Software Associate NonceBlox Pvt. Ltd.

Project submitted in fulfilment of the requirement for the degree of

Bachelor of Technology

In

Information Technology

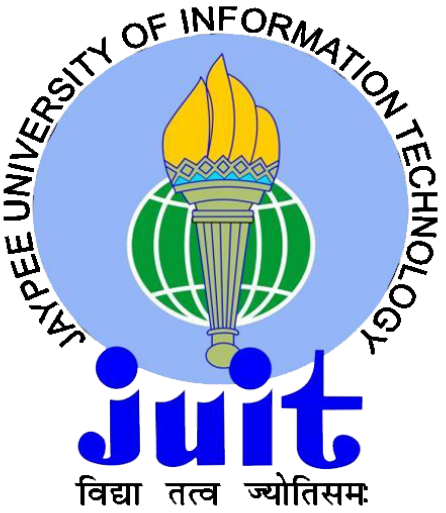
By:

Varun Chodha (191504)

UNDER THE SUPERVISION OF

Mr. Prateek Thakral

to



Department of Computer Science & Engineering and

Information Technology

Jaypee University of Information Technology

Waknaghat, Solan-173234, Himachal Pradesh

Candidate's Declaration

I hereby declare that the work presented in this report entitled " Software Associate NonceBlox Pvt. Ltd." in fulfilment of the requirements for the award of the degree of **Bachelor of Technology in Information Technology** submitted in the department of Computer Science & Engineering and Information Technology, Jaypee University of Information Technology Waknaghat is an authentic record of my own work carried out over a period from Feb 2023 to May 2023 under the supervision of Mr. Prateek Thakral Assistant Professor (Grade-II) Computer Science and Information Technology. The matter embodied in the report has not been submitted for the award of any other degree or diploma.

Varun Chodha (191504)

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

Mr. Prateek Thakral
Assistant Professor (Grade-II)
Computer Science and Information Technology
23-04-2023

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

PLAGIARISM VERIFICATION REPORT

Date: .....

Type of Document (Tick): PhD Thesis | M.Tech Dissertation/ Report | B.Tech Project Report | Paper

Name: _____ **Department:** _____ **Enrolment No** _____

Contact No. _____ **E-mail.** _____

Name of the Supervisor: _____

Title of the Thesis/Dissertation/Project Report/Paper (In Capital letters): _____

_____

_____

UNDERTAKING

I undertake that I am aware of the plagiarism related norms/ regulations, if I found guilty of any plagiarism and copyright violations in the above thesis/report even after award of degree, the University reserves the rights to withdraw/revoke my degree/report. Kindly allow me to avail Plagiarism verification report for the document mentioned above.

Complete Thesis/Report Pages Detail:

- Total No. of Pages =
- Total No. of Preliminary pages =
- Total No. of pages accommodate bibliography/references =

(Signature of Student)

FOR DEPARTMENT USE

We have checked the thesis/report as per norms and found **Similarity Index** at .....(%). Therefore, we are forwarding the complete thesis/report for final plagiarism check. The plagiarism verification report may be handed over to the candidate.

(Signature of Guide/Supervisor) **Signature of HOD**

FOR LRC USE

The above document was scanned for plagiarism check. The outcome of the same is reported below:

<table>
<tr><td>Copy Received on</td><td rowspan="4">• All Preliminary Pages
• Bibliography/Images/Quotes
• 14 Words String</td><td rowspan="3"></td><td>Word Counts</td><td></td></tr>
<tr><td>Report Generated on</td><td>Character Counts</td><td></td></tr>
<tr><td rowspan="2"></td><td>Submission ID</td><td>Total Pages Scanned</td><td></td></tr>
<tr><td></td><td>File Size</td><td></td></tr>
</table>

Checked by
Name & Signature **Librarian**

Please send your complete thesis/report in (PDF) with Title Page, Abstract and Chapters in (Word File) through the supervisor at plagcheck.juit@gmail.com

Acknowledgement

I am pleased to acknowledge my deep sense of gratitude to Jaypee University and my college, Jaypee University of Information Technology for giving me an opportunity to explore my abilities via this campus placement program. I would like to express my sincere gratitude to our Training and Placement officer, Mr. Pankaj Kumar. I am grateful to the HR department for their unwavering support, professionalism. I also wish to express my gratitude to my project supervisor for providing me with invaluable guidance, support, and feedback throughout the project's duration. I would also like to thank my teammates, who have been instrumental in completing various aspects of the project, and their contributions have been crucial to its success. Their cooperation, dedication, and hard work have helped me learn new skills and improve my abilities. I would like to record my sincere appreciation and gratitude towards all the officials, coaches, trainers, mentors and employees of NonceBlox Pvt. Ltd., without whose kind assistance, my placement program would not have been proceeding in a swift direction. The facts and other vital information provided by them have contributed towards making this report as comprehensive as possible.

Last but not the least, I would like to express my sincere thanks to all my family members, friends and well-wishers for their immense support and best wishes throughout the placement duration and the preparation of this report and I wish they would continue to contribute towards my well-being. I believe that this report will be a valuable asset not only for academic institutions, but will also be useful for all those who are interested to learn about internship/project experiences in blockchain and crypto firms.

Varun Chodha
191504

Table of Content

Certificate.....I

Plagiarism Certificate..... II

Acknowledgement..... III

Table of Content.....IV

List of Abbreviations..... V

List of Figures..... VI

List of Tables..... VII

Abstract..... VIII

Chapter 1: Project Introduction 1

Introduction 1.1.....1

Blockchain architecture 1.1.1 3

Block 1.1.2..... 4

Digital signature 1.1.3..... 5

Taxonomy of blockchain systems 1.1.4.....6

Consensus Algorithms 1.1.5.....9

Problem Statement 1.2..... 10

Objectives 1.3..... 11

Methodology 1.4..... 12

Organisation 1.5.....13

Chapter 2: Literature Survey.....14

Literature survey 2.1.....14

Chapter 3: System Development/Implementation.....24

Analysis 3.1.....24

Model Development 3.2.....25

Logical Architecture 3.2.1.....25

Physical Architecture 3.2.2.....26

Application Architecture 3.2.3.....29

Coding and UI standards 3.2.4.....30

Development environment 3.2.5.....30

Software 3.2.6.....31

Deployment 3.2.7.....31

Design 3.3.....31

Chapter 4: Experiment and Result Analysis.....34

Experimental setup 4.1.....34

Phases of Blockchain Testing 4.2.....34

Functional testing 4.2.1.....34

Security Analysis 4.2.2.....37

Performance Analysis 4.2.3.....38

Chapter 5: Conclusions..... 40

Conclusions 5.1..... 40

Future Scope 5.2..... 43

References..... 45

Appendices..... 47

List of Abbreviations

AML	Anti-Money Laundering
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
BFT	Byzantine Fault Tolerance
DAO	Decentralised Autonomous Organization
DAG	Directed Acyclic Graph
DeFi	Decentralised Finance
DLT	Distributed Ledger Technology
ERC	Ethereum Request for Comments
ICO	Initial Coin Offering
IPFS	Inter Planetary File System
KYC	Know Your Customer
MVP	Minimum Viable Product
NFT	Non-Fungible Token
P2P	Peer-to-Peer
PBFT	Practical Byzantine Fault Tolerance
PoW	Proof of Work
PoS	Proof of Stake
SHA	Secure Hash Algorithm

List of Figures

Figure 1.1 - Blockchain Transaction..... 2

Figure 1.2 - Blockchain hash..... 4

Figure 1.3 - Digital Signatures in blockchain..... 6

Figure 2.1 - Number of Blockchain papers yearly published and indexed by WoS.....19

Figure 2.2 - Growth in Healthcare Market.....20

Figure 3.1 - Authentication Flow..... 25

Figure 3.2 - Minting-coin Flow Architecture.....26

Figure 4.1 - Test structure diagram.....35

Figure 4.2 - Running Unit test Cases using Hardhat.....36

Figure 4.3 - Test case Success.....37

Figure 4.4 - Backend request cycle for blockchain-based application..... 39

List of Tables

Table 1.1 - Block Structure.....5

Table 1.2- Comparisons among public blockchain, consortium blockchain and private blockchain..... 7

Table 1.3 - Typical Consensus Algorithms Comparison.....9

Table 2.1 - Benefits and drawbacks of various platforms.....15

Abstract

Blockchain technology has the potential to revolutionise many industries by providing a secure, transparent and immutable data storage solution. Technology is used in many industries, including finance, healthcare, and supply chain management, among others. Therefore, there is a growing demand for experts who can develop blockchain applications that fit the needs of different industries. However, building successful blockchain applications requires certain techniques and skills. First, developers must have a deep understanding of technology, including various agreements, cryptography, and smart contracts. They should also be proficient in programming languages commonly used in blockchain development, such as Solidity, JavaScript, and Python. Blockchain application developers should have a good understanding of business and use cases in addition to technical skills. This includes identifying specific pain points that blockchain technology can solve and creating solutions that meet user needs. Good communication skills are also important for blockchain developers as they need to be able to explain complex concepts to non-technical stakeholders and work with a diverse team of experts. Finally, developers must keep up with the latest blockchain developments as technology changes rapidly and new applications are constantly emerging. In general, building a successful blockchain application requires a combination of expertise, business acumen, communication and commitment to keep up with the latest developments in the business. Good knowledge of programming languages, understanding of smart contracts, knowledge of cryptography, understanding of distributed systems, knowledge of database management, knowledge of development website editing, and understanding of business processes, to name a few, are some of the skills required.

Chapter-1 PROJECT INTRODUCTION

1.1. Introduction

In 2008, Satoshi Nakamoto published research "Bitcoin: A Peer-to-Peer Electronic Cash System" [1], which proposes a peer-to-peer (P2P) electronic cash system (Nakamoto, 2008). The system allows payments to be initiated by one party and sent directly to the other, without the need for a third-party financial institution. In recent years, as digital cryptocurrencies like Bitcoin have received more and more attention, researchers have gradually realised the important role of the blockchain as Bitcoin's underlying technology. Blockchain technology is a distributed ledger that uses cryptography to ensure that distributed data cannot be changed and smart contracts created from records terminate transactions. Currently, the application of blockchain technology is mainly focused on the financial sector, but has also brought about changes in non-financial sectors such as e-business, e-government, credit assessment and supply chain. Blockchain has gained prominence in the tech world due to its widespread acceptance and the business opportunities it creates for organisations that adopt it. Blockchain has become very popular, and for good reason. A highly skilled person is needed to fill the current high demand opportunity. Therefore, honing your skills as a blockchain expert is crucial if you want to gain a competitive advantage.

Today it is easier to become an expert in your field because there is a lot of blockchain technology training on the internet. Blockchain is a decentralised information and management system originally developed for the Bitcoin cryptocurrency [2]. Blockchain is a new type of database. This technology is very attractive to people because it can solve a big financial problem. This is a case of unmediated double spending. How does the technology behind blockchain work and how does it solve this problem?

Blockchain creates blocks containing various information. Each of these blocks is linked to other blocks in the blockchain of the digital currency. Proof of work is used to ensure the safety and security of the blockchain. Once connected to the blockchain, it is nearly impossible to modify or remove these blocks. One must have a very strong working power to break the blockchain. The miner is the person who calculates the hash value of a new block [3][4]. Blockchain technology has always been associated with cryptocurrencies because they are fundamental to the way cryptocurrencies work, but they are not the same thing. Blockchain technology is also used in other fields such as supply chain management and hospitals. The use of this technology increases the efficiency of work.

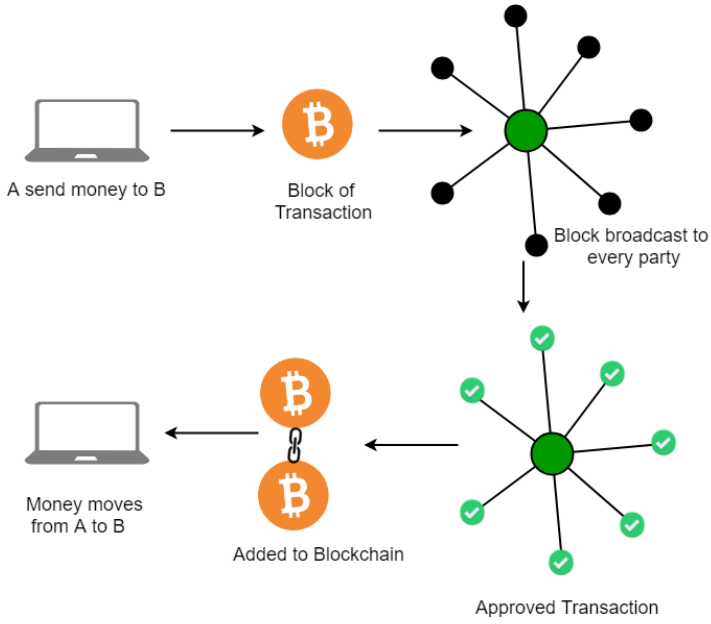


Figure 1.1 Blockchain Transaction

Interest has grown since 2008, when the concept of blockchain technology first emerged. The main feature of the blockchain is to provide security, anonymity and fair information without the control of the work by third parties, which attracts people who like it. This has led to the emergence of interesting studies, especially in terms of their implications and limitations.

Third-party organisations often mediate financial transactions between individuals or businesses. Banks or credit card companies must act as intermediaries to complete an electronic payment or currency exchange. A debit or credit card may also charge for the transaction. The same program is used for many other things, including software, games, and music. Businesses are generally neutral and instead of the two main parties involved in the transaction, all documents are processed and managed by a third party. To solve this problem, the application of blockchain technology has emerged. The technology behind the blockchain aims to create a controlled economy where data and transactions are not controlled by an external entity.

1.1.1. Blockchain architecture

In many systems, blockchain architecture can replace traditional server-based architectures. This is because blockchain offers greater security, stability and privacy in many applications. It can also support applications and digital assets in ways that centralised servers cannot, due to its immutable, transparent, and cryptographic features. Blockchain is a series of blocks containing all transactions that occur like a traditional general ledger. Figure 1 shows the blockchain in action.

Each block has a reference to the previous block; this is the hash of the previous block, called the main block. Uncle block hashes (children of block ancestors) will also be recorded on the Ethereum blockchain. The first block in the blockchain is called the genesis block, which does not have a main block.

The block structure is shown later in Section 1.1.2, following the digital signature process in Section 1.1.3. Section 1.1.4 shows the blockchain taxonomy.

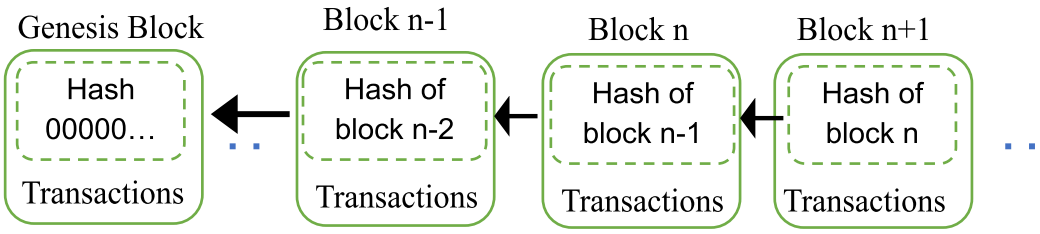


Figure 1.2 Blockchain hash

1.1.2. Block

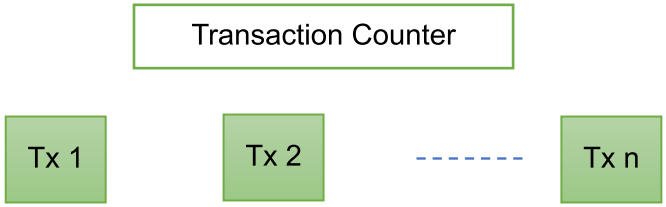
A group or group of transactions executed and confirmed simultaneously by a peer-to-peer network on a shared ledger. For example, all transactions initiated within ten minutes on the Bitcoin blockchain are confirmed and recorded as a new block. A block consists of a head block and a body block, as shown in Figure 1.1.2. Block headers specifically include:

- **Block interpretation**: indicates which set of block conformation rules to follow.
- **Parent block hash**: a 256-bit hash value that refers to the block behind.
- **Merkle tree root hash**: the hash value in the block for all the transactions.
- **Timestamp**: current timestamp as seconds since 2013-05-05T00:40 IST.
- **nBits**: It indicates the current hashing target in a minimised format.
- **Nonce**: a 4-byte field that typically begins with 0 and grows with each hash computation

Table 1.1 Block Structure

Block version	02000000
Parent Block Hash	Asfkas3h1398hf9hehf9hehfaasvyvyv

	83fhyg4F9ef82h39fg32fg9eufhuiefh
Merkle Tree Root	Gdgefgg3g2gfgueguf91uf8089f89ehf 83gf23gfgshdgfdgvd000023343gg4g
Timestamp	24d95a54
nBits	30c31b18
Nonce	Fe9f0864



1.1.3. Digital signature

A digital signature is a code used to verify the identity of the sender and the integrity of the message, as can be seen in the example in Figure 1.1.3. In a blockchain network, every user has a digital signature to identify them and ensure their transactions are secure. When users initiate a transaction on a blockchain network, they sign the transaction with their digital signature, which includes the transaction details and public keys.

Other users on the network then verify the signature using the sender's public key. This process ensures that transactions are accurate and not tampered with.

In addition to providing security and authenticity to transactions, digital signatures also play an important role in enabling smart contracts on blockchain networks. Smart contracts are standalone contracts that write promises to code. Digital signatures enable parties to sign and execute contracts without the need for third parties.

Overall, digital signatures are an essential part of blockchain technology that provides unified and seamless security, authenticity, and automation for transactions and smart contracts.

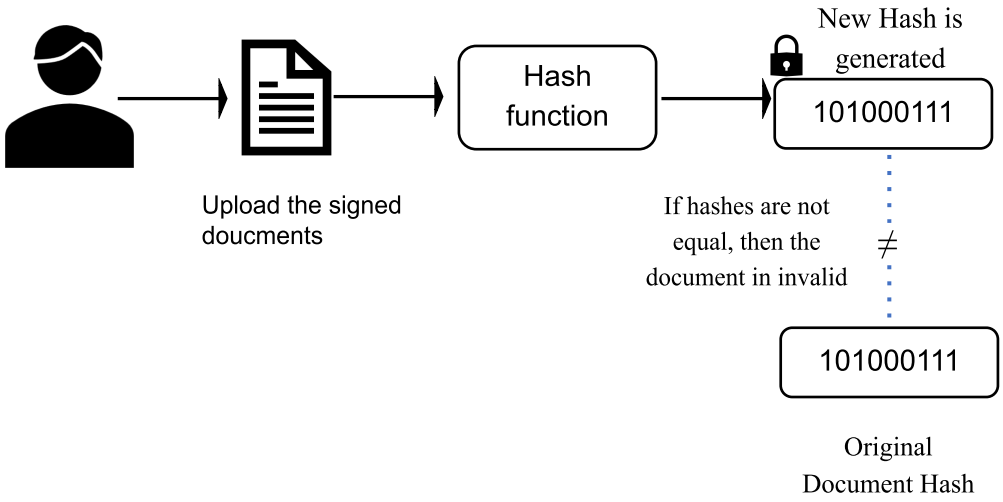


Figure 1.3 Digital Signatures in blockchain

1.1.4. Taxonomy of blockchain systems

Blockchain systems can be divided into several categories based on their features, governance standards, and practices. This taxonomy of blockchain systems provides a framework for understanding different types of blockchains and their unique features. One way of classifying blockchain systems is based on the confirmation mechanism, which determines how transactions are verified and added to the blockchain. For example, Proof of Work (PoW) and Proof of Stake (PoS) are two consensus methods used by many blockchain systems. Another way of classifying blockchains is based on permission levels, which determine who can join the network and complete transactions. In conclusion, Figure 1.1.3 shows that the taxonomy of blockchain systems provides an important framework for understanding different types of blockchains and their unique properties. By categorising blockchain

systems based on intelligence, governance, and application characteristics, it is easier to compare and evaluate different blockchain systems for specific applications. There are currently three types of blockchain systems: public blockchains, private blockchains, and consortium blockchains [5]. Consortium blockchains, on the other hand, only have a certain number of pre-selected participants in the consensus process.

In the case of private blockchains, only nodes belonging to an organisation are allowed to participate in the consensus process. Because it is completely controlled by a single entity, the private blockchain is considered the foundation of collaboration. Consortium chains created by many organisations are partially decentralised as only a small number of nodes are chosen to build consensus. Table 1.1.4.1 shows a comparison of the three different types of blockchains.

Table 1.2 Comparisons among public blockchain, consortium blockchain and private blockchain

Property	**Public blockchain**	**Consortium Blockchain**	**Private Blockchain**
Consensus Determination	All miner	Selected set of nodes	One organisation
Read permission	Public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered

Efficiency	Low	High	High
Centralised	No	Partial	Yes
Consensus Process	Permissionless	Permissioned	Permissioned

- *Consensus determination.* An accessible public blockchain where the node can participate in the consensus process. However, only one group can use blocks from the blockchain group. For private chains, it is controlled by an organisation and a specific organisation will determine the final truth, i.e. the business.
- *Read Permission.* The transactions in a blockchain that is publicly accessible are open to the public, whereas transactions in an enclosed or consortium blockchain are not.
- *Immutability.* Interfering with transactions on the public blockchain is almost impossible, as information is stored among many participants. On the other hand, transactions on private blockchains or public blockchains are easily interrupted due to the limited number of participants.
- *Efficiency.* Since there are many nodes in the public blockchain network, it takes a long time to send transactions and blocks. Therefore, speed changes are limited and delayed. Consortium blockchains and private databases can be more efficient with less verification.
- *Centralised.* The difference that distinguishes these three types of blockchains is that public blockchains provide distribution, enterprise blockchains are partially centralised, and private blockchains are fully centralised as they are under the control of a group or organisation.

Table no 1.3 Typical Consensus Algorithms Comparison

Property	PoW	PoS	PBFT	DPOS	Ripple	Tendermint
Node Identity Management	Open	Open	Permissioned	Open	Open	Permissioned
Energy Saving	No	Partial	Yes	Partial	Yes	Yes
Tolerated power of adversary	<25% computing power	<51% stake	<33.3% faulty replicas	<51% validators	<20% faulty nodes in UNL	<33.3% byzantine voting power
Examples	Bitcoin [6]	Peercoin [7]	Hyperledger Fabric [8]	Bitshares [9]	Ripple [10]	Tendermint [11]

Since the public blockchain is accessible worldwide, it can attract many users and a strong community. New blockchains with public access appear every day. Consortium blockchains can be used for a variety of business applications. Hyperledger [8] is currently working on a commercial consortium blockchain system. Ethereum also provides tools for building enterprise blockchains [12].

1.1.5. Consensus Algorithms

Consent algorithms play an important role in blockchain technology by enabling a network of partners to agree with the central government on the validity and sequence of unauthorised transactions. The main purpose of the consensus algorithm is to ensure the integrity and consistency of information distribution when there is no trust among the participants. However, reaching consensus in a decentralised environment is a difficult task due to the presence of faulty or

malicious nodes. Consensus algorithms must resolve issues such as network latency, node failure, and countermeasures to ensure the reliability and immutability of the blockchain. Reconciliation algorithms can be divided into two groups: classical consensus algorithms and Byzantine Fault Tolerant (BFT) consensus algorithms. Classic consensus algorithms such as Proof of Work (PoW) and Proof of Stake (PoS) rely on business support or computational challenges to drive business value. These algorithms are widely used in popular cryptocurrencies such as Bitcoin and Ethereum. On the other hand, BFT consensus algorithms, including Operational Byzantine Fault Tolerance (PBFT) and Tendermint, are designed to prevent Byzantine error, where nodes can exhibit malicious and malicious behaviour.

1.2. Problem Statement

It is no longer a secret that blockchain technology is changing rapidly and changing the system for the best. A technology that was once limited to trading cryptocurrencies (Bitcoin only) has defied all challenges and collaborated with many other fields [13]. This expansion has led to the prosperity of the world economy, which has had many positive effects on society. Blockchain technology is more efficient and secure because all the information entered into it cannot be changed and changed. Blockchain solutions can boast that they are the best at providing the highest level of data security. It is very reliable and reduces the risk of corruption in society and helps the government work better to improve the lives of its citizens. Governments and NGOs often have to use the services of third parties who can investigate their financial problems. This leads to increased costs and the possibility of incorrect reporting of costs. However, this can be limited to blockchain applications that allow users to track their costs and contracts by eliminating third-party applications. When it comes to social media and philanthropy, it's important for people

to be able to track their money and donations. Blockchain technology allows people to do this with the utmost transparency. The fact that all donations are put together for the public to see makes it even more believable. In this way, it evokes a sense of trust and security in the tavern. This project aims to address the following problems:

- Slow transfer of money between individual currencies/countries and subsequent non-transparency
- The disconnection of crypto from the real world
- Absence of non-dollar stablecoins
- The absence of corporate and government bonds and other real-world assets in blockchain
- Stablecoin user are not able to get exposure to bonds as a safe investment strategy
- The use of bonds as collateral isn't accessible to everyone

1.3. Objectives

Blockchain technology is a revolutionary innovation that has the potential to transform many industries by enabling secure, seamless transactions such as banks or other financial institutions. Blockchain is essentially a distributed technology that allows the creation of tamper-proof, transparent and immutable transaction records. The main purpose behind using blockchain technology is to build trust between two parties that do not need to trust each other. This is done by creating a collaborative system that uses consensus processes to implement and implement changes without the need for a central authority or individual environment. In doing so, blockchain technology eliminates the need for intermediaries and provides a secure, efficient and effective way to transfer assets and information between parties.

One of the main benefits of blockchain technology is its ability to reduce the risk of fraud and cyber attacks. Blockchains are designed to be tamper-proof, meaning that once transactions are recorded on the blockchain, they cannot be modified or deleted. This ensures that all parties involved in the transaction are confident that the transaction is legitimate and has not been manipulated in any way.

The aim of the project is to enable us to prioritise tokenized assets and tokenization as a service while advocating for greater financial visibility, efficiency and sustainability.

1.4. Methodology

Blockchain technology is a distributed and distributed information technology that enables secure, transparent and protected information. The process behind using blockchain technology includes many important concepts and methods to realise its unique capabilities and benefits.

Our solution is to fix the problems listed in the previous section. By tokenizing the world's assets and securities through our stable currency, our goal is to create a simple and accessible way to buy, sell and buy assets. This tokenization will bridge the gap between traditional finance and the cryptocurrency world, allowing users in different regions to tokenize an asset on demand, helping all assets circulate around the world with less friction. USD, EUR, CHF, CAD etc. We plan to create a contract for our stablecoins, including the United States, so that people can make investment decisions based on the investments they want to hold and the land they want to invest in, such as the US Treasury. bonds, German government bonds or stocks, real estate funds, etc. To ensure transparency and responsible management, we will regularly review our assets and resources and provide the public interest to ensure there is value and exposure to our work. By simplifying the process of investing in local or

international assets, we aim to eliminate complex terms and descriptions and eliminate intermediaries, thus providing financial transparency, efficiency and accuracy for individual investors and accounts.

1.5. Organisation

The introduction, the issue description, the inspiration, and the reasons why this project was chosen are just a few of the project-related themes covered. Blockchain has the potential to sustain your process domestically, improve process control, and significantly reduce lead times in comparison to outsourcing or relocating your process overseas. Blockchain solutions are focused on your specific needs and goals and quickly pay for themselves because of things like decreased operating expenses, shortened lead times, increased productivity, and other things. Blockchain increases trust, security, transparency, and the traceability of data shared across a business network. Although it might be difficult to foresee all of blockchain technology's societal benefits, its disruptive potential is understood. When completely adopted, blockchain technologies may increase the options for decentralised networks.

Chapter-2 Literature Survey

2.1 Literature survey

In this section, we present the "blockchain technology" case study. The literature review includes a critical evaluation of current research, highlights the strengths and weaknesses of the research, and identifies inconsistencies or inconsistencies in information. We also analyse research used in previous studies and their applicability to our research questions.

In "Smart Contracts in Blockchain Technology: A Critical Review", [14] Hamed Taherdoost provides an overview of the concept of smart contracts in the context of blockchain technology. This article examines the key features and advantages of smart contracts and the challenges and limitations associated with their implementation. The authors first define smart contracts as self-executing tasks that are stored on the blockchain and decide to execute when certain conditions are met. He explained that smart contracts have the potential to transform many businesses by reducing the need for intermediaries and increasing efficiency and transparency. This article explores the principles of smart contracts, including programming languages, data structures, and encryption techniques. The authors also discuss different types of smart contracts such as financial contracts, personal contracts, and network contracts. In addition to the benefits of smart contracts, this article also discusses the challenges and limitations associated with their use. These include issues with security, scalability, and interoperability. The whitepaper summarises the benefits and challenges associated with smart contracts and provides insight into the future of the technology. The purpose of the research is to determine where smart contracts are currently being proposed in the blockchain industry. The search was carried out with the utmost care, including a full review of all studies. Research questions, data, and data collection and analysis methods were used in the review process.

The main strategy checks the features of the first selected project to provide a transparent assessment of smart contracts in blockchain technology. The subsequent major steps comprise the overall approach:

- Reviewing the current state of the field.
- Recognising the review's importance.
- Identifying the field's difficulties and prospects for growth.
- A summary of the inquiry's outcomes.

A complete evaluation of the data should be open-minded. Before searching, a lot of relevant information has been selected to increase your ability to analyse important information. The initial source of the Scopus database was identified during the review. Professional blockchain programmers should help their clients identify the best blockchain platform and strategy for designing and implementing smart contracts to meet their organisation's needs. Smart contracts can be created and sent across multiple blockchain platforms, including Ethereum, Hyperledger Fabric, NEM, STELLAR, Waves, and Corda. Bitcoin is rarely mentioned when discussing smart contracts because its language is unwritten and emphasises security over programmability. The Bitcoin network cannot support smart contracts. Additionally, simple contracts that can be executed on Bitcoin are sometimes difficult to write and expensive to execute. Some systems offer different capabilities for creating smart contracts, including complex security levels, contract execution and contract terms. Table 2.1 explains the advantages and disadvantages of various platforms.

Table 2.1 Benefits and drawbacks of various platforms.

Platform	**Advantages**	**Disadvantages**
Ethereum	● Availability of diverse resources	● Due to subpar coding, many

	• Simple guidelines for developers • The smart contract programming language used by Solidity • Ethereum token standard • Free setup	smart contracts are vulnerable to attack. • Pricier than alternative platforms • issues with Ethereum's code's security. • network is too busy
Hyperledger Fabric	• enabling auxiliary plug-ins • consistent performance • Allowing contract coding in several languages. • Participation with permission • Free and open-source	• No token system
NEM	• Outstanding performance • Scalability • Platform-independent programming language • Simple to use	• NEM employs non-blockchain coding, making it less decentralised. • Less accessible tools • Fewer developers than other platforms
STELLAR	• Excellent performance • Simple platform • Highly respected in the business	• Unsuitable for sophisticated smart contract development

	• Cheaper than Ethereum	
WAVES	• Suitable for crowd sales • Token creation requires minimal basic knowledge	• Non-versatile platform • Still has a rather small user base
Platform	• **Advantages**	• **Disadvantages**

The next article by Suyel Namasudra and Pratima Sharma, "Achieving integrated and secure taxi sharing using blockchain technology" [15], explores the potential of blockchain technology to create an integrated and secure taxi sharing system. The authors draw attention to the problems and limitations of taxi-sharing and highlight the advantages that blockchain technology can bring to such systems. The authors claim that the basic nature of taxi-sharing makes them vulnerable to security threats such as cyber attacks and fraud. Additionally, these systems often have high transaction costs, limited transparency, and are vulnerable to information asymmetry. These problems can be solved using a decentralised system based on blockchain technology.

This article presents a public blockchain-based decentralised taxi sharing system. The system uses smart contracts to automate the ridesharing process without the need for an authority to manage the transaction. The system also includes a reputation-based system to ensure that participants in the system are trustworthy. The proposed system uses a public blockchain to store rideshare information such as journey details and transaction information. The authors argue that the public blockchain is more secure and transparent than the private blockchain because it is decentralised and transparent, making it harder for criminals to manipulate information. Additionally, using the public blockchain will increase users' trust in the system as it will allow them to verify the authenticity of the ridesharing information. Authors offer payments based on smart contracts without the need for intermediaries such as banks or

payment processors. A smart contract-based payment system ensures that money is transferred to the driver's account after the trip is complete. This eliminates the need for drivers to wait for payment and enables instant payment. The authors propose a Proof of Stake (PoS) consensus algorithm for blockchain networks.

The PoS consensus algorithm ensures that the network is safe and secure by requiring users to share their tokens to participate in the consensus process. This ensures that only trusted users are part of the approval process. This document provides a solution that addresses safety and reliability issues related to ride-hailing services. The application process is based on blockchain technology, which ensures flexibility and transparency of all changes in the system. The authors proposed a decentralised system where a network of users and service providers are interconnected via a blockchain-based platform.
The system aims to streamline the booking, payment and car sharing process by using smart contracts to provide safe and reliable ridesharing services.
The proposed system consists of three key components:

a. User Application: The user application is designed to enable users to search for available rides, book a ride, and make payments. The user application is connected to the blockchain network, which ensures the immutability and transparency of all transactions.

b. Service Provider Application: The service provider application is designed for drivers to manage their ride-sharing services. The service provider application is also connected to the blockchain network, which ensures the immutability and transparency of all transactions.

c. Blockchain Network: The blockchain network serves as the backbone of the proposed system. The blockchain network is designed to ensure the security and trustworthiness of all transactions in the system.

The article also discusses potential limitations of the proposed process, such as scalability and performance issues that may arise due to the use of public blockchain. But the authors suggest that these problems can be solved by using solutions to store business information and a consensus strategy to work well. Some of the disadvantages highlighted in this study are limitations, complexity, high energy consumption, lack of control, security concerns, and limited use.

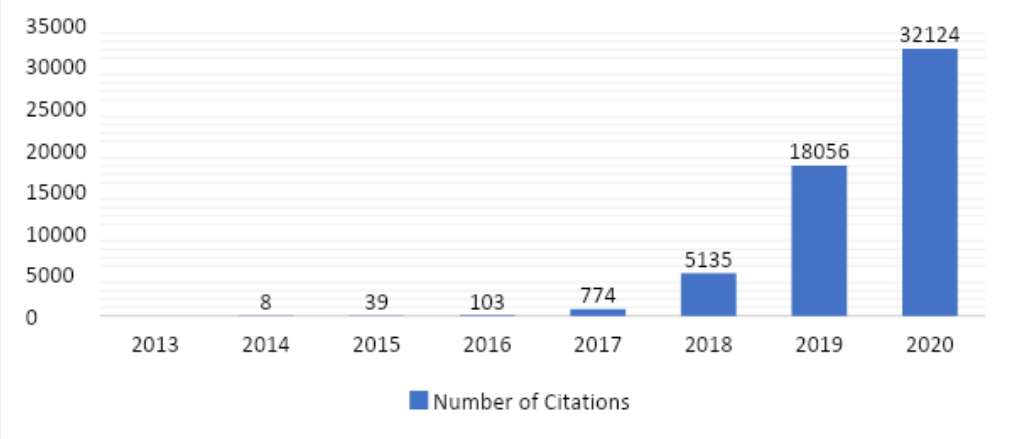


Figure 2.1 Number of Blockchain papers yearly published and indexed by WoS

The third article, "Research on Critical Success Factors for the Application of Blockchain Technology in the Healthcare Industry" [16] examines the critical success factors for blockchain technology adoption in the healthcare industry. The authors explore the benefits and challenges of blockchain technology and identify key factors affecting the success of blockchain technology in healthcare. The authors begin with a brief overview of blockchain technology and its potential applications in healthcare. They discussed how blockchain technology can be used to improve data security, improve information sharing, and simplify regulatory processes in healthcare. They also highlighted some of the challenges associated with using blockchain technology in the healthcare industry, such as regulatory issues, operational concerns, and concerns about

privacy. The authors then identify the key success factors affecting the adoption and use of blockchain technology in healthcare. They fall into three broad categories: organisation, technology, and environment. Organisations include leadership support, stakeholder engagement and change management strategies. The authors highlight the importance of cultural support and stakeholder engagement in promoting blockchain technology and ensuring its success. They also highlighted the need for effective change management strategies to address resilience to change and drive adoption of new technologies.

Key features include intelligence, information systems, and collaboration. The authors highlight the importance of expertise in the development and implementation of blockchain technology. They also highlighted the need for information design and coordination to enable information connectivity and communication between different health stakeholders. Environmental factors include regulatory frameworks, public trust, and business planning. The authors highlight the need for management support to foster innovation and collaboration in healthcare. They also highlighted the importance of gaining public trust in blockchain technology and ensuring that businesses are ready to adopt and use the technology. The steady growth can be predicted from the success of blockchain technology in healthcare and can be seen in Figure 2.1 from gminsights.com.

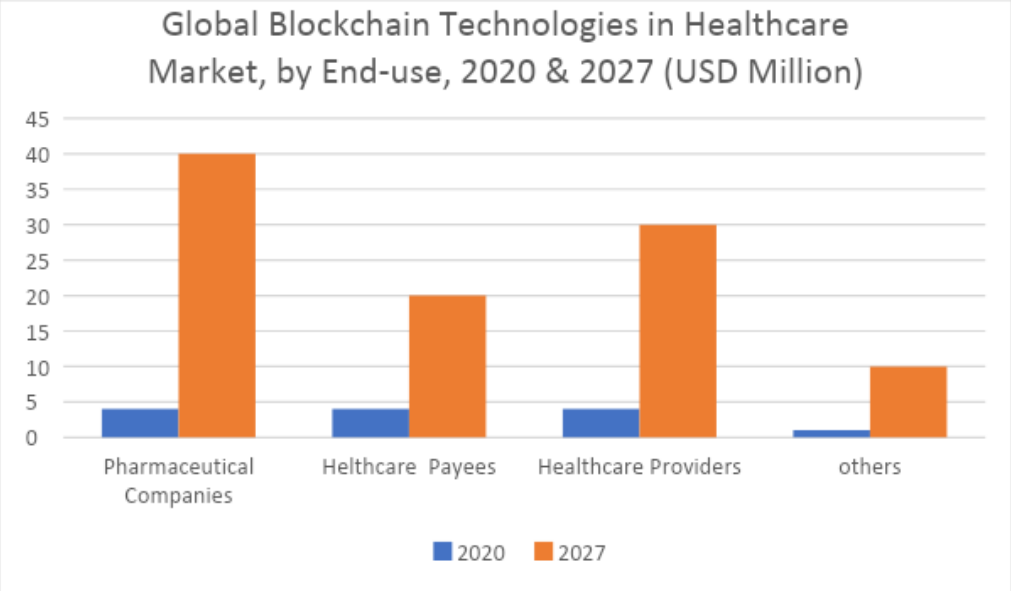


Figure 2.2 Growth in Healthcare Market

The authors conclude by discussing the potential benefits and challenges associated with the adoption of blockchain technology in the healthcare industry. They highlighted the benefits of improving information security, improving information sharing and simplifying administrative processes. They also acknowledge issues related to regulatory issues, operational concerns, and data privacy concerns. "Assessment of the importance of efficiency for the success of Blockchain Technology in Healthcare" is a document that proposes to solve problems related to the use of blockchain technology in healthcare. This article discusses key success factors to consider when using blockchain technology in healthcare. The authors outline the foundation for the success of blockchain technology in healthcare. The framework includes these key success areas: strategic planning, management, technology, data management, compliance, and user experience. M. Nour, J. P. “Analysis of blockchain potential in the energy sector and challenges of mass adoption” [17]

Article by Chaves-Ávila and Á. Sánchez-Miralles examines the potential applications of blockchain technology in the electronics industry and the challenges that must be overcome for the widespread use of blockchain in this

industry. The authors begin by discussing the issues affecting the energy industry, including the growing demand for electricity, the reintegration of renewable energy sources, and the need for safety and energy efficiency. They argue that blockchain technology can solve many of these problems by increasing security and transparency, reducing transaction costs and making energy transfers more efficient. The authors then provide an overview of blockchain technology and its key features such as decentralisation, transparency, and immutability. They explain how these resources can be used to build a secure and efficient electronic business and facilitate parties' work through smart contracts. The article then goes on to discuss various potential applications of blockchain in electronics, including peer-to-peer electronic commerce, renewable electronic certificates, and electronic payments. The authors present case studies of blockchain projects in each industry, highlighting the benefits that blockchain technology can bring to electronic commerce. However, the authors acknowledge that there are many challenges to overcome for blockchain to be adopted at scale in the economy. These challenges include regulatory uncertainty, coordination issues, and high leverage in blockchain networks. The report also suggests that blockchain technology can be used for grid management, enabling secure and efficient electronic transaction management and integration of electricity distribution into the grid. This will involve the use of smart contracts, which are standalone contracts that serve to verify and enforce the terms and conditions of the agreement.

In summary, a review of the literature on blockchain technology in various fields shows that the blockchain has a huge hidden goal to change the way transactions are executed, verified and recorded. Financial services, power chain operations, healthcare and energy, etc. Working with blockchain technology is different.

The data shows that blockchain technology can bring many benefits in financial services, such as reducing sales time, cost and intermediaries. It can also lead to economic growth and create new forms of financing similar to financial aid and microfinance. In the operation of the power chain, blockchain technology can increase transparency and traceability, reduce fraud and increase the efficiency of the chain. In healthcare, blockchain technology can improve data sharing, patient isolation, and secure data warehouses for the better. Technology can also facilitate the development of healthcare by giving patients less control over their health information and more sharing in their care. In the energy sector, blockchain technology can be used in many areas such as energy markets, demand management, and energy efficiency. Technology can facilitate the exchange of electricity and security between two parties without intermediaries, similar to electronic stores or trading companies. It can also provide customers with financial incentives, encouraging them to adjust their electricity consumption patterns during periods of high demand.

Chapter-3 System Development/Implementation

3.1. Analysis

The project outlines the challenges facing the current cryptocurrency market regarding tokenizing real-world assets and securities, coupled with the lack of inclusivity of the people from various walks of life to the current financial systems, therefore, highlighting its solution through stablecoins and what the current solutions lacks that are still in existence. This project proposes solutions to bridge the gap between traditional finance and the cryptocurrency world, including creating a token system for these assets and ensuring transparency and trust. Additionally, the project also discusses the tokenomics, technical details, roadmap, and future plans. The goal with this product is to facilitate mass adoption of these asset classes and provide a secure, reliable platform.

Presently, we are faced with a multitude of challenges that require our attention. However, the most pressing of these is the need for a straightforward solution for tokenizing real-world assets and securities, such as bonds, stocks, and commodities. This issue is inextricably linked to another challenge: the disconnection between the cryptocurrency realm and the real world and the absence of a seamless transition between the two. At the moment, we are witnessing a growing demand for tokenized real-world financial assets in the DeFi ecosystem. These assets provide users with increased options to diversify their portfolios, incorporating safer bets like bonds that can be used as collateral in DeFi. Moreover, investors from non-western countries can benefit from better access to these assets, thus facilitating greater financial inclusion across the globe.

In addition, we observe the need for more stablecoins that are backed by currencies other than the US dollar, such as the euro, Swiss franc, Canadian dollar, etc. This scarcity of stablecoins, coupled with the absence of clear "use

cases," presents a significant roadblock. Furthermore, we are witnessing a decline in trust for other stablecoin providers, over time, which further exacerbates the issue, among which the following are mostly ascertained:

a. Lack of transparency in the reserve management, thus, leading to various types of obfuscations.
b. For the stablecoins, there exists a lack of transparent asset allocation, and recourse of assets due to opaque asset management, which in turn, leads to a shortfall in conviction from the users.
c. Inability for mass adoption due to the high complexity for the average retail shop and user to move around and cash in/out just with stablecoins with low fees.

3.2. Model Development

3.2.1. Logical Architecture

The following diagram shows the big picture of Stable Architecture.

a. Authentication Flow

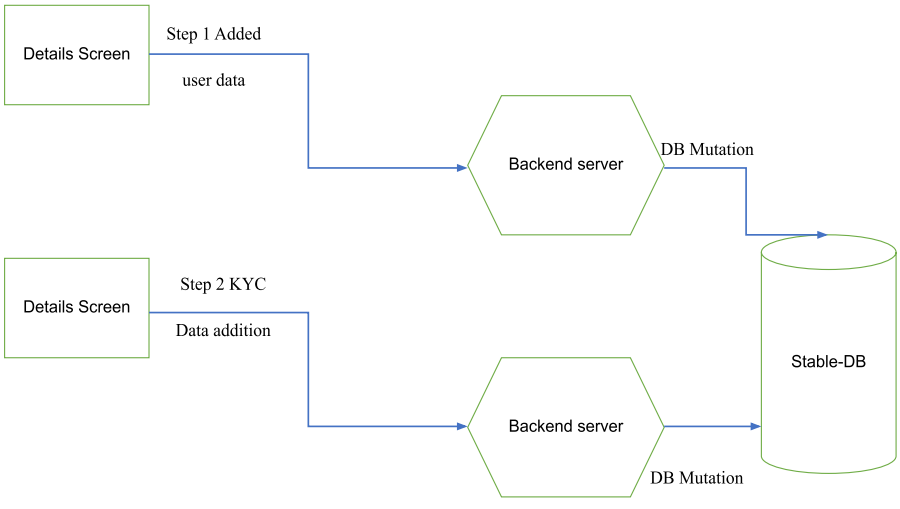


Figure 3.1 Authentication Flow

b. Minting-Coin Flow

We Use a payment provider that will take payments, will confirm the payments linked to the stable's account and initiate a mining procedure for the tokens

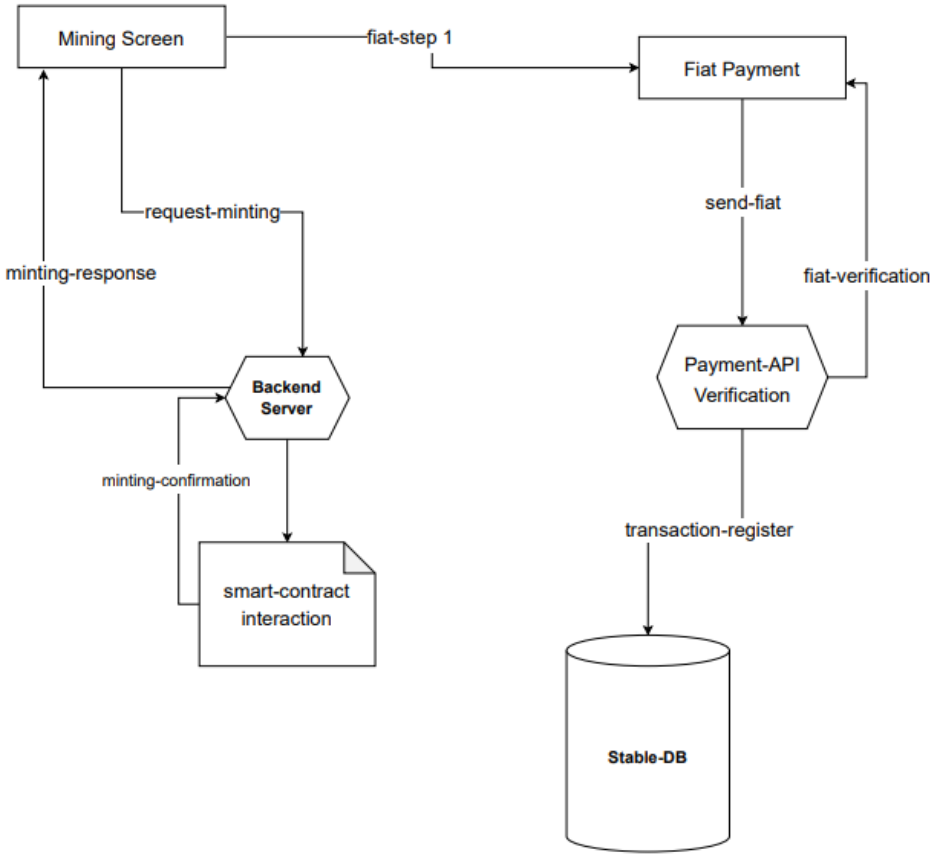


Figure 3.2 Minting-coin Flow Architecture

3.2.2 Physical Architecture

Type	Configuration	Installed Software
Web Server	Nest-JS	v9.3.0 (01-02-2023)
Database Server	MongoDB	^5.0 (22-07-2021)
Frontend	Next-JS	13.2.4 (10-03-2023)

Development		
Relational Model	Typegoose	^10.2.0
Smart Contract	Solidity	^0.8.17
Test cases and debugging	HardHat	^2.6.4
Cloud service	AWS	v3.312.0
Npm Packages for backend	jsonwebtoken mongoose node-cron typechian web3 axios bcrypt cookie-parser dotenv cors aws-sdk typechain/web3-v1	^9.0.0 ^6.10.0 ^3.0.2 ^8.1.1 ^1.6.1 ^1.3.4 ^5.1.0 ^1.4.6 ^16.0.3 ^2.8.5 ^2.1358.0 ^6.0.2

a. Nest-Js:

NestJS is the popular open source Node.js framework for building scalable, efficient and scalable external applications. NestJS aims to provide a robust architecture that supports flexibility, extensibility, and stability. It incorporates modern design principles such as injection moulding and appearance-oriented programming to make applications easier to use. A key feature of NestJS is that it supports TypeScript, a superset of JavaScript that adds features like static typing, interfaces, and classes.

This makes it easier to detect bugs early in the development process and provides better tools and code execution.

b. MongoDB:

Large volumes of unstructured data may be stored and managed using MongoDB, a well-known open source NoSQL data-oriented database. MongoDB stores data in files that resemble JSON and have a logical structure, as opposed to conventional SQL databases, which use tables with rows and columns to store data. Over conventional SQL databases, MongoDB has a number of benefits, including scalability, flexibility, availability, performance, community, and more.

c. Typegoose:

Type Goose is a library that adds TypeScript support to Mongoose. Using TypeScript classes and decorators, Mongoose lets you define schemas, making it easy to use Mongoose in safe mode. With Type Goose, you can define Mongoose schemas using TypeScript classes and interfaces; This means you can take advantage of TypeScript's IDE features such as static checking and code execution.

Type Goose offers many benefits of using the free Mongoose with TypeScript: type safety, improved IDE support, cleaner code, better editing, and more.

d. Next-JS

Next.js is a popular open source framework for building server-side rendered React applications. It was developed by Vercel (formerly Zeit) and is based on Node.js. Nextjs has many advantages over traditional React implementations, including server-side rendering, automatic code splitting, static site generation, automatic optimization, TypeScript support, and more.

e. Solidity:

Solidity is an advanced programming language used to write smart

contracts on the Ethereum blockchain. C++ is a statically related language from Python and JavaScript. Smart contracts are self-storable contracts on the Ethereum blockchain. They can be used to enforce contracts, enforce policies, and manage property changes. Solidity is the most popular language for writing smart contracts on the Ethereum platform.

f. AWS:

Amazon offers a cloud computing platform called AWS (Amazon Web Services). It provides a variety of cloud services that can be used to build, deploy, and manage applications and services in the cloud. AWS offers a wide variety of services, including compute, storage, database, analytics, machine learning, and networking.

g. Npm packages for backend:

NPM (Node Package Manager) is the package manager for Node.js, the server-side JavaScript runtime environment. NPM allows developers to develop and manage third-party packages (also called templates or libraries) that can be used in Node.js projects. The NPM package provides many functions that can be used to improve the development process and improve code quality. These packages may contain libraries for database management, logging, testing, authentication, and many other functions.

Using NPM packages, developers save time and effort by not having to write code from scratch and can leverage the expertise of other developers who have already created this package.

3.2.3 Application Architecture

a. Subsystems

➢ User Signup

- ➢ User Login
- ➢ User-info
- ➢ Join Waitlist
- ➢ Update User Info
- ➢ Verification
- ➢ Document Verification
- ➢ Connect wallet
- ➢ Deposit/Withdraw Funds
- ➢ Swap Transaction
- ➢ Bond Transactions
- ➢ Mint/Redeem
- ➢ Stake bonds
- ➢ Transaction history

3.2.4 Coding and UI standards

Coding standard followed during the project stable is also based on the latest industry standards.

3.2.5 Development environment

For the development of the project the following specifications are used:

- Ram: 8GB
- HDD: 100 GB
- Network: Above 1 MBps
- OS: Windows 10
- Blockchain: Ethereum

3.2.6 Software

- Visual Studio 2019 IDE
- Remix - Ethereum IDE
- MongoDB backend server
- MetaMask browser extension
- Nodejs

3.2.7 Deployment

For the initial deployment testnet is used for testing out the product for any changes and feedbacks and after the testing will be deployed to mainnet i.e. to the actual blockchain. The following specification are used for testnet

- Ram: 8GB
- HDD: 100GB
- Network: Above 1 MBps
- OS: Windows 10
- Testnet: Mumbai Testnet
- Backend and Frontend Host: AWS

3.3. Design

Stable's technical components can be divided into four key areas:

- Token Minting/Burning Mechanism
- Cross Chain Bridging
- Staking Contract
- Transaction Layer Subnets

A. Token Minting/Burning Mechanism

Our initial focus will be on EVM-native chains and gradually expand to include other architectural and consensus mechanisms. For now, with EVM in mind, our token standard will be an ERC-20. As a result, we can efficiently and seamlessly integrate with cross-chain interfaces, including Binance Smart Chain, Avalanche, Polygon, Optimism, Arbitrum, and many others.

B. Cross-Chain Bridging

Cross-chain bridging is a fundamental technology for facilitating cross-chain infrastructure, and it is our top priority as an organisation to make it as seamless and effortless as possible. To achieve this, we will implement multi-chain bridges that will follow a burning and minting mechanism with a verifier allocation allowing you to transfer assets between chains as desired. We have plans to partner with cutting-edge technology solutions to enhance the security and scalability of our bridging solution.

C. Staking Contract

Our staking contract aims to provide access to multiple asset classes through our stablecoins. From a technical perspective, it will be a time-locked contract that leverages decentralised oracles to retrieve the latest asset prices. Staking enables users to hold equivalent amounts of other assets supported by our platform. By staking, users will receive tokens of the corresponding assets and receive their staked stablecoins back upon maturity or if they choose to unstake.

D. Transaction Layer Subnets

Our mission is to make the financial system and transaction layer more accessible, fast, and transparent for everyone, which is where our subnets play a crucial role. We will partner with Avalanche to develop Stable's transaction layer, which will significantly enhance the overall Stable experience by:

- Expect a substantial increase in transaction speed with finalisation rates up to 4500/s
- Greater financial system adoption in previously underserved regions through the implementation of region-specific subnets
- Faster, cheaper, and smoother international transactions and investments. We have you covered.

In terms of technical aspects, you can be confident in the following as we work with an industry-standard organisation:

- The validators will be based in a country that is not subject to sanctions
- They will undergo thorough KYC/AML checks
- Additionally, they will hold at least one verification licence and have a clear background

Our partnership with Avalanche provides us with a robust and massively scalable solution, incorporating their already established validator ecosystem. This enables us to handle high volumes of transactions with minimal to zero latency.

Chapter-4 Experiment and Result Analysis

4.1 Experimental setup

We conducted several experiments to evaluate the effectiveness of our blockchain application in logistics management. The experiments were conducted using a private Ethereum blockchain network with a total of 10 nodes and 1 mining node. The app was built using Solidity and deployed on the blockchain using the Truffle framework. In order to test, compile, deploy, and debug dApps on the Ethereum network, we employed the Hardhat development environment. It plays a significant part in assisting programmers and developers with the administration of tasks, which is essential for the creation of smart contracts and dApps.

Initially the project deployment was carried out on a test network which would make it fully functional and would allow users to test out the application with dummy currency rather than spending their real cryptocurrency i.e. Ethereum or any other ERC token.

4.2 Phases of Blockchain Testing

Testing is an important step in blockchain application development. It makes apps work well and meet specific needs. The following are some of the test cases that a successful blockchain implementation should accomplish: being responsible for accuracy.

4.2.1 Functional testing

It includes smart contract functionality, transaction testing, node synchronisation testing, and consensus testing. Solidity tests and JavaScript tests are two options provided by the Truffle suite for

testing Solidity smart contracts. The question is, which should we use? The answer is both.

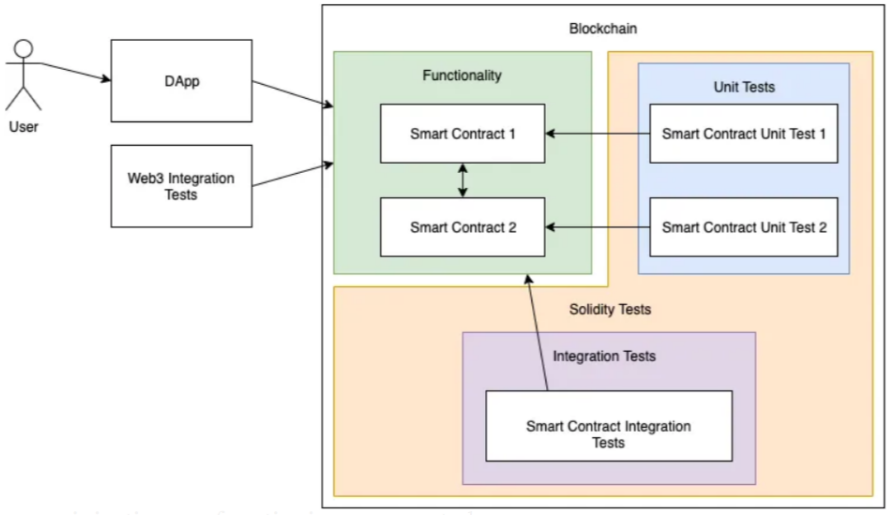


Figure 4.1 Test structure diagram

A. Solidity Tests

We can run tests on the Blockchain layer thanks to the Solidity test writing language. They enable testing to access contracts and operations as if they were actually present on the Blockchain. Smart contracts' internal behaviour may be tested by:

- To verify function return values and state variable values, create unit tests.
- Create integration tests that examine how contracts interact with one another. These make sure that mechanisms like dependency injection and inheritance are operating as intended.

B. JavaScript tests

Additionally, we must guarantee that smart contracts behave appropriately from the outside. We utilise Web3js, exactly as

our DApp, to test smart contracts from outside the Blockchain. When calling the smart contracts, we need to feel confident that our DApp front end will function properly. They are categorised as integration tests.

More is better when it comes to testing smart contracts. No effort should be spared to ensure that all methods are effectively returned to the request. Use blockchain-level Solidity tests for unit and integration tests, and Javascript tests for DApp-level integration tests.

To test out the solidity smart contract test cases were written and then Hardhat was used to run the test cases using the following command:

> npx hardhat test

The output generated can be seen in the following figure:

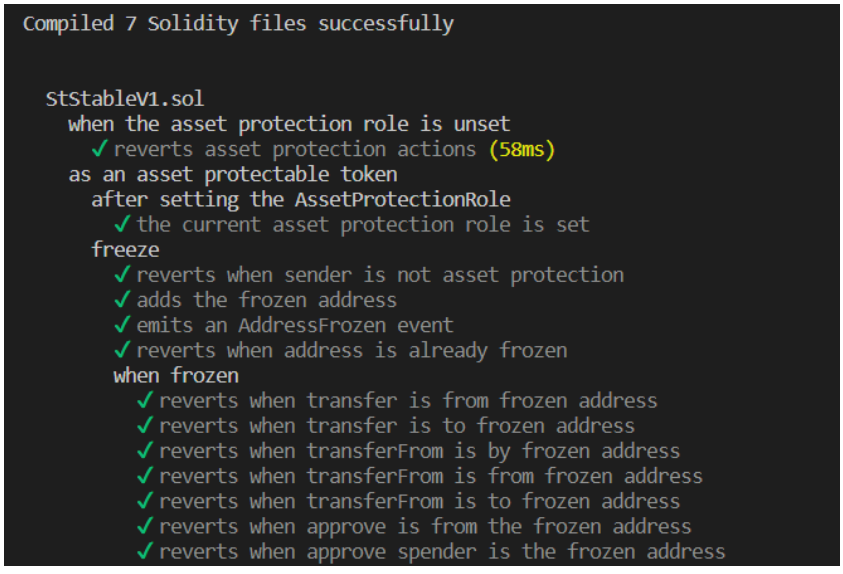


Figure 4.2 Running Unit test Cases using Hardhat

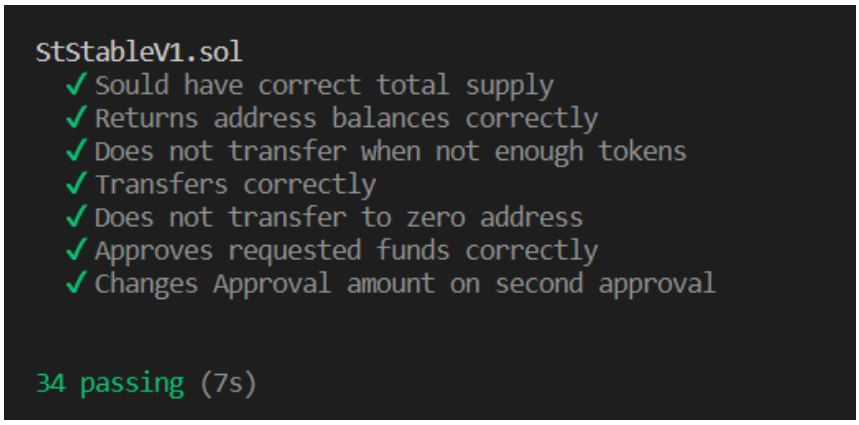


Figure 4.3 Test case Success

4.2.2. Security Analysis

Perform security analysis to identify and mitigate potential security vulnerabilities in blockchain applications. This includes testing for known security issues such as 51% attacks, Sybil attacks, Denial of Service (DoS) attacks, and more. Smart contract analysis involves analysing contract content to identify security issues, including invalid and ineffective forms, and identify ways to fix them. The audit process is an important link to ensure the security and reliability of blockchain applications.

It is often said that the law is the law in smart contracts. There is no space for error as a result of this. The contract only works in coded form. Once smart contracts are deployed, developers cannot change them. They have to create and submit a new version, which is expensive and time consuming. Intelligent Contractor Auditors can help ensure that coding is safe and secure. While blockchain technology is secure, there are vulnerabilities in the implementation of blockchain. One of the most famous cases involving smart contracts is

the theft of $50 million in 2016. The hackers exploited the underlying code in the DAO, a blockchain managed by smart contracts. These dangers may be reduced with the use of a smart contract security audit group.

A smart contract may be created and implemented for between $7,000 and $45,000. The cost of contracts utilised by large enterprises might exceed $100,000. Line-by-line manual examination and automated analysis utilising test suite tools are both provided by smart contract audit techniques. Auditing gives you peace of mind that your blockchain security is tight before you start executing your smart contracts. It can also reassure investors and clients that contracts will go as planned and that their financial resources are safe. Zero line is not a good thing but a necessity when building blockchain applications. With detailed information, you can be sure that your smart contract is secure and your app is ready to go.

4.2.3. Performance Analysis

Performance evaluation in the blockchain network includes finding vulnerabilities, reporting performance metrics, and determining which applications can be deployed. One such example includes financial services that test products to meet certain needs and conditions. Blockchain testing integrates solutions to test financial software running in a public environment using good knowledge transfer and good financial management evaluation methods.

Blockchain is a technology that has applications far beyond secure payments. As blockchain evolves into a platform for digital transformation, it offers a useful and disruptive alternative to the existing centralised storage and transaction system. Need of Performance Testing:

- To monitor the health of connected peers (disk i/o, CPU usage, and memory utilisation)
- To ensure scalability to support increasing the number of nodes
- Maintaining data integrity and preventing packet loss
- To ensure a seamless transaction
- To track the number of failed/delayed transactions due to timeouts

Many tools exist which can make this task much simpler to name a few NeoLoad, ELK Stack , JMeter, and Hyperledger Calliper Stack are just a few of the tools that may be used to assess the performance of blockchain applications.

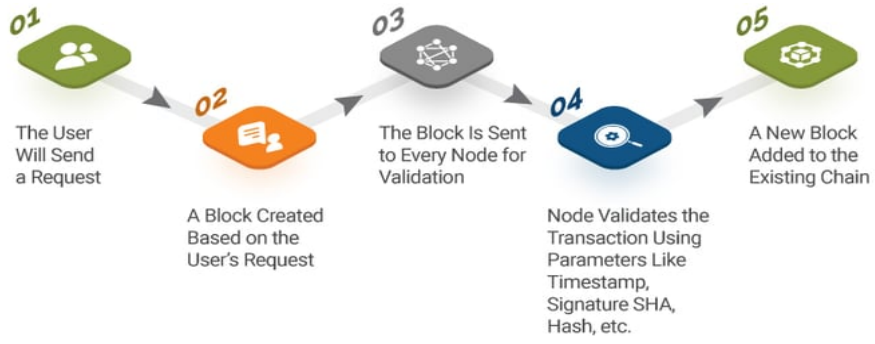


Figure 4.4 Backend request cycle for blockchain-based application

Chapter-5 Conclusions

5.1 Conclusions

Blockchain is a decentralised digital ledger technology used to securely, transparently and immutably record transactions and other information across multiple computers. Blockchain has gained immense popularity over the past few years and is used in industries for a variety of applications such as supply chain management, voting, financial transactions, and more. In this project, we are creating a blockchain-based financial transaction platform. The platform aims to provide secure, fast and transparent transactions while protecting users' anonymity and privacy. The platform was built using the Ethereum blockchain, a popular blockchain platform for building business applications. The platform has been tested to ensure it is robust, secure and scalable. We perform various tests such as load tests, security checks and integration tests to ensure that the platform can handle high volumes of transactions while maintaining a high level of security and trust.Blockchain technology has emerged as one of the most successful innovations in recent years. Originally developed for the digital currency bitcoin, blockchain has since expanded to provide regulatory, real estate, healthcare, and other applications and businesses.

The potential of blockchain technology is huge, and in this article, we will explore some of the key areas where blockchain has the potential to make a big impact.

1. Decentralised Finance (DeFi)

   Decentralised Finance or DeFi is a term used to describe new financial systems running on integrated blockchain networks. DeFi applications leverage smart contracts and other blockchain technologies to create a transparent and open financial system accessible to anyone with an internet connection. DeFi platforms offer a variety of financial services such as lending, trading and wealth management without

intermediaries like banks or other financial institutions. The potential of DeFi is huge because it can provide financial services to people who are not in the traditional financial system, while at the same time providing lower costs and transparency again.

1. Supply Chain Management

   Blockchain technology has the potential to revolutionise supply chain management by creating a transparent and secure way to track products from raw materials to final customers. Using the blockchain, immutable records can be created for all transactions and changes of ownership, making it easier to track and trace products and ensure that they are produced and delivered in a responsible and sustainable manner. This helps reduce fraud, improve product quality and increase product efficiency.

2. Self-Governing

   Blockchain technology can also be used to establish security and self-government. Thanks to the use of blockchain, it is possible to create proof of identity and personal information that can be accessed and verified without interference such as banks or government agencies. This will help reduce identity theft, fraud and other cybercrime, while also giving people greater privacy and security.

3. Health

   Blockchain technology can also be used to improve healthcare by creating a secure and transparent way to store and share medical information. Using blockchain, it is possible to create tamper-proof records of medical records that can be accessed and shared effectively by doctors and patients. This will help reduce errors, improve patient outcomes, and increase the effectiveness of treatment.

4. Real Estate

   Blockchain technology can also be used to improve the real estate market by creating a secure and transparent transaction. Using the blockchain, tamper-proof records of property and transactions can be created, making it easier to trade goods and reduce the risk of fraud. This will help increase the efficiency and ease of real estate transactions, while also providing greater transparency and security for buyers and sellers.

5. Voting Systems

   Blockchain technology can also be used to create secure and transparent voting systems that can help reduce voter fraud and increase confidence in the electoral process. Using blockchain, a tamper-proof document can be created for each ballot that can be accessed and verified by voters and voters. This will help count all the votes correctly and ensure that the election results are reliable.

6. Energy

   Blockchain technology can also be used to improve the electronics market by creating a decentralised and transparent electronic market. Using blockchain, immutable information about energy production and consumption can be generated, making it easier to trade and manage energy resources. This will help reduce energy costs and increase the efficiency of the energy industry, while promoting the use of renewable energy.

In addition to providing an overview of blockchain technology and its application in business, this article also highlights the challenges organisations face when using blockchain technology. Many of these problems are based on theory and literature considering similar effects. This is the first article to clearly and concisely describe the challenges specific to supply chain technology as well as the challenges for blockchain. The challenges to blockchain adoption on-chain have demonstrated that there are many issues affecting not only the relationship between chain partners, but also the relationship between partners' employees and stakeholders. Also included are the barriers to the adoption of blockchain, most of which stem from the unknown nature of blockchain technology. In fact, given the widespread use of blockchain technology for business, it has been started and supported by some leading companies such as IBM, Boeing, Microsoft and SAP. A survey is needed to evaluate research and experimental studies and to provide useful information to support the use of blockchain. The subsequent success and failure of this process can also be addressed in future research.

5.2 Future Scope

Problems with blockchain technology may limit its use, and future research needs to pay more attention. Effective solutions to solving's scalability problems need further research. More research is needed to explore the significance of various conflicts and to determine the relationship between them. This research will form the basis for the management of blockchain usages. Blockchain technology can reduce transaction costs, expand transactions, encourage peer-to-peer transactions, and create new models for decentralised business models. This new practice has led to the emergence of financial management that uses blockchain technology to create an alternative financial system that can be more independent, innovative, shareable, borderless and transparent. Although there are still many challenges to be solved, entrepreneurs and innovators are experimenting with business models

that traditionally do not work without blockchain technology. If successful, decentralised business models have the ability to change existing businesses and create new business opportunities and innovations. Additionally, they may compel researchers to come up with new theories to explain the benefits and costs of distribution. Blockchain technology has great potential for automation, transaction processing, optimization and data protection. It can be used for many purposes. Due to the decentralised system, there is almost no capacity limit. In addition to increasing business security, blockchain can also provide users with better personal protection. Reducing employee involvement also reduces the risk of data entry errors. Trading can be done more cheaply because there is no "third party" involved. Trading is also safer as the entire system’s transparent. However, although most of the operations are simple, it requires a lot of computing time, reliable hardware, and consumes a lot of power, so it cannot be fed white.

References

[1] https://bitcoin.org/bitcoin.pdf

[2] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PLOS ONE, 11(10), e0163477. doi:10.1371/journal.pone.0163477

[3] A. Bahga, V. Madisetti, "Blockchain Platform for Industrial Internet of Things", Journal of Software Engineering and Applications, No. 9, pp. [36]533-546, 2016

[4] A. Litviņenko, A. Āboltiņš, "Computationally Efficient Chaotic Spreading Sequence Selection for Asynchronous DS-CDMA". Electrical, Control and Communication Engineering, vol.13, pp.75-80, 2017

[5] V. Buterin, "On public and private blockchains," 2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/ on-public-and-private-blockchains/

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[7]] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proofof-stake," Self-Published Paper, August, vol. 19, 2012

[8]"Hyperledger project," 2015. [Online]. Available: https://www. hyperledger.org/

[9] "Bitshares - your share in the decentralized exchange." [Online]. Available: https://bitshares.org/

[10] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," Ripple Labs Inc White Paper, vol. 5, 2014.

[11] J. Kwon, "Tendermint: Consensus without mining," URL http://tendermint. com/docs/tendermint { } v04. pdf, 2014.

[12] "Consortium chain development." [Online]. Available: https://github. com/ethereum/wiki/wiki/Consortium-Chain-Development

[13]https://medium.com/@Nonceblox_/top-blockchain-solutions-for-social-impact-6801cd29a9af

[14] Hamed Taherdoost “Smart Contracts in Blockchain Technology: A Critical Review” , Department of Arts, Communications and Social Sciences, University Canada West, Vancouver, BC V6B, Canada; doi.org/10.3390/info14020117

[15] Namasudra S., Sharma p. “Achieving a Decentralised and Secure Cab Sharing System Using Blockchain Technology”, IEEE Transactions on Intelligent Transportation Systems (Early Access), 25 July 2022; DOI: 10.1109/TITS.2022.3186361

[16] Bali, S., Bali, V., Mohanty, R.P. and Gaur, D. (2023), "Analysis of critical success factors for blockchain technology implementation in healthcare sector", Benchmarking: An International Journal, Vol. 30 No. 4, pp. 1367-1399. https://doi.org/10.1108/BIJ-07-2021-0433

[17] M. Nour, J. P. Chaves-Ávila and Á. Sánchez-Miralles, "Review of Blockchain Potential Applications in the Electricity Sector and Challenges for Large Scale Adoption," in IEEE Access, vol. 10, pp. 47384-47418, 2022, doi: 10.1109/ACCESS.2022.3171227.

[18] https://ethereum.org/en/whitepaper/

Appendices A - Frontend

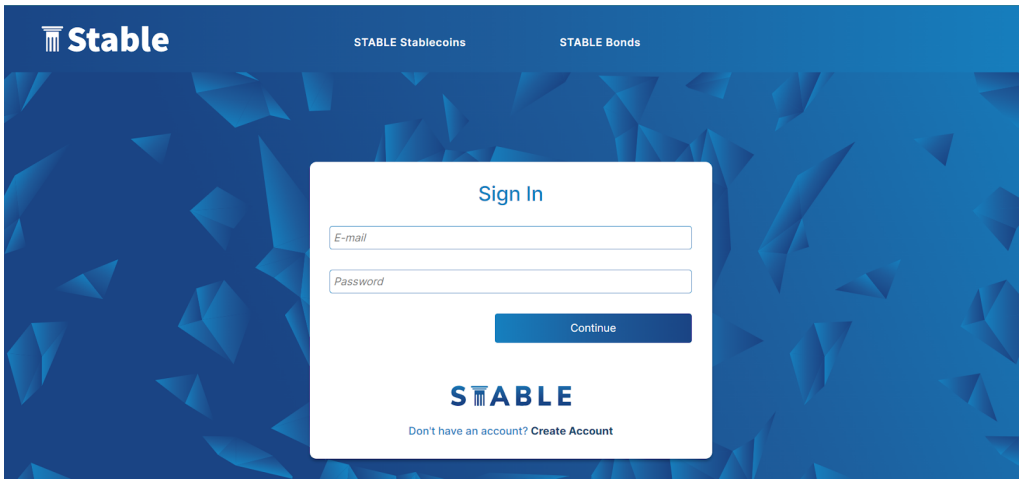


Figure A.1 Stable SignUp page

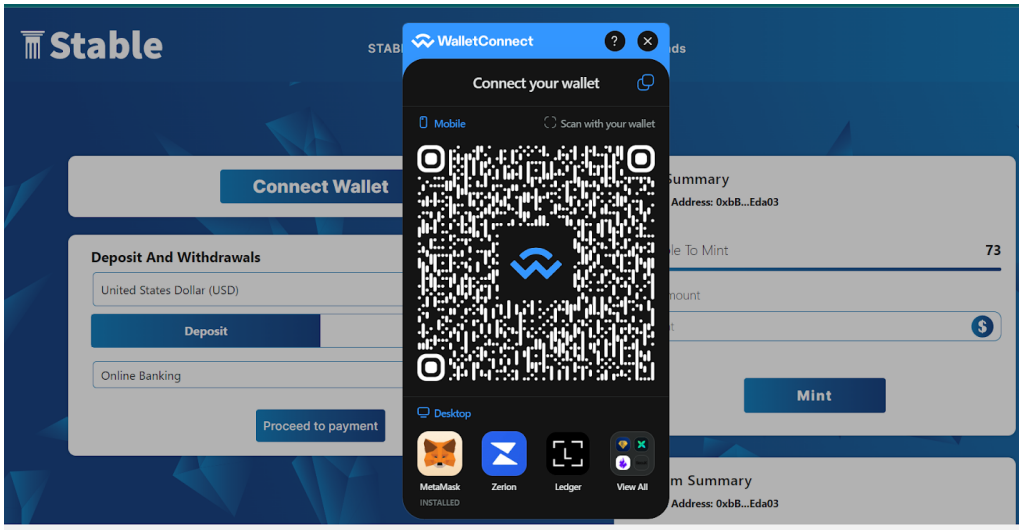


Figure A.2 Web3 Wallet connect popup

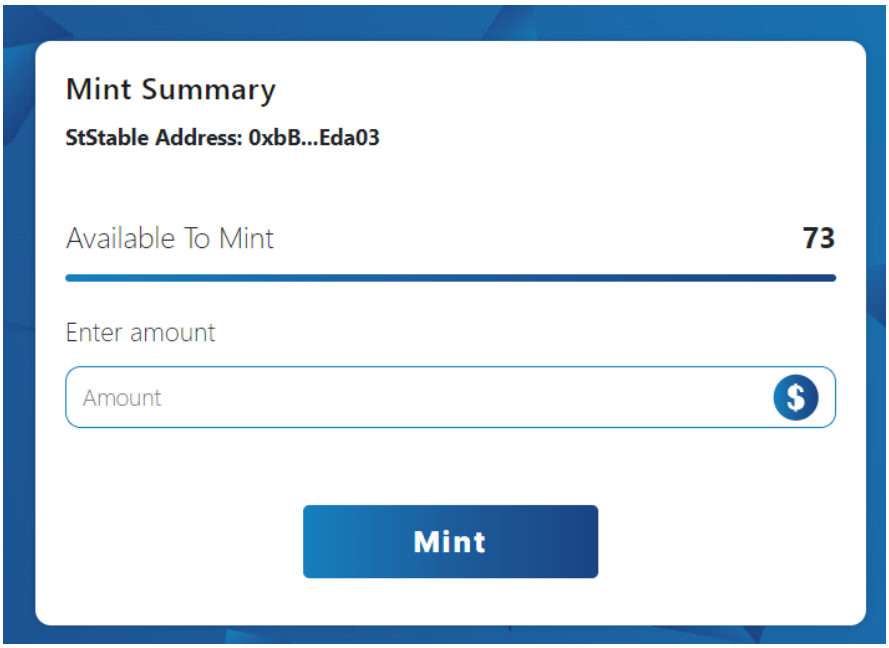


Figure A.3 Mint Redeem User Interface

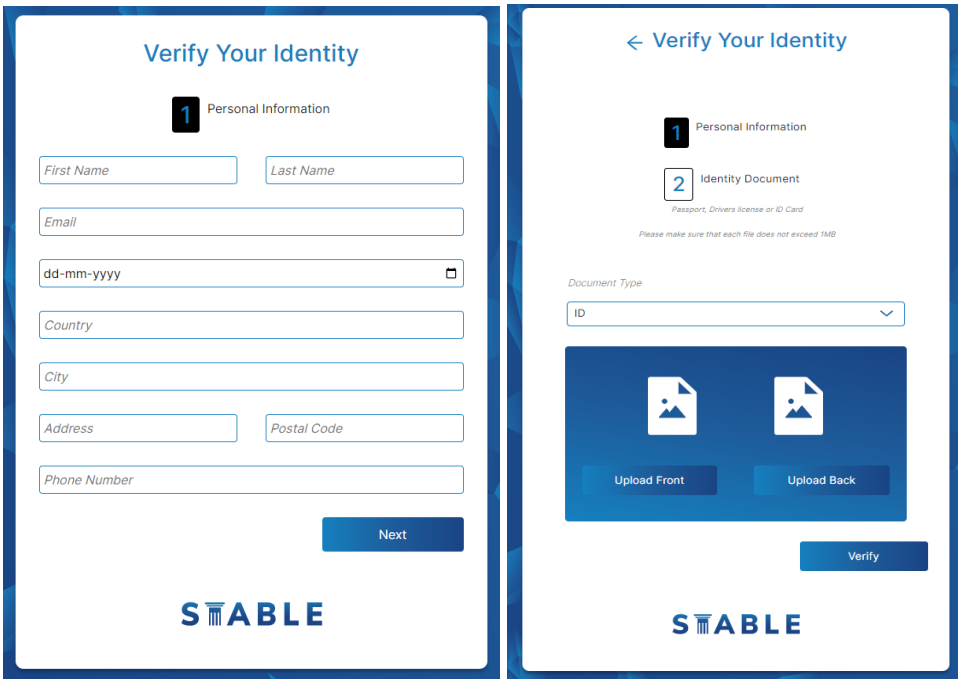


Figure A.5 Frontend Interface for Identity proof

Appendices B - Backend

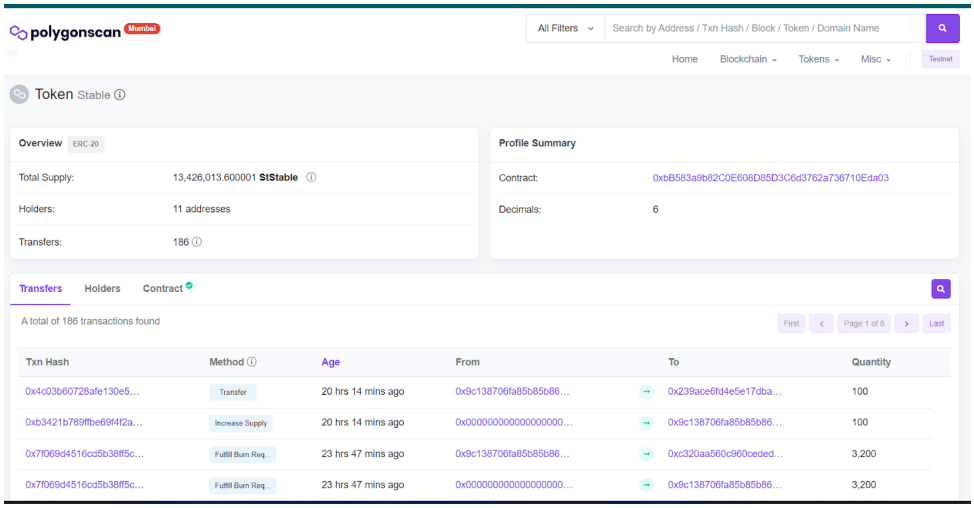

```
{
  "_id": {...},
  "password": "$2b$12$ndqvPALyEiDN.XzXDybj9elAuRPPbNBh2Ld4f.GEVqF9TwBigyXQm",
  "email": "varun@gmail.com",
  "dob": "2001-02-11",
  "address": "Kullu",
  "city": "Kullu",
  "country": "India",
  "postalCode": 175101,
  "phoneNumber": "1231231234",
  "verificationDetails": [],
  "verified": true,
  "availableFiatBalance": 73,
  "alreadyMinted": 127,
  "stGold": 0,
  "stUSTreasury": 0,
  "bankDetails": [...],
  "createdAt": {...},
  "updatedAt": {...},
  "__v": 1,
  "firstname": "Varun",
  "lastname": "C",
  "walletAddress": "0x38B151d8ed66F8a87CF73C3AC97D5D91968AE85A"
}
```


Figure B.1 User Data model

	_id ObjectId	type String	userId ObjectId	amount Int32	paymentType String
1	ObjectId('640f7124bb7cd1f5e22…	"Deposit"	ObjectId('6409cdffa2f64daf77b…	100	"ONLINE"
2	ObjectId('640f7149bb7cd1f5e22…	"Deposit"	ObjectId('6409cdffa2f64daf77b…	100	"IFSC"
3	ObjectId('640f724bd8d8881b52e…	"Deposit"	ObjectId('6409cdffa2f64daf77b…	100	"IFSC"
4	ObjectId('640f727bd8d8881b52e…	"Withdraw"	ObjectId('6409cdffa2f64daf77b…	100	"IFSC"
5	ObjectId('640f73108c922586b93…	"Deposit"	ObjectId('6409cdffa2f64daf77b…	100	"IFSC"
6	ObjectId('640f80be1d94e046a21…	"Deposit"	ObjectId('6409cdffa2f64daf77b…	100	"IFSC"
7	ObjectId('64117d23ff48b7aff31…	"Deposit"	ObjectId('6409cdffa2f64daf77b…	100	"IFSC"
8	ObjectId('64117d46ff48b7aff31…	"Deposit"	ObjectId('6409cdffa2f64daf77b…	100	"ONLINE"
9	ObjectId('64117d55ff48b7aff31…	"Withdraw"	ObjectId('6409cdffa2f64daf77b…	100	"ONLINE"
10	ObjectId('64117dabff48b7aff31…	"Withdraw"	ObjectId('6409cdffa2f64daf77b…	100	"ONLINE"
11	ObjectId('64117db8ff48b7aff31…	"Deposit"	ObjectId('6409cdffa2f64daf77b…	100	"ONLINE"
12	ObjectId('64117dc3ff48b7aff31…	"Deposit"	ObjectId('6409cdffa2f64daf77b…	100	"IFSC"

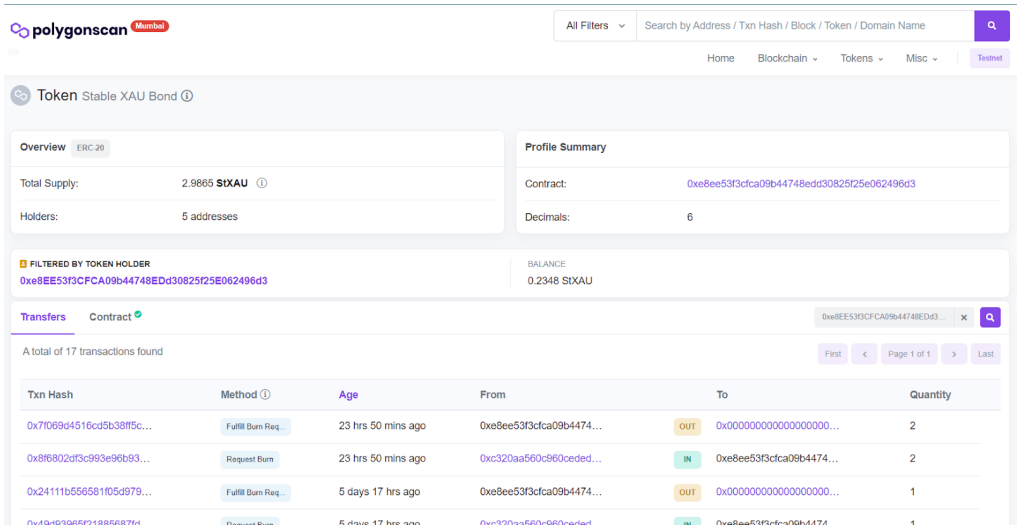
Figure B.2 Transaction Model

Appendix C: Blockchain



https://mumbai.polygonscan.com/token/0xbB583a9b82C0E608D85D3C6d3762a736710Eda03

Figure C.1 Stable Token Contract Address



https://mumbai.polygonscan.com/token/0xe8ee53f3cfca09b44748edd30825f25e062496d3?a=0xe8EE53f3CFCA09b44748EDd30825f25E062496d3

Figure C.2 Stable Staking Contract Address

Blockchain_2

ORIGINALITY REPORT

9%	6%	6%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.mdpi.com Internet Source	1%
2	www.tandfonline.com Internet Source	1%
3	Submitted to Liverpool John Moores University Student Paper	1%
4	allquantor.at Internet Source	1%
5	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	1%
6	Jay Kumar Jain, Varsha Jain. "chapter 4 A Novel Survey on Blockchain for Internet of Things", IGI Global, 2020 Publication	1%
7	Israa Abu-elezz, Asma Hassan, Anjanarani Nazeemudeen, Mowafa Househ, Alaa Abd-alrazaq. "The benefits and threats of blockchain technology in healthcare: A	<1%