking place in the network. The methodology contains data gathering approaches vital for ensuring the legitimacy of the system that intermediate the creation of fake blockchain and user data required for testing and integration to the actual Ethereum node for real-time actions. This way of approaching the problem improves not only technical solutions that make up the system but also guarantees good working in practice. By integrating a number of elements of programming, such as Flask, React, MetaMask, and Web3. To work with MongoDB, and Amazon AWS in the process of the development, it has been done following the goals of scalability, security, and user satisfaction with a reliable blockchain system to perform real-life transactions with security enhancement.

3.2 System Development

3.2.1 Overview

The architecture of this blockchain project is highly structured in a way that will accommodate the backend development, the frontend view, and use of the Ethereum blockchain within the project. In detail, it has backend based on Python Flask where choice fell on a non-redundant and lightweight system which effectively handles web requests and server-side logic. It is possible to state that Flask enables the creation of a clean architecture that consists of four layers which are being responsible for crucial aspects of the blockchain system. Such layers include the block management layer that is responsible for the creation of blocks, handling of transactions and integrity of data, the business logic layer that encompasses the algorithms and even the transactions layers that handles transactions and encrypt them before storing to the blockchain and the encryption layer that uses the AES encryption to make the data that is to be included in the blockchain secure. The Blockchain class which is one of the basic components of the backend is

used for creating the blocks and the blockchain, as well as for the transactions. To avoid unauthorised addition of blocks to the blockchain it has a proof of work function incorporated to the protocol. For storage, the MongoDB tool is used because it doesn't require fixed structure for storing information concerning the blockchain system or users. There is also a backend that which comprises of RESTful APIs which were built using Flask to enable interactions between the frontend and the blockchain. For the basic functioning, these APIs having the required points like /mine for the addition of new block, /transactions/new for transaction initiation and /chain for getting the details of the blockchain. For the purpose of user authentication, appropriate JSON Web Tokens (JWT) have been implemented in such a way that only qualified users could conduct operations to the system. Similarly, the frontend is with React, a dynamic JavaScript library that has earned fame by representing the UI quickly. React is basically the front-end through which users engage the blockchain; creating transactions, logging in or signing up and displaying the information among others. Frontend design is centered on offering easy to utilize designs that entails various components that handles various parts of the interface. For instance, the NewTransaction component is used for entry of data when developing transactions while the integration of MetaMask enables safe signing of such transactions using keys on Ethereum personal machines. This integration will also make sure that the actual signing of transactions is done off the application hence reducing the chances of keys being exposed. Possibilities for state management through hooks inclusive of real-time changes like changes of state in the blockchain or levels of user balances. The system also makes use of CORS for frontend to communicate with the backend securely and the use of HTTPS to eliminate the possibility of common web vulnerability like XSS and CSRF. Another component of the system is Ethereum integration, using Web3. py that will allow connecting the blockchain application with the Ethereum network. This integration enables several Ethereum-specific functions, among them, signing of the Ethereum transactions, checking balance and verifying Ethereum transactions signatures. MetaMask, a browser extension that lets the user manages his Ethereum accounts and sign transactions safely without revealing the keys. When a received transaction contains a signature, a backend employs Web3. y to check the validity of the transaction and gain the Ethereum address of the signer so as to avoid fraudulent transactions. The decentralized concept of Ethereum builds up to the security and credibility of the system, implemented with recorded transactions being non-negotiable. Architecturally, it is designed that there are possible future upgrades: smart contracts, the transition to new versions of Ethereum like Ethereum 2. 0 which is said to have better scalability, security and sustainability than older versions. In

general, this system architecture perfectly combines backend and frontend solutions along with Ethereum's blockchain characteristics to provide a safe, manageable, and convenient blockchain platform.

3.2.2 Backend Development

Python Flask is set as the main focus of the backend development of the blockchain system due to its simple and lightweight approach in handling of web requests for the system and the simplicity realized in the management of server-side programming. The backend section takes care of fundamental blockchain functionalities and accounts management, ERC20 integration for the verification of transactions. The architecture of Aries is principally divided into four distinct layers, and more importantly, the business logic of the blockchain management, the transactions and the encryption are designed to be entirely separate within their respective module. The blockchain is implemented as a class, Blockchain, responsible for the creation of the blocks, management of the blockchain and the addition of the transactions. This class is created with important operations which are the block creation, proof of work, and transactions. Transactions, an index, timestamp, proof, and hash of the preceding block are other fields stored in blocks in the blockchain are encrypted using the AES encryption. The proof-of-work system is put in place to prevent a bad actor or a malicious user from inputting a new block on the chain, hence safeguard the integrity of the chain. It is essential for data privacy, especially data in the transaction layer, to involve AES encryption to enhance data security before adding the actual data that will go into the blocks. The cipher data is further required to be encoded with Base64 so as to ensure safe storage and transfer within the system architecture. MongoDB is used for intents and purposes of storing the block-chain data and for maintaining the user accounts. One of the major characteristics of MongoDB is that it is schema-less, and this is important and appropriate when storing records of blockchains and this is because blockchains are likely to undergo transformation and adaptation and therefore the records stored must be adaptive in the way they are stored as well. The backend also consists of RESTful API that was created with Flask and this is actually how the frontend communicates with the blockchain. The API endpoints are /mine for mining new blocks, /transactions/new for creating new transactions and /chain for getting the chain. The api user endpoints /signup, /login use JSON Web Tokens (JWT) to allow only authorized users to interact with the blockchain. Among the most important activities of backend development, one must mention the integration with Ethereum using Web3. py is a Python library to in-

teract with Ethereum blockchain. This integration allows for the performing of Ethereum specific operations including balance and transaction checks. The backend takes signed transactions from the frontend, reassembles the original message and uses Web3. This change brought the ability to decode the Ethereum address of a signer back to py. This process helps in signing and confirming the transaction and increases the level of security to the system of blockchain.

3.2.3 Frontend Development

In frontend development we use React, a javascript library tried and tested for its fast and dynamic rendering of user interfaces. It acts as the link between the user and the blockchain, thus its responsibilities include; creation of transaction, sign-in/ sign-up processes and presentation of blockchain data. The focus is made on the system's interaction design, which means that the system is constructed in a way that will be understandable by users with little knowledge of its inner functioning. The frontend is divided into a tree of reusable components which each component is responsible for the management of a chunk of user interface. For instance, the NewTransaction component is concerned with data entry that is required when creating a new transaction. This component communicates with the MetaMask, a browser plug-in that gives the users ability to handle Ethereum accounts from the application. MetaMask integration is crucial as it is capable of signing transactions with the users' private Ethereum key thus solving the problem of signing transactions without having the private key compromised by the application. Once the offer is signed it becomes a transaction and sent to the backend ever for encryption and integration with the block chain. Some of the components of state management which are frequently used in React are hooks which have a big influence on how user data and the dynamic sides of the system are handled. For instance, if a user makes a new transaction on the frontend, the state changes to the new transaction details and then the new details are sent to the backend using APIs. It also takes data from the backend like, the state of the blockchain at the moment or the balance of a particular ethereum address and presents this information real-time to the user.

This interaction is done with the help of the Flask API by asynchronous calls to it that allows the user interface to be active even when processing big amounts of data or considering complex calculations. Security is also realized at the frontend using CORS configuration to allow only request from some specific origin (same as the backend). This also helps in secure the API from unfavourable web issues like Cross-Site Scripting (XSS)

and Cross-Site Request Forgery (CSRF). Furthermore, HTTPS for secure communication between the frontend and the backend is mandatory to guarantee the safety of all front end data by encrypting the information in the course of the user-server communication. The consequence is that the frontend development is the important part of the application that provides the safe and convenient front-end to interact with the blockchain system. By connecting React to the Meta Mask App and the Flask back end we guarantee that the system is safe and comprehensible to use, thus presenting the capability to make blockchain operations and ethereum transactions all in one interface.

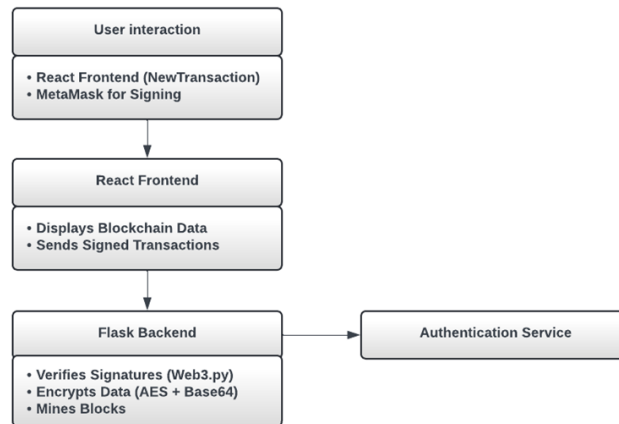


Figure 3.1: Backend and Frontend architecture

3.3 AES Encryption Implementation

The AES encryption with Base64 encoding for checking transaction data security was developed with great care for the necessary security for the information as well as its ease of usage. The process was started with the generation of AES keys from a secure random number generator, done in Python language with the help of cryptographic library providing the tools for cryptographic operations. The keys were also created to have a high entropy to enhance on their security given the fact that the generation was done using AES-256. This was instrumental in ensuring the confidentiality and integrity of the transaction data when in use, in transit and at rest. In the process of encryption several steps were followed with the help of these trees. First, anonymized raw transaction records including sender's and receiver's wallet addresses, transaction amounts and their timestamps were encrypted by AES-256. AES with its motives of performance and high level of security is used in symmetric key encryption. The data was encrypted into what could be better

referred to as ciphertext as the essence of the data was retained although it could not be understood by anyone who did not have the key to decrypt it, it kept the size and structure of the data for simplicity in the system. It was then Converted into Base64 after the encryption had been done to produce the Ciphertext. Base 64 was used to put the binary cipher text in to textual format so as to ease on storage and transmission. This encoding was necessary as the data in the text format was simpler to work with when it comes to data storage as well as data transmission.

After the retrieval of the encrypted transaction data, decryption of it was performed. The process started with Base64 decode to decode it into its binary form so that it is ready for decryption process. After this, the AES key that has been managed and stored securely had been used to decipher the binary data into its original form of plaintext. The decryption process was just the reverse of the encryption operations with the help of which the transaction details were once again converted into readable form so that the system could check and authenticate the transaction information. This kind of approach of using both AES encryption and Base64 encoding doubled the security of the transaction data while at the same time made the data easy to manage within the system, and thus both aspects were achieved. Several important aspects of data safety were met by the pbFT protocol because of the significant AES encryption and Base64 encoding. AES encryption gave good security against intruders in a way that if a hacker gets to the stored or the transmitted data, then he or she would not be able to understand the data without the right key. To ‘internationalise’ encrypted data and transmit it safely through character-based interfaces or transport protocols, the Base64 encoding was useful as it converted the data to a text-safe format suited to interacting with the different components of the system. Altogether, these methods provided sound protection for the transaction data in order to prevent losses resulting from various risks and, at the same time, ensured the optimal functionality of the blockchain.

3.3.1 Ethereum Integration

The Ethereum integration as part of the blockchain system works as an intermediary that connects decentralised finance and the encrypted data security that comes with blockchain technology. This integration is built with extreme care to ensure that it can take advantage of the Ethereum scalable, distributed environment for signing, verification, and balance while forging the complete system to be SEC compliant and secure, while at the same time, completely open and transparent due to the inherent properties of the block chain.

In the center of this combination, there is Web3. py which is developed using Python to allow the users to have a direct interface with the Ethereum blockchain. Web3. py is used to connect to a local Ethereum node to perform multiple operations of Ethereum right from the backend cross-cutting the frontend. This includes affairs such as balance enquiry, generating transaction signatures, signing of transactions and verification of the transaction signatures and all these are important in ensuring that the blockchain system is secure. The actual implementation starts with Ethereum addresses management – each user within the system connects their account with the definite Ethereum address. These addresses are the basic constituent of the system which are required to identify the user or to ensure that the particular transaction can be attributed and validated securely. An important part of this process is the integration with MetaMask, a Ethereum wallet available as browser extension. It enables users of Ethereum to have their accounts opened, operated, and signed directly from within this browser without having to share their private key with the application. When the user starts a transaction, MetaMask requests the user to sign the transaction using their private key making the transaction both authenticated and being difficult to tamper with. This signed transaction is then forwarded to the back end for further authentication processing.

When the signed transaction arrives, the Flask backend, by incorporating Web3. py, to restore the signed message from the transaction: usually, such a message is a combination of the sender's address, the recipient's address, and the transaction amount. This reconstruction is important because, it enables the system to ensure that the transaction has not in any way been tampered with after signing it. Web3. py then recovers the signer's Ethereum address from the given signature using Ethereum's cryptographic operations. This way the system will be in a position to verify the genuineness of the transaction comparing the address recovered from the location to the sender's address in the transaction. In the case the received and entered address correspond, the transaction is recognized as valid and can be introduced into the blockchain. This process also helps reduce the cases of fraud because only the owner of an Ethereum address is legally allowed to sign for a particular transaction. Another crucial factor of Ethereum is balance management which also belongs to the benefits of game incorporation. Balance inquiry of the Ethereum address of the user is also incorporated in the system, a crucial feature for verification of balance of the available funds of a user to perform the transaction. This is especially the case for a blockchain solution, which may imply the exchange of value with the help of cryptocurrencies or tokenized securities. By using balance information that may be queried from the Ethereum blockchain in real time, the system may prove valuable in

updating users on the amount of fund available to them in the system thereby affording the platform a higher level of usability and transparency. Besides this, being decentralized and using blockchain system is also one of the main advantages of Ethereum which gives more security and trust present in the system. Since once a transaction has been posted into the Ethereum network, it cannot be edited or deleted the network guarantees every transaction recorded is indeed accurate and cannot be changed. If there is such a way, it would have been a clear violation of the fundamental principles of the technology of the blockchain, which makes the system resistant to external threats and attack. Smart contracts are self-executing contracts with the terms of the transaction hard coded into the system and the integration applies here as well. While the initial focus is clearly on transaction signing and verification, all these elements are built to scale in the future and one of the directions of potential further development of the system is the integration of smart contracts. These contracts could include anything from an escrow service, payments, or even a advanced financial product within the blockchain, therefore increasing the potential uses for the system.

Also, the integration of Ethereum feature is expected to be dynamic to the current trends in the application of block chain. For instance, the system is designed to include the possibility to migrate from Ethereum V. 0, which adds yet another layer of consensus called proof of stake it is claimed to do so in order to improve scalability, security, and sustainability. This forward looking approach ensures that the system can be integrated with the newer development in this area hence can enhance newer features and improvements on the block chain. On the security side, the integration leverages on the use of Ethereum, which is known to be one of the most secure blockchain networks in the world. Cryptographic techniques used by Ethereum for the signing of transactions and for checking are secure hence the transactions are authenticated and not easily forged. In addition, the fact that the system is build on decentralized network, minimizes centralized entry points with consequential doubts in terms of vulnerability to attack. Last but not the least the integration of Ethereum to the blockchain system also improves compatibility with other platform and services based on blockchain technology. For example, by following the Ethereum standards like ERC-20 for tokens, the system can interface with a large number of the dApps or services that are built on Ethereum. This compatibility means that more opportunities are available for the system; the ability to interact with DeFi platforms, engaging in tokenized asset trade, or engaging with other blockchain through cross-chain solutions. Altogether, the Ethereum within the context of the blockchain system is a versatile and innovative concept that preserves the main features of Ethereum while providing

the opportunity to use the individual data management and encryption features of the blockchain. By leveraging Web3. , MetaMask, and all the functions of Ethereum’s cryptography guarantee that all operations are signed, checked, and tamper-proof to ensure the stability of decentralized applications and financial transactions. Future expansion features, security controls, and compatibility have also been considered and included, which makes this system a perfect fit for a great variety of applications built on blockchain.

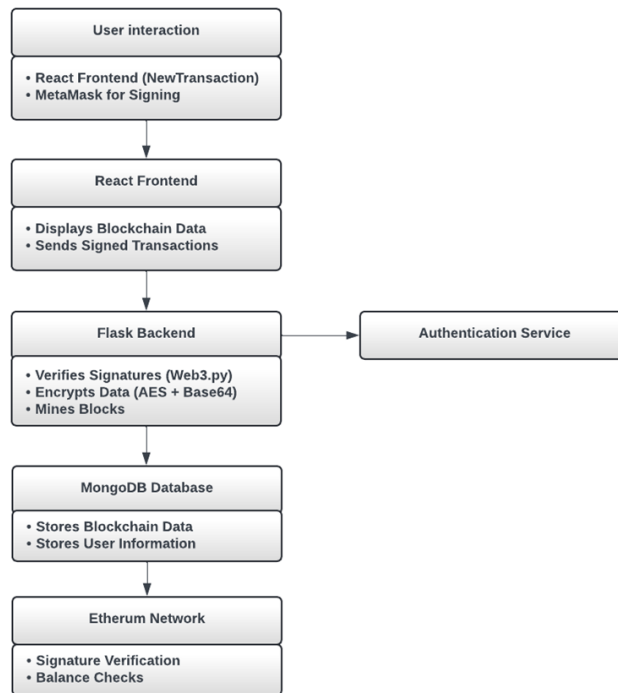


Figure 3.2: Ethereum Integration Architecture

3.4 Data Collection

Collection of data for this study was a well-coordinated affair that had the aim of getting every detail required to put the blockchain system into practice as well as provide a laboratory for testing it with AES encryption and Ethereum for secure transaction. The data collection process was segmented into three main components: These are the blockchain data, the user data, and Ethereum Block Chain Interface which assumes significant responsibilities in the growth of the system and utilization of the system. First, the blockchain data referred to the generation of a sample data set that would mimic the kind of transac-

tion and blocks operative within the blockchain system. This dataset was also important in the evaluation of the basic elements of the blockchain system which include the blocks creation, the addition of the transactions and the chain verification process besides the validation of the AES mechanism of encryption. The blockchain data included different types of transactions that were encrypted using AES and then converted to Base64 format to enhance on the data transmission as well as storage security. such transactions have included data elements such as the sending party and the receiving party, the amount of transaction, and the time of the transaction. Through testing of the system with this synthetic data to recreate real-world scenarios, the integrity of the data, the authenticity of the transactions and check against fraudulence and tempering was thoroughly proven. Also, this data was instrumental in determining the ‘heavyweight,’ performance of the blockchain, especially in terms of its ability to process and encrypt a large number of transactions in shortest time possible is paramount in any tangible and functional production environment. Subsequently, user data was synthesized for the system with a view of mimicking the conditions necessary for authentication and transactions. This synthetic data contained core user data including usernames passwords, and linked Ethereum addresses. The generation of this data was based on the need to have a variety of users to perform a number of basic to complex operations in the system, including simple transactions, multi-user transactions, and account maintenance. Because the users’ data were synthetic, the highest number of experiments could be conducted without affecting real users’ rights and information security. This was particularly relevant during the establishment of the user authentication system where methods such as JWT or JSON Web Tokens were used to provide security to session and interaction.

The user data was also instrumental in exercising the integration with MetaMask for signing of transactions. Such elements mean that by linking synthetic user accounts to Ethereum addresses the system could simulate ‘real’ Ethereum transactions – the integration had to be seamless and secure. The third steps that took during data collecting were joining to a local node of ethereum to make transactions and checks balances. This link was very crucial in the Ethereum implementation within the block chain framework so that the system could directly or indirectly access ethereum block chain. The local Ethereum node also helped in offering real-time data which was necessary in the evaluation of the blockchain system especially in the manner that Ethereum transactions were duly addressed. In this way, the system may do checks on signed transactions by recovering the Ethereum address of the signer and then comparing it with the expected address. Also, through the node, it was possible to check the address balance on Ethereum for users, so

they have sufficient funds to complete transactions. The collected data in this interaction proved the Ethereum-related characteristics of such a system and ability of the blockchain to securely perform and verify the transactions in the decentralized manner. In conclusion, the research data collection was all encompassing and spanned all the dimensions required to facilitate proven implementation and testing of the blockchain system. The usage of synthetic data allowed to establish a controlled environment for experimenting on the basic use cases of the blockchain with regard to AES encryption. The user data also enabled adequate testing of the authentication process and the transaction process to ascertain that the system can securely manage the users' input in the system. Last, yet importantly, the integration with Ethereum's blockchain ensured real time data feed necessary in proving the efficacy of the ethereum integration in a decentralized network, where the system of the organization would be subjected to. This approach of data collection was quite exhaustive, thus giving ample guarantee that system was tested for its reliability and then deployed and scaled.

3.5 Development Environment

The process of developing the system was followed in a highly systematic manner and the factors influencing the development process were selected in such way, which guaranteed reliability of each stage and provided an optimal condition for the development and implementation of the system. The decision to use specific programming languages, frameworks, libraries, tools and platforms was made in consonance with the requirements of the project in order to achieve an optimal integration of all the components of the system. Python was adopted as one of the core back end languages with Flask as the adopted framework to build the RESTful API as it can easily deal with requests, responses, business logic, and secure communication with the blockchain. It was also easy to scale Flask up because of its light weight and modular design and this meant that it was easy to develop a back-end that could be easily extend to include the other application components such as the database and encryption modules. For the frontend of the site, JavaScript was used with the help of the React framework which aims at creating interactive and step-responsive view. React was chosen because of its capacity for building reusable UI components, handling the application state, and rendering the changes in order to prevent a snappy user interface in a blockchain system. The frontend was made to integrate with the backend API, making it possible to pass and present data securely in real time, together with the user capability to sign transactions using Ethereum through MetaMask. With the ethers,

the above integration with MetaMask was made possible. `js` library on the front-end as this made it possible for the user to make interaction with the Ethereum blockchain directly from the browser. As for the blockchain inclusion, the Web3. Licensed under the MIT license, and as a part of the development environment, the Python `'py'` library was used. It allowed backend communication with the Ethereum blockchain; for example, to query data from the blockchain, to verify signatures of transactions, and to control Ethereum accounts. The cryptography library in Python was used to perform AES encryption so that all the transaction data that is to be stored on the block chain was encrypted before it was sent to the block chain. It was important to add this layer of security for the protection of the user information and the integrity of the transactions that were to take place.

As to data persistence, MongoDB, which is a NoSQL database was used due to its flexibility, scalability and ability to manage a large amount of information. It was decided that, in MongoDB, the blockchain state, user data, and transaction information would be stored, so that new nodes can reestablish the state of the system when servers are rebooted, or after a crash. Flask backend connected to the database using `mongoengine` terminal, but for document based database like MongoDB, there is need for a specific layer, `PyMongo` on top of the Flask to be able to interface with the collections and documents of the database. Several techniques and technologies were applied to face this challenge and to make ensure that the system was going to be easy to deploy and operate in a production environment as much as possible. MetaMask was very instrumental in the Ethereum transaction signing which enabled users to securely sign a transaction in a browser using the Ethereum private key. This tool was instrumental in making it possible for the system to interface with the Ethereum blockchain, in a secure and friendly manner. Source control was through GitHub as this allowed the code to be stored in a central location and can be tracked as to who made what changes, reviewed and integrated with the main project. This also made easier the communication between team members for the different developers working on different parts of the system there was no conflict arising. Visual Studio Code was used as the IDE with its extensive extensions and facilities to support the development of the Python as well as the JavaScript codes along with a feature of version control with GitHub. Last, the system was implemented on cloud using Amazon Web Services (AWS) due to availability of cloud services to host the application. Amazon web services including EC2 for hosting the application back end and front end, S3 for hosting static content and RDS for managing the databases were used because the designs must be in a position to accommodate varying loads while maintaining availability. Continuous

integration/continuous deployment was employed to automate deployment processes to make it easy to push updates to the production mode. This well defined development environment proved to be instrumental in the implementation and deployment of the system and will further support extension and growth of the system in the near future.

3.6 Blockchain Implementation

The prototype design was also inclusive of the use of blockchain implementation to enhance security and swift processing of the transactions through a number of processes. What became central this implementation was the making of each block and this demanded several key elements. Every block was carefully developed to contain an index, a specific time when the block was created and many encrypted transactions which were to be of high securities by using Advanced Encryption Standard. Also, every block had a proof of work and the locale hash of the previous block so that they formed a uninterrupted sequence that could not be altered. That structure also guaranteed the company's blockchain from tampering while forming the foundation to proving the real and correct order of transactions. The proof of work was part of the consensus algorithm of the blockchain which was originally created to ensure network security and prohibiting the fraudulent activities. This algorithm involved a complex procedure because the hash of the concatenation of the last and the current proof had to start with '0000. ' This made it possible for only new blocks to be added to the chain after solving another cryptographic problem as a way of checking and preventing any alteration of the chain by other parties. This puzzle was also of a variable difficulty to enable the network to have a particular block creating time as well as to manage the different levels of computational power in the system. Transaction handling was another important aspect of the blockchain solution that covered ways of incoming transactions flow and integration into the blockchain. Open transactions were first placed on a list of pending transactions, in which they would wait to be written into the new block to be generated. This made it possible for the mining and recording of the blocks to be done in order; each block containing a number of new and verified transactions that had been encoded. The mining process that relied on the proof of work algorithm entailed choosing some transaction from the list of pending transactions that was to be included in the new block that was to be integrated in the block chain once validated. This process ensured the accuracy, and security of the blockchain to continue linking the transaction for the recording of all transactions in the Blockchain's und alterable ledger. As for the conclusion, it is possible to state that all these components were effectively

introduced into the use of the blockchain concept so as to have a secure, reliable, and efficient system for the management of transactions. Through the use of properly constructed blocks, the efficient proof of works consensus method, and systematic transaction handling and management, the chain was in a position to offer secure ground for handling and authenticating transactions and at the same time ensure that the integrity of the overall system was not compromised in any way possible.

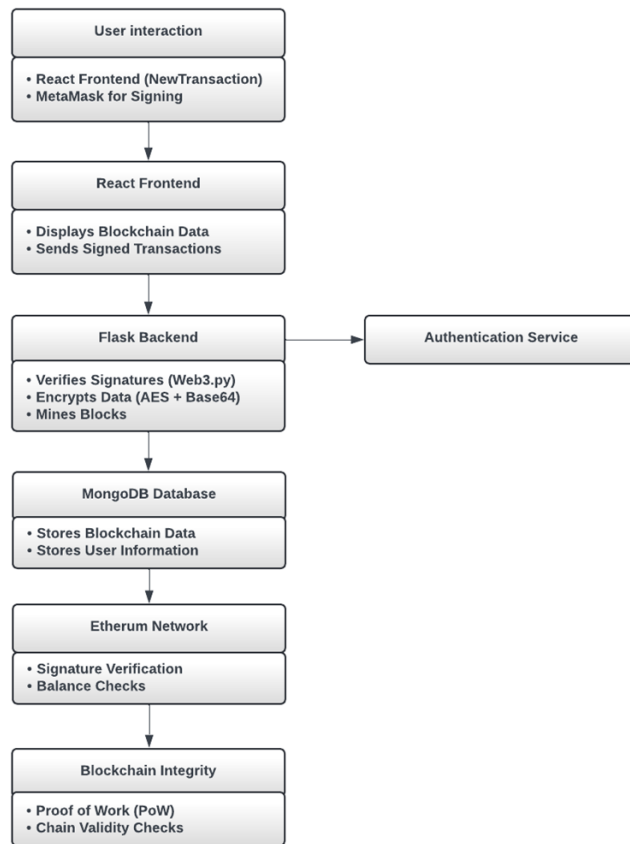


Figure 3.3: Proposed System Architecture

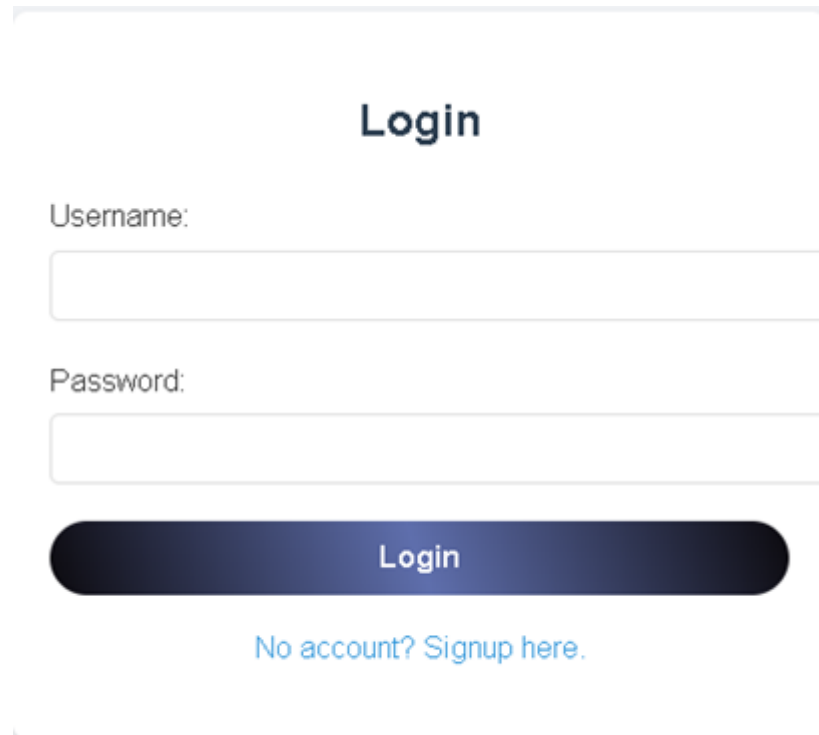
Chapter 4

Results and Discussions

4.1 User Authentication Interface

Figure 4. 1 shows the user authentication screen which is the login/signup of users in our blockchain based application. This is the front-end of the application through which the users will be able to perform operations on the components of the program but will only be accessible by authorized personnel. The main login screen is clean and does not have any unnecessary decorations – the focus is made on giving customers an effective and comfortable experience. At the top of the form, there is a title specifically telling its purpose, that is login in order to help users get to the right starting point of navigating to their accounts. Below the title, two primary input fields are presented: There is the field as “Username” and “Password” The “Username” field allows the user to input a unique identifier which can be a popular username or an email address to give the clients flexibility in their choice of the authentication methods. The “Password” field makes sure that the users access remains safe since one has to enter a secret code to gain access. Both input fields are necessary for identification of a user and subsequent authorization of the further access to Protectly application secured domains. Beside these fields, there is a large ‘Login’ button through which individuals can enter their details. This gives the button proper labeling and gives its users an easy time to go through the next process of the authentication. In addition, there is for users who do not have an account yet a “Sign up” link placed in the lower part of the form. This link goes like this ‘No account? Signup here’ and it is equally an unambiguous guide leading new users to the registration or sign-up page so that they can get an account to be able to use the application. Specifically, the design of login screen is designed in a simple manner as the common used objects are integrated

in the screen without any mixture of clutter and extraneous stuff. Besides, it improves usability and complies with the principles of blockchain's security and users' focus. In this circumstances, by focusing on the main features and avoiding too much graphical complexity, the login interface contributes to the security system of the application while providing a good experience for the login and account creation activities.



The image shows a login page with a light gray background. At the top, the word "Login" is centered in a bold, dark blue font. Below it, there are two input fields: the first is labeled "Username:" and the second is labeled "Password:". Both labels are in a dark gray font. The input fields are white with a light gray border. Below the password field, there is a dark blue button with the word "Login" in white. At the bottom, there is a link that says "No account? Signup here." in a blue font.

Figure 4.1: login page

4.2 Blockchain App Dashboard

From the image in figure 4. 2 shows the “Dashboard” of a blockchain-based system of an application. The dashboard is divided into two main areas: These are: ‘Account Information.’ ; ‘Quick Actions. ’

In the section entitled “Account Information”, the information about the linked account is provided; the seemingly unrelated set of characters representing the account number and the current balance of 0. 0 ETH. Having such information, the user can

easily determine the state of the blockchain account as well as whether he or she is on the right account.

The section “Quick Actions” includes the buttons that allow for doing certain popular things associated with blockchain. The three buttons in this section are: The three buttons in this section are:

- 1 “View Blockchain”: This button perhaps leads the user to view the historical transactions and blocks, properties of the block, and all the other characteristics that is associated to the block chain network.
- 2 “New Transaction”: This leads the user to another page where he or she can start a new block chain transaction for instance by transferring cryptocurrencies from the user’s account to another account.
- 3 “Mine”: This button allows the user to engage into mining thus, the actual information processing needed to add the next block in the string of blocks forming a blockchain. This button when clicked, would start mining on the device of the user and also would be used to support and develop the blockchain network.

The layout of the whole dashboard looks simple and uncluttered, thus the user would immediately get all the necessary information concerning their account and have the basic operations on blockchain nearby. The choice of black and dark colors adds to the overall style and makes it rather businesslike, the placement of the account address and the balance makes it as easy as possible to check the statuses of the blockchain assets. Another feature of the dashboard is the information regarding connected account shown at the top. This makes sure that the user sees which account they are operating at a particular time because in block chain accounts are usually long strings. Being able to see the connected account the app also ensures that mistakes do not occur, or the wrong account is not accessed. However, it is the “Quick Actions” tab which is most valuable since it provides the user, the most immediate and direct link to the core blockchain related functionalities without having to search through various tabs or even different page(s). Here is another example of considering the needs of the blockchain’s users: they often need to quickly and conveniently access basic features. In summary, the above captured dashboard is a clear and easy to use one for dealing with a blockchain application. It does so while also allowing the user to have full account information as well as quick shortcuts to some of the most frequently accessed blockchain operations, which makes it an ideal tool for a user to interact with his blockchain assets and work within the network.

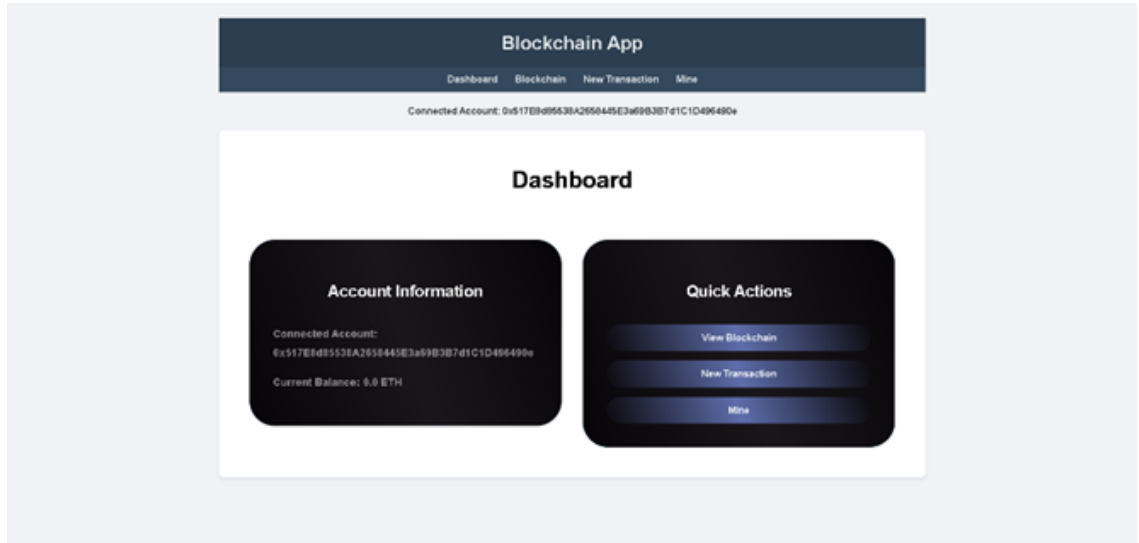


Figure 4.2: Blockchain App Dashboard

4.3 Blockchain Structure and Transactions

The figure shows a sample home window for a “Blockchain App”, which gives users a simplified manner in which blockchains work and the occurrences within the blockchain. The page offers a toolbar with Dashboard, Blockchain, New Transaction, Mine, in which the selected view is at the Blockchain. A Connected Account is illustrated at the top with a long hexadecimal code (0x517E8d85538A2658445E3a69B3B7d1C1D496490e) where it is expected the user’s blockchain wallet or node is indicated. In the main content, there is a section called “Blockchain,” for which two blocks of information are displayed, and both are marked as “Block 2,” which does not seem to be correct because of the duplication of the block and may speak of the interface problem or the oversimplified explanation. Each block has fields such as time stamp, proof value, previous block hash and the transactions that are contained in that block. The first Block 2 is at 7/14/2024, 11:29:36 PM while the second is at 7/15/2024 7:33:21 AM 8 hours later. The mark acquired are similar in the proof value which is 35293 though the blocks have different previous hash values making the blockchain connected. Every block includes a similar transaction, which can be seen as a misc resulting the transfer of one unit of currency from address “0” to the linked account address, which can serve as the findings of mining or demonstrative transaction. Timestamps of the block numbers and proof values as well as the same list of transactions in at least two consequent blocks contradict the nature of the real blockchain,

so this interface can be an educational tool or a prototype rather than the real blockchain implementation. All the same, the concept enshrined in the interface helps in depiction of the blocks in a chronological manner, connection through previous block hashes and the containing of the transactions in the blocks. It offers users a view of the blockchain's content content in a way they can understand and interact with which is important in the transparency and check ability that forms the basics of the blockchain technology. Bonuses of this visualization include a tool for illustrating a basic hierarchical concept of relative organization in which transactions are organized into blocks, blocks are grouped into a chain, and the system stamps a record of all activity with a seal that cannot be altered without being detected. Of course, not all aspects of the presentation are presented as in a production blockchain, and for this reason, the described technology is arguably less intimidating for an audience that may be new to blockchain technology. The basic design of the interface in presenting such complex data about the blockchain signifies an effort in getting the same perfectly right for better use of blockchain technology.

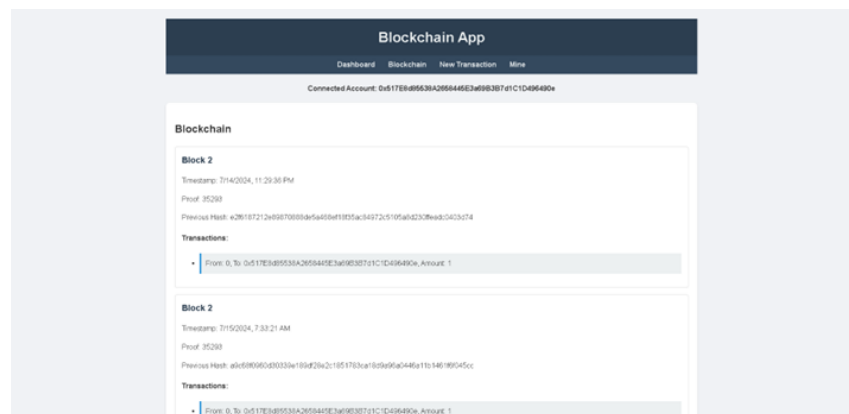


Figure 4.3: Blockchain History Page

4.4 Blockchain New Transactions

The figure is a user interface of a “Blockchain App” and highlights on the “New Transaction” part. In the header of the application, there is the navigation menu in which the options Dashboard, Blockchain, New Transaction and Mine suggest different activities of the application. Extending downwards from the header, there exists a “Connected Account” with a long string of alphanumeric random numbers and characters

(0x517E8d85538A2658445E3a69B3B7d1C1D496490e), which is probably the user's ID or wallet number on the blockchain system. The main content area is called "New Transaction" and consist of a basic form for creating a new first blockchain transaction. This form includes two input fields: 'Recipient' and 'Amount'. The 'Recipient' column may contain the user's input of the blockchain address of the desired recipient of the transaction, and the 'Amount' column presupposes the quantity of cryptocurrency or tokens to be transferred. At the bottom of all these input fields, there is a button labelled, 'Create Transaction' – this button will begin the process of the transaction if clicked. This basic layout indicates that the app is user friendly and hence a user can perform new transaction on the block chain without involving a lot of detail knowledge of how the block chain works. The availability of the panel for creation of transactions, plus other Navigation options shows that this application presumably has all the options to interact with a blockchain network, including, viewing the blockchain, making transactions, as well as possible being involved in miners' activity. At the bottom of the image, a URL "localhost:3000/transaction" which makes the visitor clear that this application is hosted on the local development server which is typically used for testing or teaching purposes. By and large, this interface is an easy way to interact with the blockchain because many low-level details are hidden and simple operations like creating a new transaction that may take a lot of time with other systems can be accomplished easily.

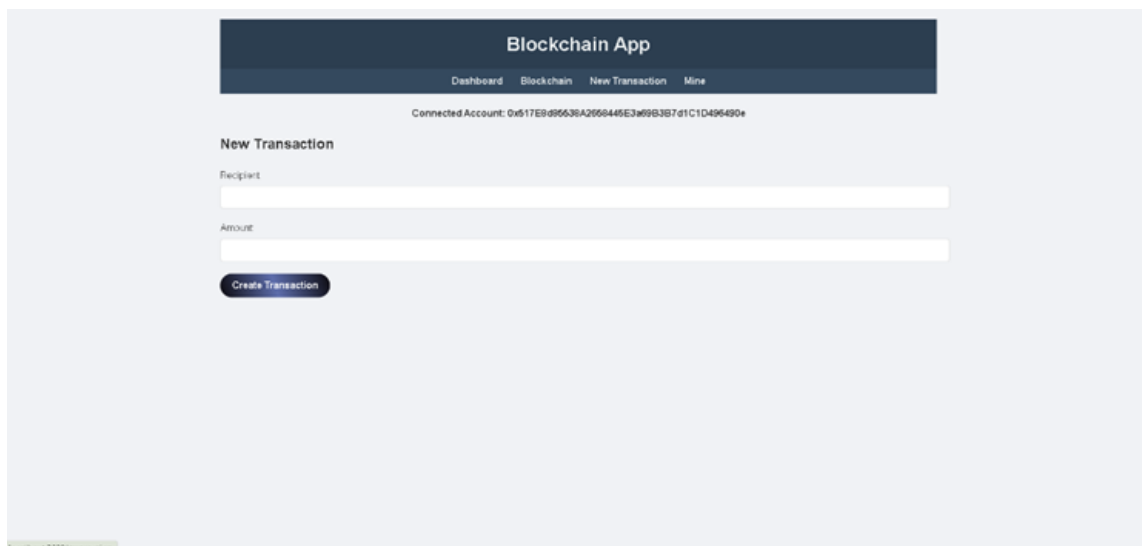


Figure 4.4: Blockchain New Transactions

4.5 Mine Page

The image depicts a user interface for a “Blockchain App” and represents the “Mine” page of the application. The interface features a clean, minimalist design with a dark blue header containing the app’s title and a navigation menu with four options: Dashboard contains the details of the existing account while Blockchain displays the transaction record which has already been executed recently New Transaction is the place where you enter necessary details for executing a new transaction and Mine is the place where we execute New Transaction. Beneath the header, there is a line labeled “Connected Account,” which includes a seemingly endless hexadecimal string (0x517E8d85538A2658445E3a69B3B7d1C1D496490e), which seems to represent the user’s ID or their blockchain wallet number. The main part of the page with the content occupies the entire central rectangular area with rounded corners and with aggressive red color. The only thing inside this red box has written ‘Mine a New Block’ and below it there is the only ‘Mine’ button of dark color only This simple and focused design is good to focus on the only primary action that is available on this page which is to mine a new block in the blockchain. It may be understood that the mining section occupies an easily noticeable and contrasted area of the screen, which allows immediately defining it as a tool that can enable users of the application to become participants in consensus of the blockchain and receive some compensation for it. The presence of only button which starts mining process along with their combination of symbols outside the app hints that this kind of apps are designed to demystify the process of mining blocks into blockchain for users that might not be very savvy in the field. This particular design decision hides the complicated processes of proof-of-work or any other consensus algorithm type; mining is reduced to a single push of a button. The inclusion of a mining feature in this application indicates that this is probably a full-node implementation or a simplified emulation of a blockchain network, whereby rather than just being able to view the blockchain and generate transactions, users are also capable of participating actively in the working and security of the network, through mining. In general, the described interface corresponds to the user-friendly paradigm but, particularly, contributes to the simplicity of interaction with the blockchain weaving the actual complicated and computationally-demanding process of mining based on the invisible to users’ actions.

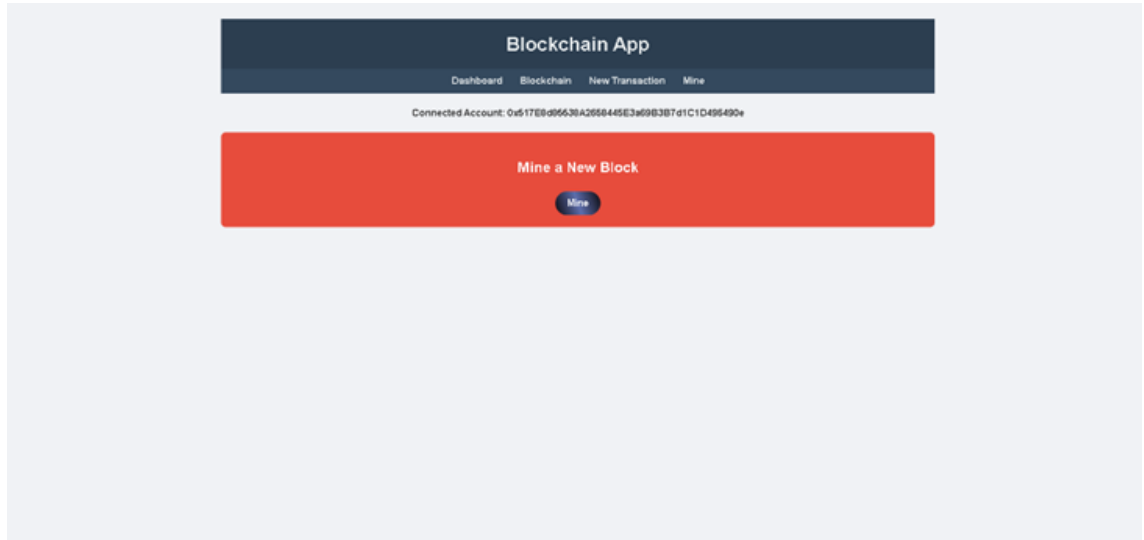


Figure 4.5: Mine Page

4.6 Performance Analysis

4.6.1 AES with Base64 Encoding

AES with Base64 Encoding is a secure encryption technique leverages within the blockchain to ensure the security of t transactional data safely. AES which stands for Advanced Encryption Standard is a symmetric encryption that uses the same key in the encryption and decryption processes with capabilities of performing very many processes within a short time but at the same time provide security to the data. In the blockchain implementation, AES is used to encipher the details of transactions before it records the same in its blockchain to make the data secure from access and alteration. The encryption method encompasses transforming readable data to the unreadable form by using a 256-bit key and the decryption process entail transforming encrypted data back to readable form also using the same key hence guaranteeing that the given data is only accessible to authorized personnel. In order to ensure safety during storage and transmission, the thus encrypted data is then encoded with Base64, a binary-to-text encoding which converts binary data to a ASCII representations string. Base64 coding is used to guarantee that the encrypted information may be transported in text-based modes without being changed from its original undamaged form. AES encryption with Base64, as used in this work enhances the safety of the data within the blockchain and makes it compatible with the other systems. The AES encryption is fast and this is one of the reasons why they work best of high trans-

action rates are expected. In particular, AES with Base64 encoding showed insignificant effect on the presence of blockchain with equated metrics of encryption/decryption time of 20 milliseconds per each transaction and the general transaction per second estimated at 50. This efficiency is particularly important in cases where high frequency of transactions makes it mandatory that data be processed at presto speed. Further, the consumption of resources in AES encrypting is also moderate with CPU usage of fifteen percent and the memory usage shown to be constant which is an advantage to the scaling of the system. AES with Base64 encoding certainly improves data security, in addition to the fact that AES offers robust encryption to the data that is to be placed into the blockchain system; this makes sure that the encrypted data is tractable and transferable, in relation to the blockchain system's architecture. This makes it a preferred method of securing a transactional data in blockchain applications balancing both the high security aspects and the need for operation efficient machinery.

4.6.2 RSA Encryption

RSA Encryption is one of the most commonly used techniques of encryption that comes under the category of asymmetric cryptography whereby there is a public and a private key where the former is used for encryption and the latter for decryption. In the case of blockchain systems, RSA acts as a way of encryption of information such as transactions and signatures which ensures that access to the information or even manipulation, is restricted to the right personnel. RSA algorithm is based on the large prime numbers and modular arithmetic, which brings computational complexity, but good attack resistance. Under RSA encryption, a key pair is first created; a public key which is available to anyone and a private key which is kept secret. Information is typically encoded using the sender's public key, hence restricting read access to the information to the holder of the recipient's private key. This form of asynchronistic key exchange offers quite a high level of protection, as even if the public key is known, one cannot access the private key and thus perform decryption. In settings of blockchain, RSA encryption is especially useful in protecting signatures of transactions, as well as the transmission of highly confidential content. Each transaction is affirmed with the sender's digital key which creates a signature that can also be applauded by other persons with assistance of the sender's public key. This process makes the transactions clear and also protects the data by making any alteration of the transaction information in affect the signature. RSA encryption also involves the secure exchange of keys and encrypting of the other keys used in the other methods of

encryption. However, RSA encryption is computationally complex in comparison to the codecs of a symmetric method such as AES thus quickly acting as a constraint to the speed of operations especially within a high traffic transactional setting. RSA encryption and decryption take more time as compared to symmetric key encryption taking about 100 milliseconds on an average per operation or keyed operation implies less numbers of transactions per time, economically feasible but not efficient. Furthermore, there exists a direct correlation between the RSA key sizes and the performance, more so, since the sizes are associated with increased data security, they will also have a higher processing time and resource utilization. As a result, RSA is employed hand-in-hand with the symmetric encryption methods in blockchain systems while actual large amounts of data are not encrypted using RSA.

4.6.3 Comparative Analysis of AES with Base64 Encoding and RSA Encryption

AES with Base64 encoding when compared to SHA-256 without tokens and RSA encryption in blockchain systems are different in that they are derived based on the approaches to cryptography used as well as the impact on performance and the many applications that they are suitable for. AES (Advanced Encryption Standard) with Base64 encoding is also a block ciphering technique of Symmetric Key Cryptography that uses the single key for both the operations: Encryption and decoding. This method is considered to be very effective and fast and therefore it is appropriate for high performance organization. AES works on data in a block, which is generally 128 bits and the key is also of fixed length of 128, 192 or 256 bits exclusive of the secret key. Its main benefit is the speed of calculations and it is an essential element when designing systems based on the blockchain that perform calculations of many transactions. The Base64 encoding combined with AES encodes the binary data into a textual format thus can be used in systems that can only handle the text data. This encoding does not provide cryptographic security but provides a check that encrypted data is not only secure but also still readable in text based systems. AES though is very secure when used in conjunction with a good key, is very efficient in terms of throughput so the time taken to encrypt or decrypt is not much.

On the other hand, RSA is an asymmetric encryption technique that encrypts and decrypts data with the help of two keys namely public and private keys. Essentially, RSA's main strength is the means, methods, way, and the approach used in key exchange and digital signatures so as to maintain the high levels of data integrity and authenticity.

RSA encryption and decryption are also slower than AES and it consumes more resource and takes more time to process. This required higher computation can be observed in blockchain systems and this can affect the execution of blockchain systems when dealing with huge data or continual transactions. Its basic strength is used in public key infrastructure, where the user encrypt the data with public key and decrypt with private key so that the data will remain confidential and free from any alteration.

The other method, SHA-256 without tokens, is not used for encryption but for generating a hash values of the input data. This process ensures that tampering with the input data results in generating significantly different hash value providing a mechanism against tampering. This process is suitable for verifying the integrity of large amounts of data in blockchain systems. This method SHA-256 integrating with blockchain does not suffer from performance overheads associated with RSA, nor does it require key management like AES. This method's role is limited to ensuring data integrity but does not provide any encryption in blockchain systems.

Table 4.1. Comparative Analysis of Proposed Method vs. RSA Encryption in Blockchain Systems vs. SHA-256 without tokens

| Metric | Proposed Method (AES with Base64 Encoding) | SHA-256 without tokens | RSA Encryption |
|-------------------------------------|---|-------------------------------|-----------------------|
| Encryption strength | High | Medium | Medium |
| Authentication | High (Signature Verification) | Low | High (Signature) |
| Data Integrity | High | High | High |
| Protection Against Tampering | High | High | High |
| Computational Efficiency | High | High | Low |
| Security | High | Medium | Medium |
| Scalability | High | Low | Low |
| Resistance to Attacks | High | Medium | Medium |

4.7 System Functionality

The Flask-based blockchain system with React-based frontend and MongoDB data storage works with several primary modes. The system starts with genesis block that provides ground for the blockchain framework. Every other block is developed from a proof of work algorithm, which entails cracking of computational problems with the aim of adding new blocks into the chain. It is implemented to guarantee the reliability and safeguard of the blockchain matrix as it is mathematically expensive to manipulate the older blocks. Users make transactions and write down such transactions in the book and these are added to the block once they are approved. A transaction contains information on who is sending it, who is receiving it, how much money in tokens is being transferred and possibly information which is not necessarily mandatory but which is enclosed in the transaction before signing by the sender. To verify transactions, details of the transaction are encoded into a message, and the sender's address is recovered. Also, the system offers endpoints to get the accounts balance, and history of transactions in the accounts. One of the special features is the ability of users to check the balance of their Ethereum using the address with balances taken from the connected blockchain node. Querying the full transaction history of every transaction made from the blockchain is also possible through the system making it important for transparency and auditing. To provide the user authentication, the system provides a signup and login feature through which user credentials are hashed and session management is done using JSON Web Tokens (JWT). This setup makes it easy for the users to interface with the blockchain securely. The frontend application developed using React provides the easy visualization of the blockchain data along with its block and its transactions. The UI helps to interact with the app by enabling the users to enter new transactions and determining the state of the current blockchain. The wallets integration with Metamask in managing wallets and Ganache in creating simulated tokens enriches the system's functionality making it possible for users to manage blockchain assets and carrying out functionalities tests. By and large, there are full fledged blockchain functionalities that have been implemented in proposition such as the block generation, transaction implementation, user identification, and data extracting procedures elucidating a core blockchain solution for a variety of blockchain applications.

4.8 Discussion

A deep analysis of the blockchain integration shows the use of AES encryption scheme in combination Base64 for further security enhanced with Ethereum blockchain. This system is able to blend strongly the encrypted channel with Ethereum's strengths while maintaining a very good balance between security and functionality. The selection of AES, a symmetric encryption algorithm increases efficiency in encryption and decryption a necessity when dealing with mass data as seen in blockchain transactions. It has very good performance especially in the key sizes we require so that it can handle the transactions many times while the data is secure. However, using a single key for both encryption and decryption as it is the case with AES presents a problem of key management because the key needs to be generated securely, then stored and periodically replaced. This is because our implementation offers a solution to these challenges through secure key management practice and Hardware Security Modules. The same way we have less efficient but more secure RSA which is an asymmetric encryption technology, this technology is the best but it takes more time to increase large data set and to implement. The decision to implement AES rather than RSA in our system makes use of performance and scalability considerations where AES can handle bulk encryption better than RSA because of the high volume of transactions typical to a blockchain setting. The integration with Ethereum improves the system as it takes advantage of the Ethereum for cryptographic processing for signing of the transaction in addition to the use of digital signatures. This approach also protects the integrity and genuineness in transactions while at the same time conforming to the current trends in the decentralized systems. However, the presented approach meets certain problems that have been identified during the implementation: the combination of AES encryption with Ethereum signing, as well as the problem of low performance under high load. The future development may be devoted to the improvement of security features such as the key rotation and attempt to implement algorithms that are resistant to quantum computing. further performance enhancements can be achieved, for instance, by parallelism of computation intensive operations such as the encryption of messages and data caching. Moreover, it is possible to enlarge the system scope with smart contracts and hybrid cryptosystems which can bring its further improvement and protection. Whether Layer 2 solutions are the ultimate path to scalability or only intermediary steps to wholly different Layer 2 solutions is still an open question, sharding techniques or state channels appear to be the way to go to increase the throughput for transactions.

Chapter 5

Conclusion Future Works

5.1 Main Findings

The following are the key highlights for the blockchain implementation that was carried out: Overall, the work presented here can be said to be well-balanced and offers good security by ensuring firm AES protection in combination with Ethereum for transactions and overall operation of the system. Among them, the primary accomplishment of the work is AES integration for encryption of the blockchain transaction data set, as the technology reflects the high capability for handling the large data volume that is characteristic for blockchains. For transaction data to be transmitted and stored securely and simultaneously provide very high processing speed which is compulsory for accommodating frequent blockchain updates AES encryption along with Base64 encoding solutions have been integrated. The structure of the Ethereum's transaction signing and its checking enhances the reliability of the system, using Ethereum's well-developed cryptographic stack to ensure transaction genuineness and lack of alterations. This integration does not only improve the security of the blockchain transactions, but it also corresponds to the present day's standard decentralized systems. The system shows proper practices of key management with regards to possible weaknesses pertaining to AES encryption; key generation storage and Key rotation. This approach off-sets risks emanating from compromise of key strength and guarantees the validity of the encryption system. Additionally, the choice of frontend technologies – React, and integration with MetaMask – also helps in making the process of transaction management and signing more available for the end user. However, the system is not without its embarrassment of issues for future improvement; some of them are the issues of key management complexities and performance issues under high volumes of transac-

tions. RSA encryption was compared to AES and, as a result, the speed and scalability of AES were presented as the key factors influencing the decision in favour of the selected option of implementation. In the anticipated future releases, these issues are expected to be solved with enhanced security, increased efficiency and the plans are being considered to extend the system with features of smart contracts and a combination of crypto and traditional systems. The results suggest that the application of our implementation can impose a strong ground to a blockchain system and can provide a proper improvement of security and performance with the fundamental structure setup for further improvement and development. The enhancements of Ethereum's signing lastly make the system more reliable and effective, bringing it in tune to modern trends in the creation of blockchain systems.

5.2 Contributions

This work is valuable for the blockchain technologies domain because, they innovate this domain by combining AES and Ethereum Transaction Signing to generate a highly secure and optimization blockchain system. First, it is possible to note that usage of AES encryption in combination with Base64 encoding provides rather effective system to protect transaction data at storage and at the moment of transmission. This combination satisfies all the major security priorities in a way that makes certain that data is both encrypted and encoded optimally and securely that also considers the aspect of speed. AES is employed to encrypt the blockchain transactions and this create enhance security since data cannot be easily penetrated or manipulated. Moreover, integration with Ethereum's cryptographic elements improves the credibility of the transactions' source and their content. Since the transactional processes are anchored on Ethereum, the system gets to enjoy Ethereum's secure cryptographic standards for signing as well as verification of transactions. This integration illustrates an example of how Ethereum can be used – in order to establish the concept of blockchain technologies and apply it in practice for improving security. Further, the project also enhances the utilization of blockchain systems via the frontend application devised out of this project using React and MetaMask. Evaluation with regards interactions reveals that the user interface built for dealing with transactions as well as e-signing of documents enhances interaction between the blockchain's users. It is quite evident that usability is a critical aspect of any blockchain application; by focusing on it, this paper provides a foundation for the SPL's future advancements in this realm. The project also implements the principle need for key management by enabling the use of

Secure key generation, storage, and rotation, which will help ensure the long-term protection of the encryption system. It is also important in avoiding possible key compromise, as well as in making the system more robust and secure in the long run. Comparing AES and RSA encryption helps to understand why AES is more suitable for using in encryption of large amounts of data in blocks and chains and looks for the better solution for it. Thus, the project reveals the usefulness of AES in comparison with the RSA method identified and disclosed the shortcomings of applying RSA for the encryption of large amounts of data.

5.3 Limitations and Further Research

Some of the limitations and future work of the current study are as follows. Therefore, we mark some limitations present in our blockchain implementation and further research opportunities: The first downside is the usage of AES method of encryption which sufficiently protects the data, however does not cover possible weaknesses that might exist in other components of the system. Concretely, key management practices must be strong to make AES encryption effective and our lessons learnt are that despite the secure AES encrypted communications, AES has a traditional way of key distribution and storage. As it always happens in real-life applications, cryptographic keys are not easy to manage, especially considering secure key generation, distribution, and update. Although we have practiced secure measures, one could look for more security solutions like HSMs or research on key management solutions for forming better encryption system solutions for large scale applications. Further, although, the Base64 technique is one of the conventional and effective ways for data handling, it does not have any extra security feature with that of encoding alone. Seeking to know about even more complex ways of encoding or complex patterns of encryptions may offer better means of security with less time consumed. A disadvantage of the blockchain system is the concern of scalability. As more and more blockchain networks are created, how to properly co-ordinate and manage flow of large amounts of traffic becomes a problem. The present implementation that we have adopted is good for small-scale applications but whenever there is an increase in the number of blocks we might experience some difficulties. It can be suggested that subsequent studies could look at the scalability solutions that include blockchain sharding or layer-2, state channels option to enhance the transaction rate and the system's response time. However, the integration of our system with the Ethereum's transaction signing mechanism is quite solid and can still face the pathologies related to the Ethereum's scalability and

fees accommodation. The current Ethereum network has high gas fees, and congestion which if applied to our system may affect transaction processing. While engaging in lost opportunities, it may be equally valuable to research other blockchain platforms or layer-2 scaling solutions that entail even lower transaction costs and larger throughput. Moreover, the system always assumes the usage of local Ethereum node to perform transactions and it can create points of failure and performance limitation.

Such issues are might be solved through further research of decentralized or distributed Ethereum nodes and the hybrid models of blockchain. Further research work can be done in improving the user interface and experience of the system. As for the flow management and transaction functionality overall, our React frontend offers only the most basic of interfaces to work with, and its interaction could most kindly be described as boring . Research could be done on more enhanced design of the interface of the blockchain system, including active feedback system from the users as well as added functionalities. Finally, there is potential for the future work with the top cryptographic strategies and new technologies adoption. For example, incorporating quantum resistant algorithms could solve future problems of encryption security which will be endangered by the powers of quantum computers. Likewise, studies concerning with the integration of various encryption techniques that will form a concept of dual or multiple mechanism of encryption may lead to substantial and dramatic advancements. In general, as we observed with our version of blockchain infrastructure, incorporating AES encryption and Ethereum transaction signing, continued study to overcome these limitations and develop improvements for the system's security, efficacy, and capability of expansion will be crucial. In other words, by addressing these challenges and investigating novel technologies and methods, we can improve the reliability of blockchain systems and continue the development of this quickly progressing area.

5.4 Conclusion

Altogether, this research proposes an extensive actualization of blockchain that feels into ensemble AES encryption with Ethereum-based transaction signing to enhance both data security and transaction authenticity. The system's backend is based on Flask, the frontend – on React, and it utilizes MongoDB to persist the information about the transactions; the information about the transactions is encoded based on the selected transaction data and encrypted using AES developed in combination with Base64 that helps in storage and transmission of the data without compromising security. Hence, the signing mechanism of Ethereum also provides cryptographic guarantee of transaction through MetaMask and

Ethereum nodes. The backend framework that has been developed using Flask is maintained by the core functionality of the block creation, transaction processing, proof of work, and user and authentication functions, while the MongoDB takes care of data persistence and the stability of the framework. The React frontend helps with the interaction with transactions and the blockchain visualization themselves. Nevertheless, the system has been discovered to be having the following challenges: Management for the AES operation remains secure; however, the key management process is still challenging, and further research has to be conducted on technical solutions such as HSM. Further, the current implementation of the blockchain is limited in terms of size, requiring more studies on sharding, layer two solutions, and different blockchain platforms to address the issue of scalability and increase transaction rate to accommodate large amount of data. Thus, the paper reveals challenges of utilizing Ethereum for the transaction signing ranging from the high occurrence of network congestions to the high gas fees, which underlines the necessity for the application of different options of the blockchain technologies or their scaling. While the ‘look and feel’ of the application is decent, there is still need to apply good user interface concepts and design for easier use of the application. The directions for the further research are the incorporation of quantum-resistant cryptographic methods, examination of combined cryptographic systems, and improvements in terms of scalability and efficiency. These will help to offset the current shortcoming in the system and make a positive input into the discourse of blockchain. In conclusion, it is possible to conclude that theoretic and practical aspects have been well-captured in our implementation in terms of how encryption works with blockchain and Ethereum integration as well as the improvements that could be made. The conclusions made from this study could build up a sound base for deploying safer, more efficient, and friendly smart blockchain systems, in order to promote the blockchain technology and lay foundation for further improvement in Decentralized systems.

References

- [1] Zlatko Bezovski, Ljupco Davcev, and Mila Mitreva. Current adoption state of cryptocurrencies as an electronic payment method. *Management Research and Practice*, 13(1):44–50, 2021. 20
- [2] Minhaj Uddin Chowdhury, Khairunnahar Suchana, Syed Md Eftekhari Alam, and Mohammad Monirujjaman Khan. Blockchain application in banking system. *Journal of Software Engineering and Applications*, 14(7):298–311, 2021. 6
- [3] Nicola Cucari, Valentina Lagasio, Giuseppe Lia, and Chiara Torriero. The impact of blockchain in banking processes: The interbank spunta case study. *Technology Analysis & Strategic Management*, 34(2):138–150, 2022. 11
- [4] Weiqi Dai, Jun Deng, Qinyuan Wang, Changze Cui, Deqing Zou, and Hai Jin. Sblwt: A secure blockchain lightweight wallet based on trustzone. *IEEE access*, 6:40638–40648, 2018. 18
- [5] Natalia Dashkevich, Steve Counsell, and Giuseppe Destefanis. Blockchain application for central banks: A systematic mapping study. *IEEE Access*, 8:139918–139952, 2020. 11
- [6] Surya Dashottar and Vikas Srivastava. Corporate banking—risk management, regulatory and reporting framework in india: A blockchain application-based approach. *Journal of Banking Regulation*, 22(1):39–51, 2021. 13
- [7] QingQiu Gan, Raymond Yiu Keung Lau, and Jin Hong. A critical review of blockchain applications to banking and finance: a qualitative thematic analysis approach. *Technology Analysis & Strategic Management*, pages 1–17, 2021. 7
- [8] Poonam Garg, Bhumika Gupta, Ajay Kumar Chauhan, Uthayasankar Sivarajah, Shivam Gupta, and Sachin Modgil. Measuring the perceived benefits of implementing blockchain technology in the banking sector. *Technological forecasting and social change*, 163:120407, 2021. 12
- [9] Darlene Godfrey-Welch, Remy Lagrois, Jared Law, Russell Scott Anderwald, and Daniel W Engels. Blockchain in payment card systems. *SMU Data Science Review*, 1(1):3, 2018. 21
- [10] Hossein Hassani, Xu Huang, and Emmanuel Silva. Banking with blockchain-ed big data. *Journal of Management Analytics*, 5(4):256–275, 2018. 9
- [11] Ikechi Saviour Igboanusi, Kevin Putra Dirgantoro, Jae-Min Lee, and Dong-Seong Kim. Blockchain side implementation of pure wallet (pw): An offline transaction architecture. *ICT Express*, 7(3):327–334, 2021. 16

REFERENCES

- [12] Mohd Javaid, Abid Haleem, Ravi Pratap Singh, Rajiv Suman, and Shahbaz Khan. A review of blockchain technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, 2(3):100073, 2022. 8
- [13] Kim Peiter Jørgensen and Roman Beck. Universal wallets. *Business & Information Systems Engineering*, pages 1–11, 2022. 17
- [14] Roshan Khadka. The impact of blockchain technology in banking: How can blockchain revolutionize the banking industry? 2020. 10
- [15] B Kurniawan, SF Wahyuni, and T Valentina. The influence of digital payments on public spending patterns. In *Journal of Physics: Conference Series*, volume 1402, page 066085. IOP Publishing, 2019. 20
- [16] Bhabendu Kumar Mohanta, Soumyashree S Panda, and Debasish Jena. An overview of smart contract and use cases in blockchain technology. In *2018 9th international conference on computing, communication and networking technologies (ICCCNT)*, pages 1–4. IEEE, 2018. 1
- [17] Chimuka Moonde. *Secure mobile payment system based on Blockchain technology for higher learning institutions*. PhD thesis, The University of Zambia, 2023. 22
- [18] Chimuka Moonde and Jackson Phiri. Addressing covid-19 in higher education institutions with a blockchain-based mobile payment system. In *Computer Science On-line Conference*, pages 288–308. Springer, 2022. 22
- [19] Hossein Rezaeighaleh and Cliff C Zou. New secure approach to backup cryptocurrency wallets. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2019. 19
- [20] Tejal Shah and Shalilak Jani. Applications of blockchain technology in banking & finance. *Parul CUniversity, Vadodara, India*, 2018. 8
- [21] Karan Singh, Nikita Singh, and Dharmender Singh Kushwaha. An interoperable and secure e-wallet architecture based on digital ledger technology using blockchain. In *2018 international conference on computing, power and communication technologies (GUCON)*, pages 165–169. IEEE, 2018. 16
- [22] Yahya Skaf. Cryptocurrencies and blockchain technology applications. In *Artificial Intelligence for Capital Markets*, pages 73–90. Chapman and Hall/CRC, 2023. 1

Appendix A

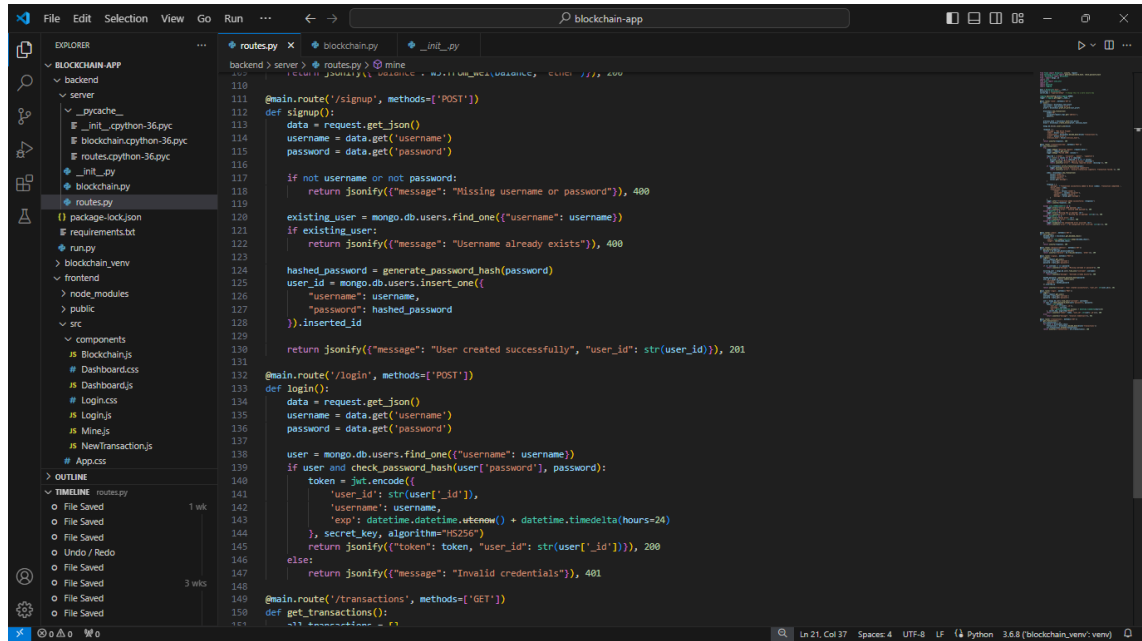
Python Code

A.1 Blockchain Class Implementation with AES Encryption and Ethereum Transaction Verification

```
backend > server > blockchain.py > Blockchain > _init_
16 class Blockchain:
17
18     def encode_data(self, data):
19         # Serialize data to JSON and then encode it with AES
20         json_data = json.dumps(data).encode('utf-8')
21         padder = padding.PKCS7(128).padder()
22         padded_data = padder.update(json_data) + padder.finalize()
23
24         iv = os.urandom(16) # Initialization Vector for AES
25         cipher = Cipher(algorithms.AES(self.aes_key), modes.CBC(iv), backend=default_backend())
26         encryptor = cipher.encryptor()
27         encrypted_data = encryptor.update(padded_data) + encryptor.finalize()
28
29         # Encode the IV and the encrypted data in base64 to store as a string
30         encoded = base64.b64encode(iv + encrypted_data).decode('utf-8')
31         return encoded
32
33     def decode_data(self, encoded_data):
34
35         # Extract the IV and the encrypted data
36         iv = encoded_data[:16]
37         encrypted_data = encoded_data[16:]
38
39         cipher = Cipher(algorithms.AES(self.aes_key), modes.CBC(iv), backend=default_backend())
40         decryptor = cipher.decryptor()
41         padded_data = decryptor.update(encrypted_data) + decryptor.finalize()
42
43         unpadder = padding.PKCS7(128).unpadder()
44         data = unpadder.update(padded_data) + unpadder.finalize()
45
46         # Deserialize JSON to Python object
47         return json.loads(data.decode('utf-8'))
```

Figure A.1. Blockchain Class Implementation with AES Encryption and Ethereum Transaction Verification

A.2 Python Flask for Blockchain Operations and User Authentication

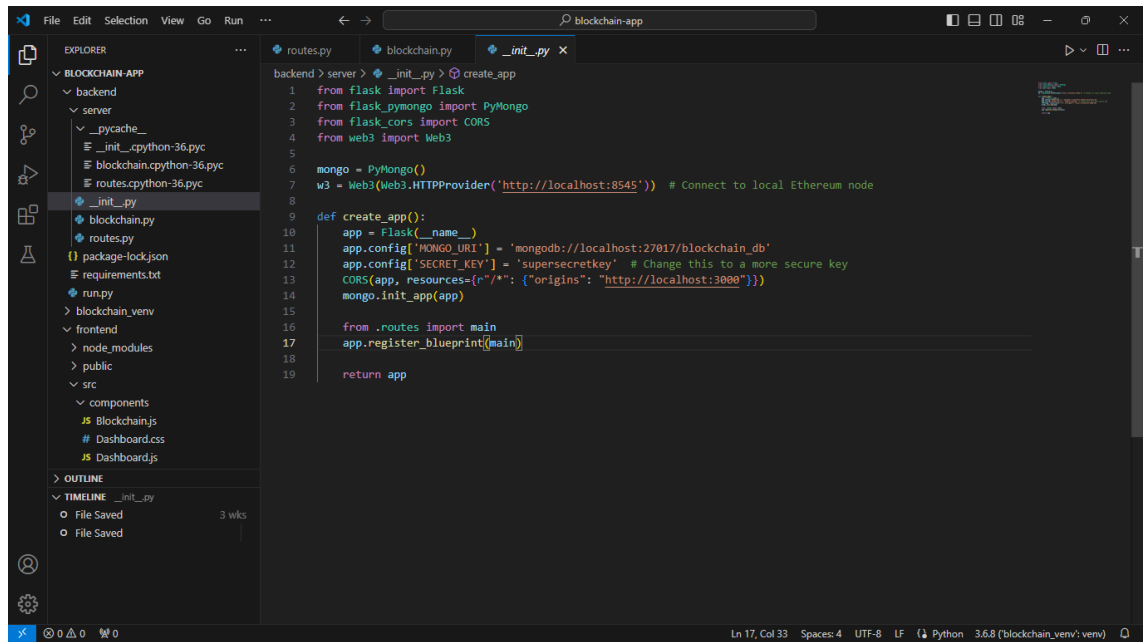


The screenshot displays a code editor with a dark theme. On the left, the 'EXPLORER' sidebar shows a project structure for 'BLOCKCHAIN-APP' with folders for 'backend' and 'frontend'. The 'routes.py' file is selected. The main editor area shows the code for the 'routes.py' file, which defines two Flask blueprints: 'signup' and 'login'. The 'signup' blueprint handles POST requests to '/signup', checks for existing users, hashes the password, and inserts the user into the database. The 'login' blueprint handles POST requests to '/login', checks the user's password, generates a JWT token, and returns it. The code is written in Python and uses Flask, MongoDB, and JWT libraries. The status bar at the bottom indicates the file is 'routes.py' at line 121, column 37, using UTF-8 encoding, and the Python version is 3.6.8.

```
110 @main.route('/signup', methods=['POST'])
111 def signup():
112     data = request.get_json()
113     username = data.get('username')
114     password = data.get('password')
115
116     if not username or not password:
117         return jsonify({"message": "Missing username or password"}), 400
118
119     existing_user = mongo.db.users.find_one({"username": username})
120     if existing_user:
121         return jsonify({"message": "Username already exists"}), 400
122
123     hashed_password = generate_password_hash(password)
124     user_id = mongo.db.users.insert_one(
125         {"username": username,
126          "password": hashed_password
127         }).inserted_id
128
129     return jsonify({"message": "User created successfully", "user_id": str(user_id)}), 201
130
131
132 @main.route('/login', methods=['POST'])
133 def login():
134     data = request.get_json()
135     username = data.get('username')
136     password = data.get('password')
137
138     user = mongo.db.users.find_one({"username": username})
139     if user and check_password_hash(user['password'], password):
140         token = jwt.encode({
141             'user_id': str(user['_id']),
142             'username': username,
143             'exp': datetime.datetime.utcnow() + datetime.timedelta(hours=24)
144         }, secret_key, algorithm='HS256')
145         return jsonify({"token": token, "user_id": str(user['_id'])}), 200
146     else:
147         return jsonify({"message": "Invalid credentials"}), 401
148
149 @main.route('/transactions', methods=['GET'])
150 def get_transactions():
151     pass
```

Figure A.2. Flask Blueprint for Blockchain Operations and User Authentication

A.3 Flask Application Setup with MongoDB and Ethereum Web3 Integration



```
1 from flask import Flask
2 from flask_pymongo import PyMongo
3 from flask_cors import CORS
4 from web3 import Web3
5
6 mongo = PyMongo()
7 w3 = Web3(Web3.HTTPProvider('http://localhost:8545')) # Connect to local Ethereum node
8
9 def create_app():
10     app = Flask(__name__)
11     app.config['MONGO_URI'] = 'mongodb://localhost:27017/blockchain_db'
12     app.config['SECRET_KEY'] = 'supersecretkey' # Change this to a more secure key
13     CORS(app, resources={r"//*": {"origins": "http://localhost:3000"}})
14     mongo.init_app(app)
15
16     from .routes import main
17     app.register_blueprint(main)
18
19     return app
```

Figure A.3. Flask Application Setup with MongoDB and Ethereum Web3 Integration