Trusted Framework for Online Banking Blockchain Framework

A Project Report Submitted
in Partial Fulfillment of the Requirements
for the Degree of

Bachelor of Technology

in

Computer Science and Business System

by

Mr. Rohit Shende	**PRN No.:1943110028**
Mr. Indrajit Datar	**PRN No.:1943110076**
Mr. Adwait Shinde	**PRN No.:1943110070**
Mr. Anurag Gulavane	**PRN No.:1943110073**

Under the guidance of

Prof. Reshma Kanse

COMPUTER SCIENCE AND BUSINESS SYSTEM
BHARATI VIDYAPEETH (D.U.)
DEPARTMENT OF ENGINEERING AND TECHNOLOGY,
OFF CAMPUS, NAVI MUMBAI

June 5, 2023

UNDERTAKING

We declare that the work presented in this project report titled "*Trusted Framework for Online Banking Blockchain Framework*", submitted to the Computer Science and Business System Department, Bharati Vidyapeeth Deemed to be University, Pune, Department of Engineering and Technology, Off Campus, Navi Mumbai, for the award of the ***Bachelor of Technology*** degree in ***Computer Science and Business System***, is our original work. We have not plagiarized or submitted the same work for the award of any other degree. In case this undertaking is found incorrect, We accept that my degree may be unconditionally withdrawn.

June 5, 2023
Navi Mumbai

Mr. Rohit Shende
PRN No.:1943110028
Mr. Indrajit Datar
PRN No.:1943110076
Mr. Adwait Shinde
PRN No.:1943110070
Mr. Anurag Gulavane
PRN No.:1943110073

CERTIFICATE

Certified that the work contained in the project report titled "***Trusted Framework for Online Banking Blockchain Framework***", by the following students:

Mr. Rohit Shende ***PRN No.:1943110028***
Mr. Indrajit Datar ***PRN No.:1943110076***
Mr. Adwait Shinde ***PRN No.:1943110070***
Mr. Anurag Gulavane ***PRN No.:1943110073***

has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

Prof. Reshma Kanse
Computer Science and Business System
Bharati Vidyapeeth (D.U.)
Department of Engineering & Technology
Off Campus, Navi Mumbai

June 5, 2023

Synopsis

Blockchain has emerged as an important financial software system. They rely on a secure distributed ledger data structure. They are increasingly becoming more popular in the world today. People seem to be finding newer ways to leverage the power of the blockchain for intuitive applications that provide solutions to real-world problems. An integral part of such systems, mining adds records of past transactions to the distributed ledger. On average, a block (the structure containing transactions) is mined every 10 minutes. Miners compete to solve a difficult mathematical problem based on a cryptographic hash algorithm. When a block is 'solved', the transactions contained are considered confirmed, and the Bitcoin concerned in the transactions can be spend. The Blockchain, it allows users to have secure, robust consensus for each transaction. One of the major applications of blockchain is Cryptocurrencies. They require strong, secure mining algorithms and since they lack a central authority to mediate transactions because they were designed as p2p systems, they rely on miners to validate the transactions. The ways in which emerging blockchain and distributed ledger technology (DLT) could transform the industry are enticing to companies constantly on the lookout for lower costs and greater efficiency. If fully adopted, it will enable banks to process payments more quickly and more accurately while reducing transaction processing costs and the requirement for exceptions. Therefore, we find the need to upgrade our banking system to mediate transactions and to this new technology. In this proposed system we design and develop custom blockchain technology with SHA, Mining and Chain Consensus Algorithm for provide security and privacy of secure baking transactions and also addition of designing a secure authentication technique with the help of keylogging

secure authentication methodology. Blockchain is a framework which is provide peer-to-peer (P2P) verification and validation protocols and using this protocols provide security and privacy of banking transaction systems.

There are several blockchain frameworks that could be used for online banking, but one of the most trusted and widely used is Hyperledger Fabric. Hyperledger Fabric is an open-source enterprise-grade blockchain framework that is designed to be highly scalable, secure, and flexible.

Hyperledger Fabric provides several key features that make it ideal for online banking, including:

1. **Permissioned network:** Hyperledger Fabric allows for a permissioned network, which means that only authorized participants can access the network and conduct transactions. This is important for online banking, as it ensures that only authorized parties can access sensitive financial data.
2. **Confidentiality:** Hyperledger Fabric supports confidentiality, which means that transactions can be kept private between the parties involved. This is important for online banking, as it ensures that sensitive financial information is not disclosed to unauthorized parties.
3. **Flexibility:** Hyperledger Fabric is highly flexible and allows for the creation of smart contracts that can be customized to meet the specific needs of the online banking system.
4. **Scalability:** Hyperledger Fabric is highly scalable, which means that it can support a large number of transactions and users.
5. **Security:** Hyperledger Fabric uses advanced cryptographic techniques to ensure that transactions are secure and tamper-proof.

Overall, Hyperledger Fabric is a trusted and reliable blockchain framework that could be used for online banking. However, it is important to note that implementing a blockchain-based online banking system requires careful consideration and planning, and should only be done with the guidance of experienced blockchain developers and security experts.

Acknowledgements

We would like to express my sincere gratitude to HoD **Prof. Reshma Kanse** of **Department of Computer Science and Business Systems** of Institute **"Bharati Vidyapeeth (D.U.), Department of Engineering and Technology, Offcampus, Navi Mumbai"** for their valuable support and guidance during this project. His dedication towards providing quality education, state-of-the-art infrastructure, and research opportunities has been instrumental in enabling us to undertake this project. The Institute's resources, facilities, and faculty members have provided us with an excellent platform to learn, grow and explore our potential.

We would like to express our sincere gratitude to our Supervisor **Prof. Reshma Kanse** for her invaluable contributions to this project.

Prof. Reshma Kanse's guidance, support, and mentorship have been critical in helping us to develop a deep understanding of the subject matter and to undertake this project with confidence. her constructive feedback, attention to detail, and commitment to excellence have inspired us to strive for the highest standards of quality and professionalism.

Throughout the project, Prof. Reshma Kanse provided us with his/her extensive knowledge, expertise, and insights, which helped us to navigate through the challenges and make informed decisions. Her collaborative and inclusive approach towards learning has fostered a culture of innovation and creativity, which has been vital in shaping our ideas and perspectives.

Moreover, We would like to thank Prof. Reshma Kanse for her generosity in sharing

her time, resources, and expertise with us. her unwavering support and encouragement have been instrumental in helping us to complete this project successfully.

Finally, We would like to express my deep appreciation to Prof. Reshma Kanse for her unwavering support and mentorship throughout the project. We are truly fortunate to have had the opportunity to work with her, and we will always cherish this experience.

Once again, thank you, Prof. Reshma Kanse, for your invaluable contributions to this project. We deeply appreciate all that you have done for us, and we are grateful for your guidance, support, and mentorship.

This Dissertation is Dedicated

To Mrs. Reshma Kanse whose support, guidance, and inspiration have been instrumental in making this research possible. Mrs.Reshma Kanse have been a constant source of encouragement and motivation throughout the journey of this dissertation. Her unwavering commitment towards our project has been critical in shaping our ideas and perspectives, and their leadership and mentorship have been invaluable in navigating the challenges and complexities of the research process.

Contents

List of Figures

List of Tables

List of Algorithms

Chapter 1

Introduction

A blockchain system may be considered as a simply incorruptible cryptographic database where vital and confidential user's information will be recorded. The system is maintained by a network of computers, which is accessible to anyone running the software. Blockchain operates as a pseudo-anonymous system that has nonetheless privacy problem in view that all transactions are exposed to the general public, even though it is tamper-proof inside the sense of data-integrity. The access control to manage heterogeneous user's confidential records across a couple of MNC establishments and devices had to be cautiously designed. Blockchain itself isn't designed as a massive-scale storage system. Within the context of framework for secure banking, a decentralized storage solution would significantly complement the weak point of blockchain within the perspective. The blockchain network as a decentralized system is extra resilient in that there is no single-point assault or failure compared to centralized systems. However, because all the bitcoin transactions are public and everyone has got right of entry to, there already exists analytics equipment that picks out the members within the community based totally on the transaction records [2].

In this proposed work fig.1 shows the system overview, and the most important module is blockchain implementation comprises two kinds of records: blocks and transactions. In every block contains a timestamp and a link to a preceding block

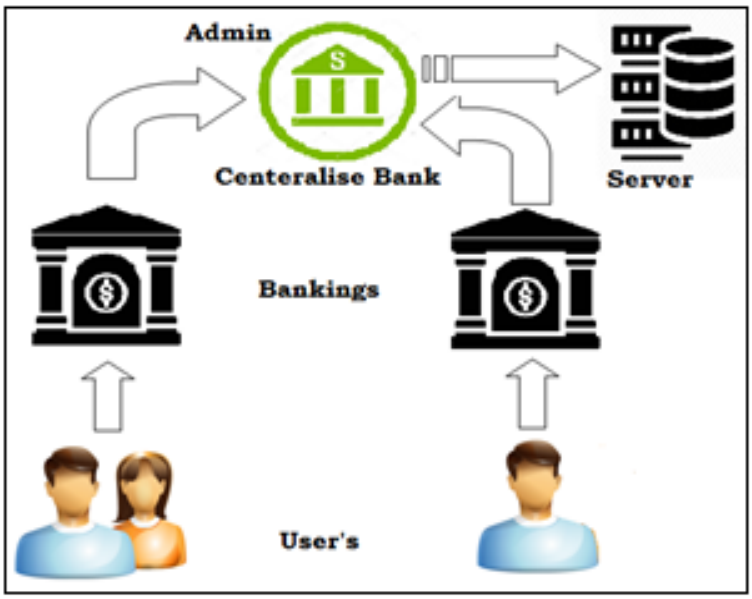

Figure 1.1: System Overview

is supplied via the secure hash algorithm. During the storage, the transaction information into the blockchain system executes various algorithms like SHA for hash generation, mining for generating a valid hash, smart contract for system policy, and consensus for validating current blockchain on all Peer to Peer nodes. Therefore, banking application is more secure. Second thing is that data storage and accessibility. For this point use the Secret Shamir hashing technique and keyword as well as content-based cryptography techniques.

The purpose of this project report is to provide an in-depth analysis of the use of blockchain technology as a trusted framework for online banking. The report focuses specifically on the use of the Hyperledger Fabric blockchain framework, which is widely regarded as one of the most trusted and reliable blockchain frameworks for enterprise-level applications.

The report begins by providing a brief overview of the history of blockchain technology and its applications in various industries. It then goes on to discuss the unique

features of the Hyperledger Fabric blockchain framework and how they make it ideal for online banking. The report also explores the challenges and risks associated with implementing a blockchain-based online banking system and provides recommendations for mitigating these risks.

In addition to the technical aspects of the project, the report also considers the business and regulatory implications of using blockchain technology for online banking. This includes a discussion of the potential benefits of using blockchain technology, such as increased security, transparency, and efficiency, as well as the challenges associated with regulatory compliance.

Finally, the report concludes with a summary of the key findings and recommendations for organizations looking to implement a trusted framework for online banking using blockchain technology. Overall, the report provides a comprehensive analysis of the potential benefits and challenges associated with using blockchain technology for online banking and offers practical guidance for organizations looking to adopt this innovative technology.

In this project, Our **contributions** are listed below.

1. Analysis of the potential benefits of using blockchain technology for online banking: The report provides a detailed analysis of the potential benefits of using blockchain technology, such as increased security, transparency, and efficiency, for online banking.
2. Discussion of the unique features of the Hyperledger Fabric blockchain framework: The report provides an in-depth discussion of the unique features of the Hyperledger Fabric blockchain framework that make it ideal for online banking, including its permissioned network, confidentiality, flexibility, scalability, and security.
3. Consideration of the challenges and risks associated with implementing a

blockchain-based online banking system: The report provides a detailed analysis of the challenges and risks associated with implementing a blockchain-based online banking system and offers recommendations for mitigating these risks.

4. Exploration of the business and regulatory implications of using blockchain technology for online banking: The report considers the business and regulatory implications of using blockchain technology for online banking, including a discussion of the potential benefits and challenges associated with regulatory compliance.

5. Provision of practical guidance for organizations looking to implement a trusted framework for online banking using blockchain technology: The report offers practical guidance and recommendations for organizations looking to adopt blockchain technology for online banking, including recommendations for technical implementation, regulatory compliance, and risk management.

Overall, the contributions of the project report provide valuable insights and guidance for organizations looking to implement a trusted framework for online banking using blockchain technology.

1.1 Research Objectives

1. To provide an overview of the history and evolution of blockchain technology and its applications in various industries.

2. To examine the unique features of the Hyperledger Fabric blockchain framework and how they make it ideal for online banking.

3. To explore the potential benefits of using blockchain technology for online banking, including increased security, transparency, and efficiency.

4. To consider the challenges and risks associated with implementing a blockchain-based online banking system and offer recommendations for mitigating these risks.

5. To examine the business and regulatory implications of using blockchain technology for online banking, including the potential benefits and challenges associated with regulatory compliance.

6. To provide practical guidance and recommendations for organizations looking to adopt blockchain technology for online banking, including recommendations for technical implementation, regulatory compliance, and risk management.

7. To assess the potential impact of blockchain technology on the future of online banking and financial services.

Overall, the objectives of the project report aim to provide a comprehensive analysis of the use of blockchain technology as a trusted framework for online banking, and to offer practical guidance and recommendations for organizations looking to implement this innovative technology in their financial services.

1.2 Report Organization

- Introduction: This section provides an overview of the report's objectives and scope, as well as an introduction to blockchain technology and its potential applications in online banking.

- Background: This section provides a brief history of blockchain technology and its evolution, as well as an overview of its applications in various industries.

- Blockchain Frameworks: This section discusses the different blockchain frameworks available for online banking and focuses on the Hyperledger Fabric framework, explaining its features and benefits.

- Benefits of using Blockchain in Online Banking: This section examines the potential benefits of using blockchain technology for online banking, including increased security, transparency, and efficiency.

- Challenges and Risks: This section explores the challenges and risks associated with implementing a blockchain-based online banking system, including regulatory compliance, scalability, and data privacy.

- Business and Regulatory Implications: This section considers the business and regulatory implications of using blockchain technology for online banking, including a discussion of the potential benefits and challenges associated with regulatory compliance.
- Implementation: This section provides practical guidance and recommendations for organizations looking to implement a trusted framework for online banking using blockchain technology, including recommendations for technical implementation, regulatory compliance, and risk management.
- Future Outlook: This section discusses the potential impact of blockchain technology on the future of online banking and financial services, as well as emerging trends and future developments in the field.
- Conclusion: This section summarizes the key findings of the report and offers final recommendations for organizations looking to adopt blockchain technology for online banking.
- References: This section provides a list of sources and references used in the report.

Overall, this report organization provides a clear and logical structure for presenting the analysis and findings of the project report on Trusted Framework for Online Banking Blockchain Framework.

Chapter 2

Related Works

This chapter presents the relevant existing efforts of ChatGPT-like AI tools. There are several tools similar to ChatGPT that use natural language processing (NLP) to enable conversational interfaces. Here are some examples:

- Jiin-Chiou Chen, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen "Blockchain and Smart Contract for Digital Certificate" [1] In order to solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology would be proposed. By the unmodifiable property of blockchain, the digital certificate with anti- counterfeit and verifiability could be made. The procedure of issuing the digital certificate in this system is as follows. First, generate the electronic file of a paper certificate accompanying other related data into the database, meanwhile calculate the electronic file for its hash value. Finally, store the hash value into the block in the chain system. The system will create a related QR-code and inquiry string code to affix to the paper certificate. It will provide the demand unit to verify the authenticity of the paper certificate through mobile phone scanning or website inquiries. Through the unmodifiable properties of the blockchain, the system not only enhances the credibility of various paper-based certificates, but also electronically reduces the loss risks of various types of certificates.

- Austin Draper, Aryan Familrouhani, Devin Cao, Tevisophea Heng, Wenlin

Han "Security Applications and Challenges in Blockchain" [2] Blockchain technology is a highly popular yet highly misunderstood concept that is used today and in future applications. To enhance security and privacy, many applications adopt Blockchain. However, there are intrinsic drawbacks and emerging challenges. In this paper, we study popular security applications in Blockchain, present their major problems, as well as other challenges in Blockchain which allows future research to be conducted more efficiently.

- Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni and Luca Spalazzi Certificate "Validation through Public Ledgers and Blockchain" [3] Public key infrastructures (PKIs) are of crucial importance for the life of online services relying on certificate-based authentication like e-commerce, e-government, online banking, as well as e-mail, social networking, cloud services and many others. One of the main points of failure of modern PKIs concerns reliability and security of certificate revocation lists, which must be available and authentic any time a certificate is used. Classically, the CRL for a set of certificates is maintained by the same (and sole) certification authority (CA) that issued the certificates, and this introduces a single POF in the system. We address this issue by proposing a solution in which multiple CAs share a public, decentralized and robust ledger where CRLs are collected. For this purpose, we consider the model of public ledgers based on blockchain, introduced for the use in Cryptocurrencies that is becoming a widespread solution for many online applications with stringent security and reliability requirements.

- Santosh Pandey, Gopal ojha, Rohit Kumar and Bikesh Shresha "BlockSIM: A practical simulation tool for optimal network design, stability and planning" [4] In this paper we introduce BlockSIM, a comprehensive and open source blockchain system simulation tool which can assist blockchain architects better evaluate the performance of planned private blockchain networks by running scenarios and decide the optimal system parameters suited for their purposes. We compare the results of our simulation with real blockchain networks and demonstrate that BlockSIM can be used effectively by architects of blockchain

systems to plan and implement scalable, stable and resilient blockchain networks. Finally, we demonstrate via a real life example how architects can apply BlockSIM to plan and design real-world blockchain systems.

- Christopher Ehmke, Florian Wessling and Christoph M. Friedrich "Proof-of-Property - A Lightweight and Scalable Blockchain Protocol" [5] The approach proposed in this paper is based on the idea of Ethereum to keep the state of the system explicitly in the current block but further pursues this by including the relevant part of the current system state in new transactions as well. This enables other participants to validate incoming transactions without having to download the whole blockchain initially. Following this idea use cases can be supported that require scalable blockchain technology but not necessarily an indefinite and complete transaction history.

- S. Sunitha kumara, D. Saveetha "Blockchain and Smart Contract for Digital Document Verification" [6] In the proposing system along with the degree certificate entire personality and behaviour activities of the person using personal id will be uploaded in blockchain. Because of unmodifiable property it is stored in block chain. Initially the student request for the e-certificate by uploading certificate or personal id to electronic certificate system. If requesting for e-certificate, then the system will review certificate from the university or schools or from organization and get the assurance and store the serial number and e-certificate to the block chain. The system will be generating the QR code and send it to the user. When applying for company user will send only the certificate serial number and QR code received from the e- certificate company.

- Arvind Ramachandran, Dr. Murat Kantarcioglu "Using Blockchain and smart contracts for secure data provenance management" [7] In this work, we leverage blockchain as a platform to facilitate trustworthy data provenance collection, verification and management. The developed system utilizes smart contracts and open provenance model (OPM) to record immutable data trails. We show that our proposed framework can efficiently and securely capture and validate

provenance data, and prevent any malicious modification to the captured data as long as majority of the participants are honest.

- Ahmed Ben Ayed "Secure storage service of electronic ballot system based on block chain algorithm" [8] In this paper, we are going to leverage the open source Blockchain technology to propose a design for a new electronic voting system that could be used in local or national elections. The Blockchain-based system will be secure, reliable, and anonymous, and will help increase the number of voters as well as the trust of people in their governments.

- Kaidong Wu "An Empirical Study of Blockchain-based Decentralized Applications" [9] This paper presents a comprehensive empirical study on an extensive dataset of 734 dapps that are collected from three popular open dapp marketplaces, i.e., ethereum, state of the dapp, and DAppRadar. We analyse the popularity of dapps, and summarize the patterns of how smart contracts are organized in a dapp. Based on the findings, we draw some implications to help dapp developers and users better understand and deploy dapps.

- Jialiang Chang, Bo Gao, Hao Xiao, Jun Sun and Zijiang Yang "sCompile: Critical Path Identification and Analysis for Smart Contracts" [10] In this work, we propose an alternative approach to automatically identify critical program paths (with multiple function calls including inter- contract function calls) in a smart contract, rank the paths according to their criticalness, discard them if they are infeasible or otherwise present them with user friendly warnings for user inspection. We identify paths which involve monetary transaction as critical paths, and prioritize those which potentially violate important properties. For scalability, symbolic execution techniques are only applied to top ranked critical paths. Our approach has been implemented in a tool called sCompile, which has been applied to 36,099 smart contracts. The experiment results show that's Compiling is efficient, i.e., 5 seconds on average for one smart contract.

These are just a few examples of the various platform that use Blockchain Technology to enable conversational interfaces. Each platform has its own strengths and

Table 1: Proposed System Like Platforms

Tool	**Open Source**	**Model Size**	**Languages**
Ethereum Blockchain	Yes	Large	Multiple
Custom Blockchain	No	Medium	Multiple
Public Blockchain	Yes	Large	Multiple
Private Blockchain	No	Large	Multiple

weaknesses, and the best choice will depend on the specific use case and requirements.

In this example 1, we have created a table to compare Proposed System-like platforms based on several factors: whether the tool is open source, the size of the model, and the languages supported. The table has four columns: Tool, Open Source, Model Size, and Languages. Each row represents a platform, and we have included four examples: Proposed System, Ethereum, Custom, Public, and Microsoft Private Frameworks.

Chapter 3

Proposed System Algorithms

In this chapter, we will summarize the Proposed System Algorithms and services.

3.1 Hash Generation

Algorithm 3.1 Algorithm 1 for Hash Generation

Require: Genesis block, Previous hash, data D

Ensure: Generated hash H according to given data

1: **function** KeywordSearch(D, Q)
2: Step 1 : Input data as d
3: Step 2 : Apply SHA 256 from SHA family
4: Step 3 : CurrentHash= SHA256(d)
5: Step 4 : Retrun CurrentHash

A hash algorithm is a function that converts a data string into a numeric string output of fixed length. The output string is generally much smaller than the original data. ... Two of the most common hash algorithms are the MD5 (Message-Digest algorithm 5) and the SHA-1 (Secure Hash Algorithm). 3.3

Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value. It is

also used in many encryption algorithms.

3.2 Protocol for Peer Verification

Algorithm 3.2 Algorithm 2 for Protocol for Peer Verification

Require: User Transaction query, Current Node Chain CNode[chain], Other Remaining Nodes blockchain NodesChain[Nodeid] [chain]

Ensure: Recover if any chain is invalid else execute current query

1: **function** KeywordSearch(D, Q)
2: Step 1 : User generate the any transaction DDL, DML or DCL query
3: Step 2 : Get current server blockchain Cchain Cnode[Chain]
4: Step 3 : For each
5: NodesChain[NodeId, Chain](GetChain)
6: End for
7: Step 4 : Foreach (read I into NodeChain) If (!.equals NodeChain[i] with (Cchain))
8: Flag 1
9: Else Continue Commit query
10: Step 5 : if (Flag == 1)
11: Count = SimilaryNodesBlockchian()
12: Step 6 : Cacluate the majority of server Recover invalid blockchin from specific node
13: Step 7: End if End for
14: End for

All peers on a blockchain network reach a consensus to verify transactions. This consensus is governed by an algorithm fed into the protocol layer of the blockchain. The blockchain gives all peers an identical copy of each transaction which eliminates trust thus making a trustless, distributed network. **??**

3.3 Mining Algorithm for valid hash creation

Algorithm 3.3 Algorithm 3 for Mining Algorithm for valid hash creation

Require: Hash Validation Policy P[], Current Hash Values hash Val

Ensure: Valid hash

1: **function** ValidHash(D, Q)
2: Step 1 : System generate the hash Val for ith transaction using Algorithm 1
3: Step 2 : if (hash Val.valid with P[]) Valid hash
4: Flag =1 Else Flag=0
5: Mine again randomly
6: Step 3 : Return valid hash when flag=1

Mining algorithms are the algorithms or functions that make the task of mining crypto-currencies possible.
Mining algorithms are the algorithms in charge of making possible the cryptocurrency mining. Normally these algorithms are cryptographic hash functions very complex and they can adjust the mining difficulty. A process that makes it more or less difficult for you to put together the puzzles that must be solved by the miners. This is to get miners to do complex computational work that, once solved, allows them to access a reward for that work. **??**

Chapter 4

Proposed System Implementation Details

The implementation details for the project report on Trusted Framework for Online Banking Blockchain Framework can include the following:

1. **Design and Architecture:** The first step in implementing a trusted framework for online banking using blockchain technology is to design and architect the system. This includes identifying the different components of the system, such as the nodes, channels, smart contracts, and consensus mechanism, and defining the rules for how they will interact.

2. **Hyperledger Fabric Setup:** The Hyperledger Fabric framework is a popular choice for implementing a blockchain-based online banking system due to its unique features such as a permissioned network, confidentiality, flexibility, scalability, and security. The implementation details for setting up a Hyperledger Fabric network can include configuring nodes, channels, smart contracts, and consensus mechanisms.

3. **Integration with Existing Banking Systems:** Once the blockchain network is set up, it needs to be integrated with existing banking systems to

enable seamless transactions between the blockchain network and the traditional banking system. This requires the use of APIs and other integration tools to enable communication between the two systems.

4. **Smart Contracts Development:** Smart contracts are the backbone of a blockchain-based system, and they need to be developed and deployed on the network to facilitate transactions. Smart contracts can be developed using various programming languages such as Go, Java, and JavaScript, depending on the requirements of the system.

5. **User Interface Development:** A user interface (UI) is essential to enable users to interact with the system. The UI can be developed using various front-end frameworks such as React, Angular, or Vue.js, and it should be designed to provide a seamless user experience.

6. **Testing and Deployment:** Once the system is developed, it needs to be thoroughly tested to ensure that it meets the required performance, scalability, and security standards. The system can then be deployed to a production environment for use by customers.

7. **Ongoing Maintenance and Support:** A blockchain-based online banking system requires ongoing maintenance and support to ensure that it remains up-to-date and secure. This can include regular updates to the system, bug fixes, and security patches.

Overall, the implementation details for a trusted framework for online banking using blockchain technology require careful planning, development, and testing to ensure that the system meets the required performance, scalability, and security standards. The system should also be designed to integrate seamlessly with existing banking systems and provide a user-friendly interface for customers.

It may include:

1. Use-case Diagram

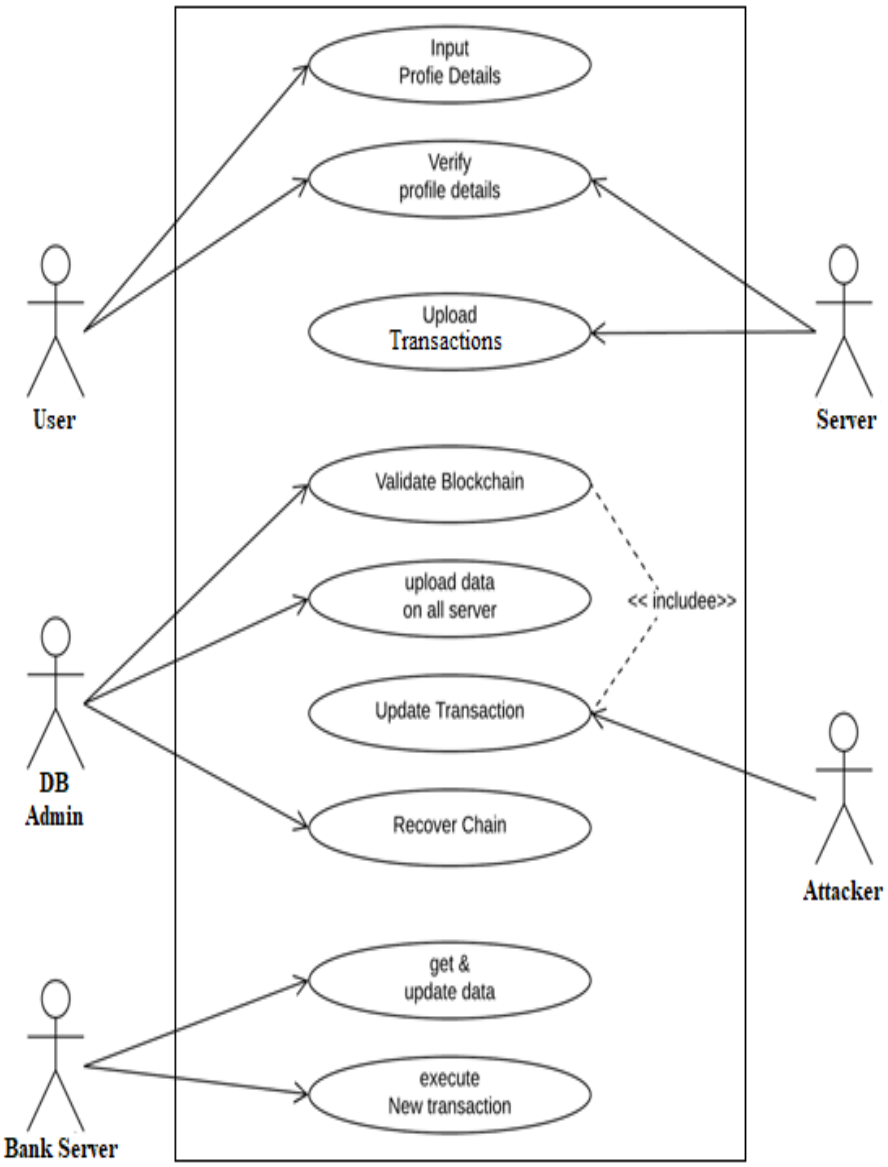

Figure 4.1: UseCase Diagram

2. Activity Diagram

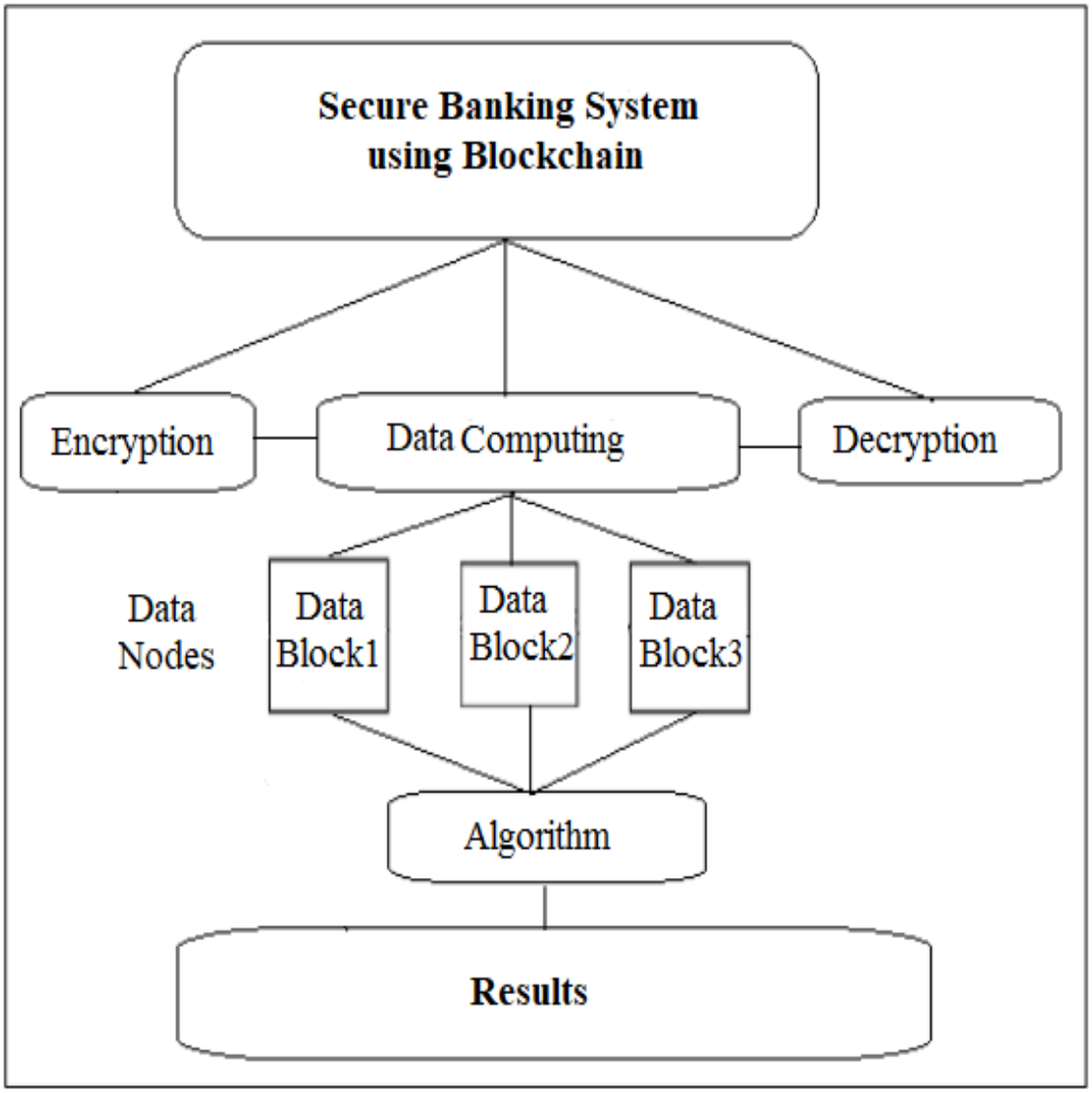

Figure 4.2: Activity Diagram

3. Sequence Diagram

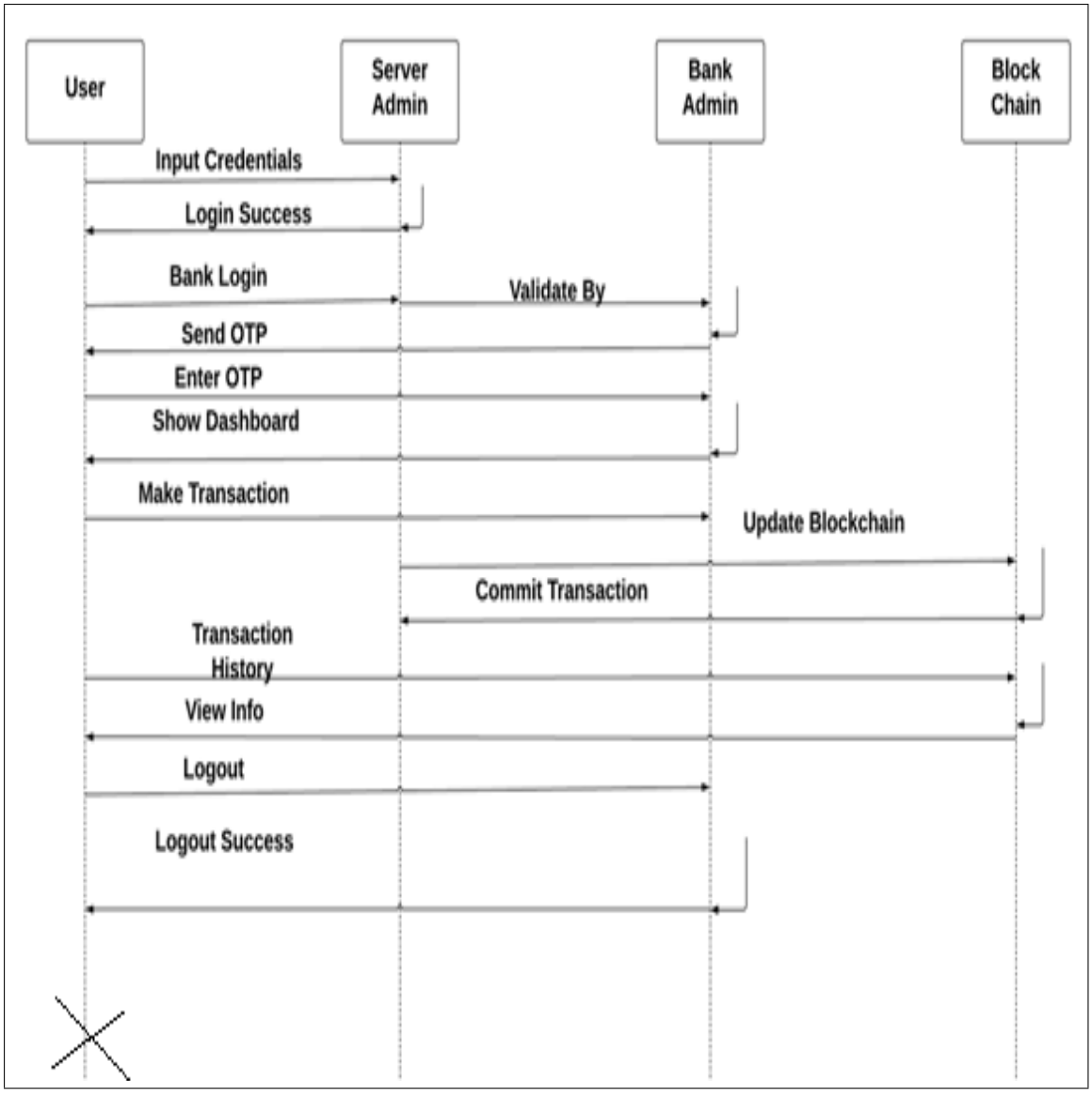

Figure 4.3: Sequence Diagram

4. Class Diagram

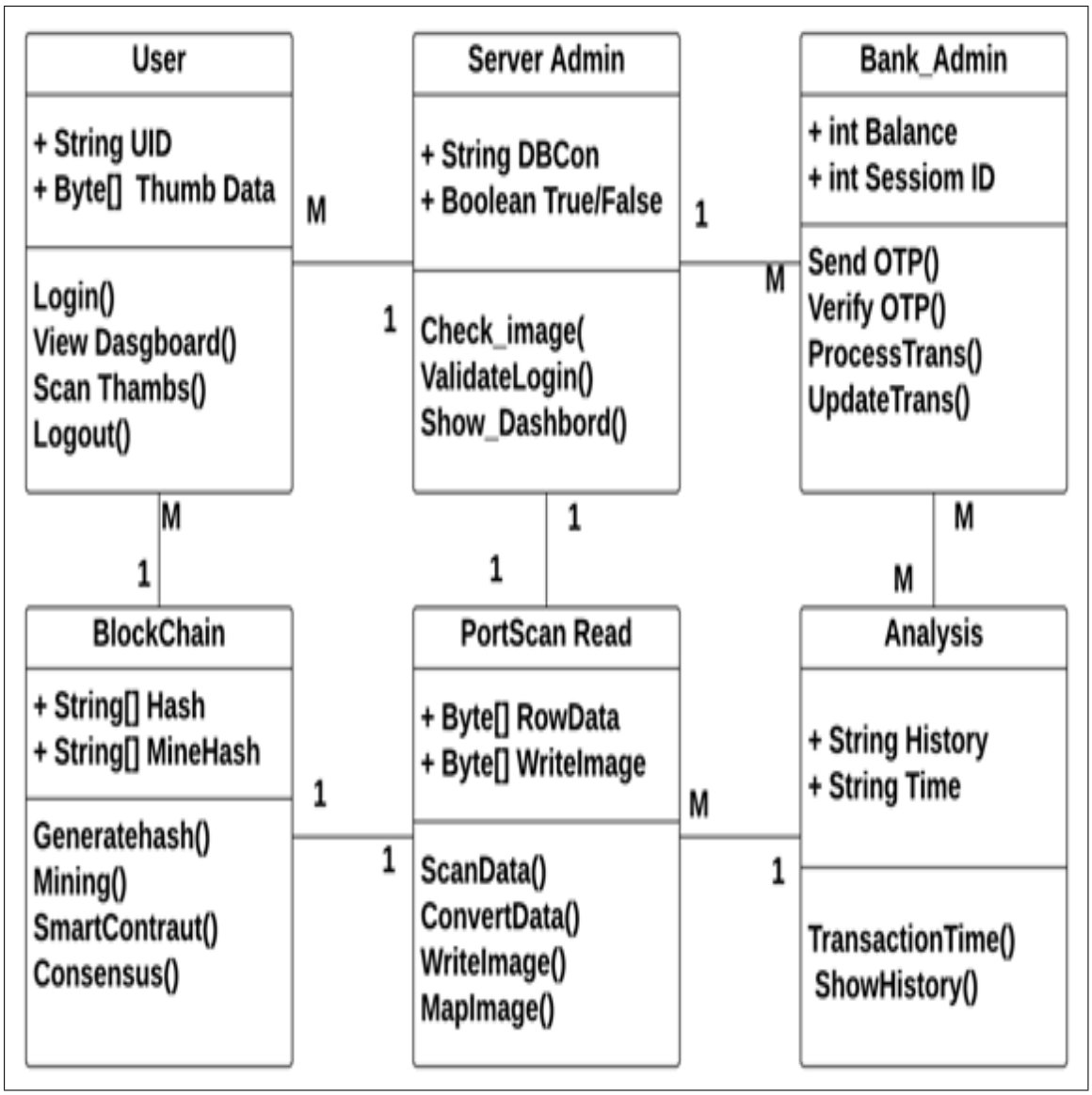

Figure 4.4: Class Diagram

5. Architecture Diagram

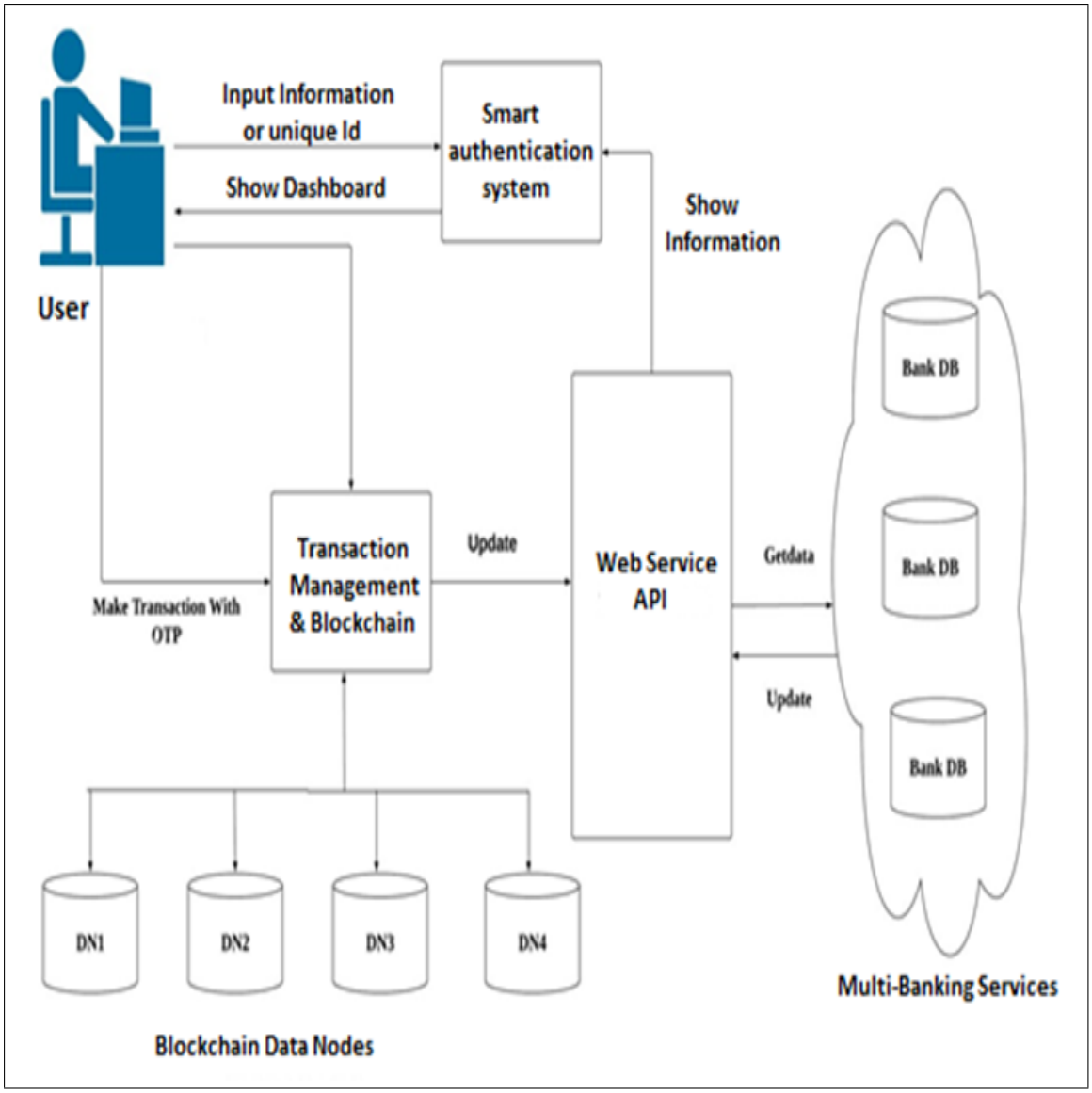

Figure 4.5: Architecture Diagram

Chapter 5

Result Analysis and Discussion

The result analysis and discussion for the project report on Trusted Framework for Online Banking Blockchain Framework can include the following:

- Increased Security: One of the most significant benefits of using a blockchain-based system for online banking is increased security. By using blockchain technology, it is possible to create a tamper-proof and immutable ledger that ensures the integrity of all transactions. Additionally, the use of cryptography in the blockchain network provides a high level of data security and confidentiality, reducing the risk of fraud, theft, and cyber-attacks.
- Improved Transparency: The use of blockchain technology in online banking can also improve transparency by providing a clear and auditable record of all transactions. This can help to reduce the risk of errors and fraud, as well as improve accountability and trust in the banking system.
- Enhanced Efficiency: Blockchain technology can also enhance the efficiency of online banking by reducing the time and cost associated with transaction processing. This is because transactions can be processed more quickly and with fewer intermediaries, reducing the risk of delays and errors.
- Challenges and Risks: Despite the potential benefits of using blockchain technology for online banking, there are also several challenges and risks associated

with implementation. These can include regulatory compliance, scalability, and data privacy concerns. Organizations need to carefully consider these challenges and risks before implementing a blockchain-based system.

- Business and Regulatory Implications: The adoption of blockchain technology for online banking can have significant business and regulatory implications. Organizations need to consider the potential benefits and challenges associated with regulatory compliance, including the need to comply with existing regulations and the potential for new regulatory frameworks to be developed.
- Future Outlook: The adoption of blockchain technology for online banking is still in its early stages, and there is a lot of potential for future development and innovation in this area. This includes the potential for new use cases and applications of blockchain technology, as well as the development of new regulatory frameworks to govern the use of blockchain in the banking sector.

Attribute	Public	Private	Consortium
Nature	De- centralized	Centralized	Semi-centralized
Homogeneity	Anonymous user.	Identified users Verified	Verified users
Administration	All nodes can mine	Centralized nodes can mine	Permissioned nodes can mine
Consensus Mechanism	All miners	Organization owners	Only Authorized nodes
Consensus Cost	Expensive	Inexpensive	Inexpensive
Time for verification	Few minutes	Few milliseconds	Few milliseconds
Protocol Efficiency	Low	High	High
Intrusion	Impossible	Possible	Possible

Figure 5.1: Contrast of Different Types of Blockchain

Overall, the result analysis and discussion for the project report on Trusted Framework for Online Banking Blockchain Framework highlight the potential benefits and challenges of using blockchain technology for online banking, as well as the need for careful consideration of regulatory compliance and data privacy concerns. The report also highlights the potential for future development and innovation in this area, which could transform the way that online banking services are delivered and consumed.

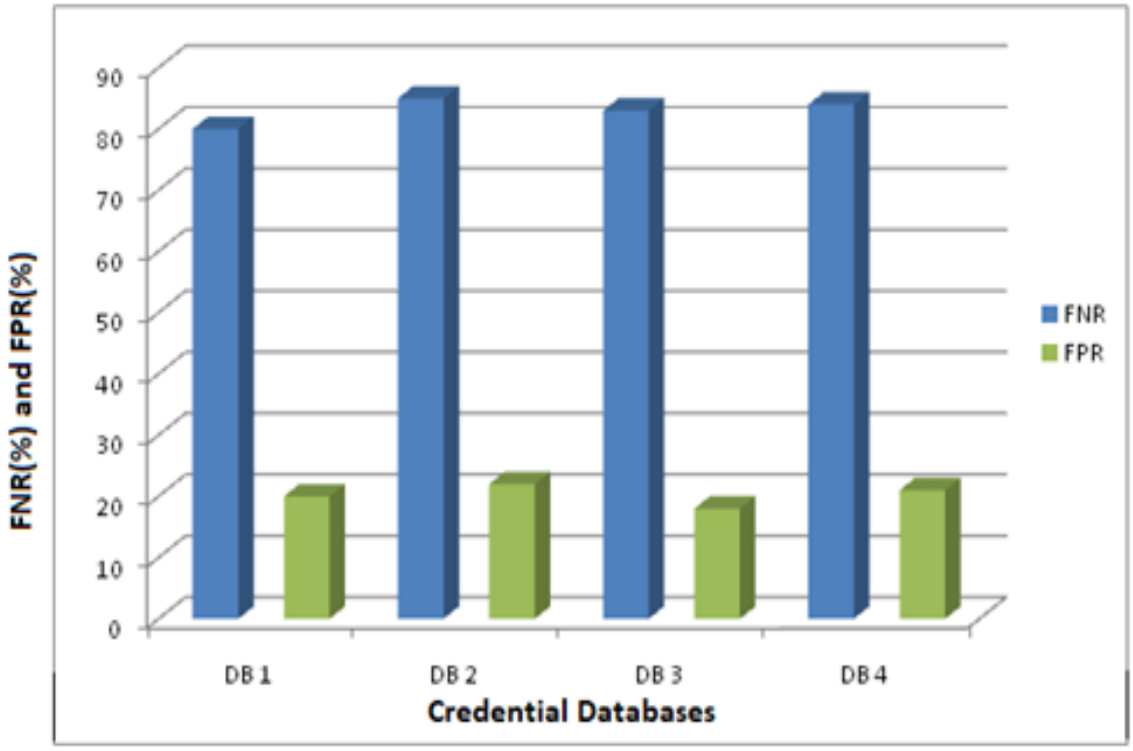

Figure 5.2: Performance of our proposed multi-factor Authentication

Chapter 6

Conclusion and Future Work

6.1 Conclusion

In conclusion, a trusted framework for online banking using blockchain technology has the potential to transform the way that online banking services are delivered and consumed. The implementation of a blockchain-based system can enhance security, transparency, and efficiency while reducing the risk of fraud, theft, and cyber-attacks. However, the adoption of blockchain technology for online banking also comes with challenges and risks, including regulatory compliance and data privacy concerns. Organizations need to carefully consider these challenges and risks before implementing a blockchain-based system.

6.2 Future Work

There are several areas of future work that could be explored in the context of a trusted framework for online banking using blockchain technology, including:

- Interoperability: The interoperability of blockchain networks is a critical challenge that needs to be addressed to enable seamless communication between

different blockchain networks. Future work could focus on developing solutions to address this challenge and enable interoperability between different blockchain networks.

- Scalability: Scalability is another critical challenge associated with the implementation of blockchain-based systems. Future work could focus on developing solutions to address this challenge and enable blockchain-based systems to process a large volume of transactions more efficiently.
- User Experience: User experience is an essential aspect of any online banking system. Future work could focus on improving the user experience of blockchain-based online banking systems to ensure that they are easy to use and provide a seamless customer experience.
- Regulatory Compliance: Regulatory compliance is a critical challenge associated with the adoption of blockchain technology for online banking. Future work could focus on developing new regulatory frameworks to govern the use of blockchain in the banking sector, ensuring that blockchain-based systems comply with existing regulations.
- New Use Cases: The adoption of blockchain technology for online banking is still in its early stages, and there is a lot of potential for new use cases and applications of blockchain technology in the banking sector. Future work could focus on exploring new use cases for blockchain technology in online banking, including the potential for decentralized finance (DeFi) and digital identity solutions.

Overall, the future work for a trusted framework for online banking using blockchain technology presents exciting opportunities for innovation and development in the banking sector. By addressing the challenges associated with the adoption of blockchain technology, organizations can leverage the potential benefits of this technology to deliver more secure, transparent, and efficient online banking services.

References

[1] Sabout Nagaraju and LathaParthiban, "Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway," Open Access Journal of Cloud Computing: Advances, Systems and Applications (2015)

[2] Dorri, S. S. Kanhere and R. Jurdak, "Blockchain in internet of things: Challenges and Solutions," arXiv: 1608.05187 [cs], 2019.

[3] Sukhodolskiy, Ilya, and Sergey Zapechnikov. "A blockchain-based access control system for cloud storage." Young Researchers in Electrical and Electronic Engineering (EICon- Rus), 2018 IEEE Conference of Russian IEEE, 2018.

[4] Yang, Huihui, and Bian Yang. "A Blockchain-based Approach to the Secure Sharing of Healthcare Data." Proceedings of the Norwegian Information Security Conference. 2020.

[5] Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006.

[6] Wang, Hao, and Yujiao Song. "Secure cloud-based EHR system using attribute-based crypto-system and blockchain." Journal of medical systems 42.8 (2018): 152.

[7] Michalevsky Y, Joye M. "Decentralized Policy-Hiding Attribute-Based Encryption with Receiver Privacy".

[8] Wu, Axin, et al. “Hidden policy attribute- based data sharing with direct revocation and keyword search in cloud computing.” Sensors 18.7 (2018): 2158.

[9] Khan S, Khan R. “Multiple authorities’ attribute-based verification mechanism for Blockchain micro-grid transactions”. Energies. 2018 May; 11(5):1154.

[10] Guo, Rui, et al. “Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems.” IEEE Access 776.99 (2018): 1-12.

[11] Monika D. Rokade, Dr. Yogesh Kumar Sharma, “Deep and Machine Learning Approach’s for Anomaly based Intrusion Detection of Imbalanced Network Traffic.” IOSR journal of Engineering (IOSR JEN), ISSN (e): 2250-3021, ISSN(p): 2278-8719

[12] Monika D. Rokade, Dr. Yogesh Kumar Sharma, “MLIDS: A Machine Learning Approach for Intrusion Detection for real time Network Dataset.” 2021 International Conference on Engineering Smart Computing and Informatics (ESCI), IEEE.

[13] Monika D. Rokade, Dr. Yogesh Kumar Sharma. (2020) “Identification of Malicious Activity for Network Packet using Deep Learning.” International Journal of Advance Science and Technology, 29(9s), 2324-2331.

[14] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Bitcoin.org, 2008.

[15] D. J. Hwang and K. Lee, “Analysis of security threats and solutions in payment systems,” Information Security Journal: A Global Perspective, vol. 25, no. 2, pp. 50–58, 2016.

[16] T. Dierks and C. Allen, “The TLS Protocol Version 1.3,” Internet Engineering Task Force, 2018.

[17] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Bitcoin.org, 2008.

[18] P. Koshy, D. Koshy, and P. McDaniel, “An Analysis of Anonymity in Bitcoin

Using P2P Network Traffic," in Financial Cryptography and Data Security, 2014, pp. 469–485.

[19] T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469–472, 1985.

[20] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.

[21] A. Shamir, "How to Share a Secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.

[22] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[23] B. A. Forouzan, Cryptography and Network Security: Principles and Practice, McGraw-Hill Education, 2015.

[24] B. C. Neuman and T. Ts'o, "Kerberos: An Authentication Service for Computer Networks," IEEE Communications Magazine, vol. 32, no. 9, pp. 33–38, 1994.

[25] J. Salowey et al., "The Secure Sockets Layer (SSL) Protocol Version 3.0," Internet Engineering Task Force, 1996.

[26] M. C. Rosu, M. Danubianu, and M. V. Rosu, "Blockchain Solutions for the Digital Banking Revolution," Procedia Economics and Finance, vol. 23, pp. 200–204, 2015.

[27] P. Koshy, D. Koshy, and P. McDaniel, "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic," in Financial Cryptography and Data Security, 2014, pp. 469–485.

[28] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum.org, 2014.

[29] D. J. Hwang and K. Lee, "Analysis of security threats and solutions in payment

systems," Information Security Journal: A Global Perspective, vol. 25, no. 2, pp. 50–58, 2016.

[30] C. N. Chuang, Y. C. Liao, and Y. C. Chen, "A Privacy-Preserving Cloud-Based Electronic Health Record System Based on Blockchain Technology," Journal of Medical Systems, vol. 42, no. 8, p. 139, 2018.