Cross Banking transaction system using Multichain Blockchain systems

by

Shihab Sharar
19241007
Ishfaq Morshed
19301177
Kazi Sumaia Sadia
18301120

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
Brac University
January 2024

Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Shihab Sharar
19241007

Ishfaq Morshed
19301177

Kazi Sumaia Sadia
18301120

Approval

The thesis titled "Cross Banking transaction system using Multichain Blockchain systems" submitted by

1. Shihab Sharar (19241007)
2. Ishfaq Morshed (19301177)
3. Kazi Sumaia Sadia (18301120)

Of Fall, 2023 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on January 9th, 2024.

Examining Committee:

Supervisor:
(Member)

Dr. Md. Sadek Ferdous, PhD
Associate Professor
Computer Science and Engineering
Brac University

Co-Supervisor:
(Member)

Dr. Muhammad Iqbal Hossain, PhD
Associate Professor
Computer Science and Engineering
Brac University

Thesis Coordinator:
(Member)

Md. Golam Rabiul Alam, PhD
Thesis Coordinator
Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Sadia Hamid Kazi, PhD
Head of Department
Computer Science and Engineering
Brac University

Abstract

Money is the most common form of exchange for goods and services across the world. Ensuring that this money is kept safe and transferred to the right person has been essential ever since the concept of money has been present. In this research paper we will be introducing a new method of creating transactions using smart contracts in a permissioned blockchain to ensure secure transactions across the globe. This will not only boost security, but may also increase efficiency and reduce overall compute overhead. The framework of choice for this paper is Hyperledger Fabric (HF) as HF provides us with a permissioned blockchain capable of creating channels to facilitate multichain functionality and can utilize smart contracts to perform information exchange without a cryptocurrency requirement. Using HF also allows us to set up a hierarchical setup with unique policies as required by the system design.

Keywords: Blockchain, Hyperledger Fabric, Multichain, Channels, Cross Banking

Acknowledgement

Firstly, all praise to the Great Allah for whom our thesis have been completed without any major interruption.
Secondly, to our supervisor Dr. Md. Sadek Ferdous sir and co-supervisor Dr. Muhammad Iqbal Hossain for his kind support and advice in our work. They have both helped us whenever we needed help.
And finally to our parents without their throughout sup-port it may not be possible. With their kind support and prayer we are now on the verge of our graduation.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Current banking technology largely revolves around using Database Management Systems (DBMS) and bespoke accounting software. This makes transactions extremely slow and time-consuming. Even assuming transactions are simple, a bigger issue arises in the ability to carry out transactions with users who belong to different banks [1], [2]. There are several different protocols that verify different transactions in different manners and then allow for the transactions to take place within about 24-48 hours or even more [3] [4], [5], [1], [6], [7]. Not to mention, sending money to and from abroad is a whole new story as you need to be able to withdraw money and then send it through a company that promises a secure channel, which also requires a substantial fee for the transfer [8], [9]. All this combined makes it very cumbersome and difficult to transfer money nowadays; even with the recent developments in technology, it seems like the banking sector is still behind by quite a significant margin. To solve all these problems, we are going to research ways of utilizing blockchain technology to our benefit. Blockchains are secure means of making transactions with users with little or no intervention from a third party. Here, we will attempt to create a blockchain-based system that will not only allow users to transfer money to anyone at will but also allow them to do this quickly with little intervention from the banks themselves. With this research, we hope to cut costs on money transfers not only on a localized scale but globally as well, making it more efficient and cost-effective for the banks to manage money and also be able to provide great levels of security that come with blockchain technology.

1.1 Motivation

Our main goal is to establish such a system that allows for seamless transactions between different blockchains while also increasing effectiveness and efficiency and ensuring the security and reliability of the transactions and that they are accurate, consistent, and, most importantly, trustworthy. For any transaction, it will establish a secure way to exchange required information between two blockchains.

1.2 Problem Statement

Although several solutions have been presented over the past couple of years since Blockchains have emerged, one major problem exists that holds us back from com-

pletely being able to utilize blockchain technology for banking transactions. This is the ability to trade between people who remain disconnected due to the existence of multiple banks. The problem is that every implementation till now talks about how we can create blockchains that will allow for basic transactions, ones between peers of the same blockchain, and this does not include communicating with a peer which is not present in the blockchain itself.

1.3 Research Objectives

Our primary objective is to create a system where two blockchains can perform any form of transaction or establish a method of communication between themselves to be able to perform transactions between users of the two blockchain systems. This should be done both reliably and securely. The objectives of this research are as follows:

i Exploring the effectiveness of a multichain blockchain system having the ability to decrease the transaction cost, improve efficiency, and reduce the risk of counterfeit financial instruments/transactions while enhancing asset verification in banking processes.

ii While investigating the challenges and limitations associated with integrating a multichain blockchain system into existing banking infrastructure, explore the interoperability of different blockchain networks within a multichain system along with assessing its impact on cross-border banking transactions.

iii Evaluate the potential impact of a multichain blockchain system on reducing fraud and minimizing operational risks in banking processes including implementation of a blockchain system to ensure secure transactions between users, ensuring that the process is scalable so that the process can be shipped out for public use.

iv Investigate the challenges associated with integrating a multichain blockchain system with legacy banking systems and infrastructure and assess potential solutions and strategies for overcoming these challenges.

1.4 Structure

In Chapter 1, we provided a concise overview of the deficiencies within the existing system and outlined the objectives of our research. Chapter 2 delved into the background of blockchain technology, encompassing fundamental concepts crucial to our study. Chapter 3 entailed a comprehensive comparative analysis between our work and existing publications. Our proposed model was introduced in Chapter 4, where we presented a detailed exploration of its macro-level system design. Chapter 5 delved deeper into the intricacies of our proposed model's implementation, offering a comprehensive breakdown of various use cases with a detailed protocol flow. Chapter 6 concentrated on a thorough analysis of the system requirements concerning the study's objectives, elucidating the benefits, limitations, and potential future scopes of our research. Finally, Chapter 7 underscored the significance of our methodology, providing a concluding discussion to encapsulate the essence of our paper.

Chapter 2

Background

2.1 Blockchain

To begin with, let us look at what Blockchain Technology really is all about. A blockchain is essentially a method of storing transactions in the form of a ledger. These transactions and assets can be tracked. Transactions are stored as records, which we call record blocks. To keep these blocks secure, we hash these blocks, and similar to a linked list, we add the previous block's hash to the new block created. This chain-like connection of blocks is what gives it the name Blockchain. Due to the hashes, we can ensure that blocks cannot be altered, as any change will be reflected in the chain when the hashes are recalculated and compared. Thus, Blockchains tend to be very difficult to manage when a change is needed in a previous block. This is usually resolved by creating a new block that can reverse the issues faced while creating the previous block. A Blockchain consists of a P2P network where the devices maintain a distributed ledger system containing the details of the transactions. Although a P2P network, due to the design of the blocks, it is possible to easily find any asset in the network by going up the chain.

2.2 Interoperability of Blockchains

Interoperability of Blockchains generally talks about how we can bring together different blockchains and make them interact with each other in ways that will be beneficial to us. Interoperability can operate on different layers (the explanation can be compared to how the internet has several layers on which it operates, only this is less diverse and more specific on how malleable the integration is between the different layers due to the complexity, technical, and semantic interoperability is mostly the point of focus). The layers that are in the scope of this paper are as follows -

- Technical interoperability - This refers to the mechanisms by which there is an integration between blockchains in a technical manner.
- Semantic interoperability - This refers to methods by which the data integrity and its state is conserved while performing an interoperability transition between blockchains.

The purpose of interoperability is not solely to provide portability between different applications and allow for flexibility, but interoperability also allows for better scalability, higher efficiency, and better privacy.

2.3 Blockchains and how they work

The term blockchain refers to one of two meanings: a data structure and a system. We mostly refer to blockchain as a system of distributed nodes. Here computers are on a P2P network, each in an effort to perform transactions and document it in a distributed ledger system. We call it a distributed ledger because no one computer holds the ledger. Every device is involved in maintaining and storing it with the required storage and computational resources. These nodes are not always trusted to keep data safe, so the ledger is stored in all the nodes to make sure they are all the same. This is trusted due to the number and diversity of the nodes present which makes it trustable. Programs are usually given smart contracts, which are used to make transactions by making specific calls. These smart contracts are run inside a special environment known as a Virtual Machine (VM), e.g. Ethereum Virtual Machine (EVM). Tokens are implemented by using the aforementioned smart contracts. These are objects (or blockchain abstractions) that can be owned and have a known value (an exchangeable object such as currency). Token formats include - ERC-20, ERC-721. There are 2 types of tokens -

- Fungible - These are tokens that can be exchanged for an asset that generally belongs to the same type.
- Non-Fungible - These tokens tend to be unique, and they have properties that are specific to themselves.

Blockchains can be formed by combining the transactions from different blocks. These blocks contain a hashed value of the previous block present in the chain, allowing it to be properly traced back and forming a chain (hence the name blockchain). This makes blockchains unchangeable after a certain transaction, a change will require the re-calculation of all the hashes in the following transactions in the chain. This also ensures that the transactions are left untouched and haven't been tampered with, as changing even a single bit in the whole block would cause the hashes to fail to match. Due to the nature of distributed ledger systems, they have to be very resistant against faults, such as being Crash Fault-tolerant or Byzantine Fault (some nodes provide false information) tolerant. Consensus algorithms are important as they help us identify which data is correct in situations where Byzantine faults occur.
Proof of Work (PoW) is a major role player in terms of consensus algorithms as this allows peers to be approved for a certain transaction after a certain cryptographic hash challenge has been completed. The PoW is not a means of making sure that the node is verified, but more importantly, it is a method of making the cost and resource requirement per transaction heavier so that people are not interested or don't find it useful to run malicious nodes. One important note is that the PoW hash is usually asymmetric, where it is difficult for the peer to complete the hash but very easy for the verifier to make sure that the hash received is correct and valid. An example of another Byzantine Fault Tolerant system - Tendermint's Hyperledger

Fabric - Uses the concept of setting a small group of nodes as endorser peers who can use Crash Fault Tolerant consensus, allowing lower computational requirements while others perform full (Crash+Byzantine) consensus. This allows the verification of blocks to be easier while maintaining the ease of transactions.

- Permissionless (PUBLIC) Blockchains - No authentication from peers required, anyone can contribute to and access the ledger. e.g., Bitcoin and Ethereum.
- Permissioned (PRIVATE) Blockchains - Authentication required. Peers are held responsible as there is a governing system to decide which peers have performed the calculations properly. eg. Hyperledger Fabric, Corda, Quorum, Tendermint, Multichain.

The encryption, storage, and networking layers provide a way for the consensus to be verified. This allows the transactions to be approved, and this is added to the blockchain. Hyperledger Fabric is based on endorsement policies and is thus quite modular. In Bitcoin, nodes are incentivized to produce trusted blocks of transactions because blocks are expensive, and Bitcoin is received as a reward. On the contrary, in Hyperledger Fabric, business incentives are provided, and nodes are punished according to governing rules. One very important concept is decentralization, where unique goals and incentives allow the blockchain to be run by parties without the need for a trusted centralized party. Decentralized Application (dApps) is a piece of software that runs on a decentralized P2P network. These are based on a blockchain design but also have other decentralized components that allow it to function.

2.4 Cross-Blockchain Communication (CCC)

To perform cross-blockchain communication, there have to be two chains present: a source and a destination blockchain. General purpose interoperability takes place following a simple 3-step procedure

- Locking (extinguishing) of the smart contract on the source blockchain - Stopping any form of transactions from happening and securing its current state.
- Blockchain transfer commitment - confirming that the conversion/transfer will take place.
- Creating a representation of the asset on the specified destination blockchain.

Cross-Chain Communication Protocol (CCCP) is a method by which two blockchains can perform transactions across two chains properly, this allows homogenous blockchains to be able to communicate.
Cross-Blockchain Communication Protocol (CBCP) - A method using which two blockchains can perform cross-blockchain transactions properly; this allows heterogeneous blockchains to be able to communicate.
CCCP requires the two blockchains to be of the same type, following similar protocols or having the same constructs, while CBCP uses an additional translation process to allow for one blockchain to be implemented/communicated with another while using completely different structures/protocols. The biggest problem with any form of CCC is the fact that a third party is always required to ensure that the

consensus algorithm can provide adequate tolerance against misbehaving nodes for both centralized and decentralized systems.
Cross-Chain Transactions (CC-Tx) - transaction in-between blockchains of the same blockchain system (homogenous blockchains), e.g., EVM-based blockchains.
Cross-Blockchain Transactions (CB-Tx) - a transaction between blockchains of the different blockchain systems (heterogenous blockchains), e.g. Hyperledger Fabric and Bitcoin.
CC-Tx and CB-Tx are usually used synonymously and mostly refer to CC-Tx systems as that is the common use case in the blockchain industry.
Cross-Chain Decentralized Application (CC-dApp) - This is a dApp that utilizes CC-Tx to make use of inter-blockchain transactions/conversions in a practical manner. CC-dApps and CB-dApps are used interchangeably. They are also known as inter-chain decentralized applications or inter-blockchain decentralized applications.
Internet of Blockchains (IoB) - This is when homogeneous and heterogeneous decentralized networks communicate to allow for cross-chain transactions [2].
Blockchain of Blockchains (BoB) - the structure that brings together blocks from different blockchains into "meta blocks," that is organized with the help of a consensus mechanism using posets (partially ordered sets) and total order theory [10].
Here, we can see that CC-dApps can be used for semantic interoperability, and this would require the presence of the BoB approach. The BoB approach, on the other hand, requires the presence of an IoB approach and thus requires the technical interoperability layer to be able to assist in the successful completion of proper semantic translation from one blockchain to the other, which is most sought after. In the case of CC-dApps, it is all maintained by a protocol called the CC-dApp protocol that makes sure that transactions are completed and have been carried out in the manner it holds meaning semantically for both heterogeneous and homogenous blockchains.
There are 3 major approaches to interoperability between blockchains -

i **Public connectors**

Mostly devised to enable interoperability between cryptocurrencies [11]

i Sidechains and Relays - Sidechains are mechanisms for 2 existing blockchains to be able to interoperate [8], [12], [13], scale [14] and upgrade [15], where a blockchain will make itself the sidechain or extension to another sidechain. The primary chain keeps track of the assets in a ledger, and the sidechain is attached to the main chain via a cross-chain communication protocol. Main chains can also be side chains of other main chains, which will allow both chains to connect to other side chains. Layer-0 is usually the main blockchain, while side chains are considered Layer-1. Layer-2 can be further side chains similar to having a branching tree structure, this layer will usually handle off-chain transactions between users by having messages sent back and forth between the directly connected chains, meaning that the lower layers will act as methods of off-loading transactions from the upper layers (main chain). Communication between different chains occurs via a CCP.

ii Notary Schemes - Notary schemes allow one chain to get information regarding another chain's state or transactions. This system allows for chain A to be able to process a transaction depending on the state of chain B, such as a certain transaction being complete on chain B. This is a great method to be able to gate-lock transactions, one behind the other.

iii Hashed Time-Lock Contracts - This form of contract is where a chain is hash-locked and time-locked until another transaction is complete on a separate chain. If the transaction fails, the chain is released with no transaction performed. If the transaction succeeds, the transactions are rightfully updated and the lock is released.

ii Blockchain of Blockchains

iii Hybrid Connectors

i Trusted Relays

ii Blockchain-Agnostic Protocols

iii Blockchain Migrators

2.5 Hyperledger Fabric

The Hyperledger [3] initiative of the Linux Association is responsible for creating the well-known blockchain-based system Hyperledger Fabric. It is intended to make it easier to create blockchain solutions that benefit businesses that include aspects like anonymity, flexibility, scalability and adaptability. As an authorized blockchain technology, Hyperledger Fabric necessitates that users get explicit authorization before they register or sign in as well as engage with the network.
Why we are using Hyperledger Fabric in our Model :

i **Scalability:** As Hyperledger Fabric is designed to scale effectively, it can manage the kind of intricate and extensive financial transactions that our three-layer banking infrastructure would be expected to deal with. Simple adaptability as the range of transitions and users rises is made possible by its lightweight construction.

ii **Privacy and confidentiality:** We may establish distinct channels for various transaction circumstances (e.g., local and international transactions). Hyperledger Fabric's channel-based privacy feature allows it to do so. In this case, confidentiality and regulatory compliance are improved since only the pertinent parties may observe and access the data.

iii **Permissioned Network:** A permissioned network, for instance, the Hyperledger Fabric, secures that only those who are authorized parties, including central banks, banks can access the network's chains and conduct transactions since our concept incorporates a hierarchical framework that has multiple tiers. The following improves system management and confidentiality.

iv **Smart Contract:** Hyperledger Fabric is compatible with smart contracts or chain code as fabric refers to it. Rules are enforced throughout transactions and company procedures may be automated with smart contracting. This functionality fits in nicely with the goal of our plan, which is to create a blockchain-based banking structure that allows for secure, encrypted, and reliable transactions.

v **Identity Management:** Strong authentication and authorization capabilities offered by Hyperledger Fabric that allow users to have authorized and validated credentials on the system. The following lowers the possibility of fraudulent activity and assures secure conditions for finances.

vi **Interoperability:** The seamless integration of Hyperledger Fabric enables it to interface with databases alongside additional networks which may be vital to integrating our suggested banking framework with current banking structures.

vii **Comprehensive Documentation and Support:** With an extensive library of instructions, records, and assistance from the community, Hyperledger fabric helps both developers and companies better comprehend, apply, and manage blockchain networks.

viii **Consensus Mechanism:** Since Hyperledger Fabric offers a variety of decentralization techniques, you may select the system for consensus that best suits the needs of any transactional situation in our proposal.

In a nutshell, the blockchain framework Hyperledger Fabric works seamlessly with our suggested three-layer bank design. The efficiency, scalability, smart contracts, identity management, and the other above-mentioned characteristics are a few of its properties that make it a good fit for a secure and effective financial system. In addition, the architecture's consent and interoperability processes offer the flexibility necessary to accommodate a range of transaction situations.

2.6 Financial System

In the Bangladesh banking industry, a wide range of institutions, marketplaces, and intermediaries help currency move between depositors and lenders. It is necessary to allocate finances, utilize savings, and promote the country's economic growth. The key components of Bangladesh's banking system are as follows :

i **Banking Sector:** An essential component of Bangladesh's financial system is the banking sector. It is made up of a variety of banks, including foreign, specialized, and commercial banks. To ensure stability and effectiveness, the Bangladesh Bank, the nation's central bank, controls and monitors the banking sector and develops monetary policies.

ii **Microfinance Institutions:** Microfinance organizations have become more well-known in Bangladesh, particularly in rural regions, by providing financial assistance to low-income individuals and owners of small enterprises who do not have the opportunity to use standard banking facilities.

iii **Capital Market:** Businesses may acquire money by trading bonds and stocks on the stock exchanges in Bangladesh which comprise the nation's capital marketplace. Two major markets are the Dhaka Stock Exchange (DSE) and the Chittagong Stock Exchange (CSE).

iv **Non-Bank Financial Institutions (NBFIs):** NBFIs in Bangladesh consist of merchant banks, mutual funds, leasing businesses, and insurance companies. These companies play a critical role in providing different financial services to different demographic groups.

v **Government Bonds and Securities:** The government of Bangladesh distributes contracts and securities to generate funds for different infrastructure initiatives and to regulate its fiscal concerns.

2.7 Banking System

The banking system of Bangladesh is an important component of the economy structure of the country. This is made up of several types of banks. The fundamental elements of the financial structure are as follows :

i **Commercial Bank:** The biggest participants in the banking sector are commercial banks. Commercial banks provide several kinds of financial services to individuals, businesses as well as governmental entities.In addition to offering a number of load products and financing for trade. Moreover they take deposits along with offering other banking services.

ii **Foreign Banks:** The activities of foreign banks in Bangladesh are governed by the rules and regulations of the Bangladesh Bank. They not only make trading internationally easier but also provide businesses who are involved in it with specialist support services.

iii **Specialized Banks:** Many specialist banks in Bangladesh serve certain business sectors, including foreign commerce and trade, manufacturing finance, and agricultural expansion. Banks like these are essential to the development of certain industries in the economy.

iv **Central Bank:** The Bangladesh Bank serves as both an industry-specific central bank and its administrative agency. It creates and carries out monetary policy, prints money, oversees banks, and controls the nation's foreign exchange reserves.

v **Rural and Microfinance Banks:** "Rural and microfinance banks" are financial institutions that focus on offering economic assistance for entrepreneurs of micro-businesses and rural communities. These organizations promote rural growth and financial empowerment.

Overall, Bangladesh's banking and financial systems play a critical role in fostering economic expansion, directing savings toward profitable ventures, and offering fundamental financial services to citizens and businesses nationwide.

2.8 Traditional techniques

There are key electronic payment systems and facilities in Bangladesh. These systems play a crucial role in facilitating various types of financial transactions, improving efficiency, and promoting a cashless economy in the country. Here's a summary of the mentioned systems:

i **Bangladesh Automated Cheque Processing Systems (BACPS):** This system uses Cheque Imaging and Truncation (CIT) technology to electronically process paper-based instruments like cheques, pay orders, warrants for refunds along with profits, etc. It resolves transactions submitted within the day at pre-fixed times employing batch processing methods.BACPS handles both High-Value (HV) Cheque Clearing (cheques of Tk. 5,00,000 or above) and Regular Value (RV) Cheque Clearing.

ii **Bangladesh Electronic Funds Transfer Network (BEFTN):** Introduced in February 2011, BEFTN is the country's first paperless electronic inter-bank funds transfer system. It enables credit and debit transactions for various payments, including payroll, remittances, bill payments, corporate payments, government taxes, and person-to-person transfers.

iii **National Payment Switch Bangladesh (NPSB):** Operational since 2012, NPSB has established interoperability among participating banks for account and card-based transactions. It facilitates interbank ATMs, Point of Sale (POS), and Internet Banking Fund Transfer (IBFT) transactions, allowing cash withdrawal, balance inquiry, fund transfer, and mini statements through interbank ATMs. NPSB also mandates Two-Factor Authentication (2FA) for online, e-commerce, inter-banking, and card-not-present transactions.

iv **Real-Time Gross Settlement System (RTGS):** Introduced in October 2015, the Bangladesh Real-Time Gross Settlement (BD-RTGS) system enables real-time settlement of high-value, time-critical payments. It allows banks and corporations to instantly settle large-value transactions, providing efficiency and security.

Overall, these electronic payment systems have contributed to the advancement of Bangladesh's financial infrastructure and have had a significant impact on modernizing the country's banking and payment processes.

Chapter 3

Literature Review

In [4], the authors introduced a banking system using Ethereum blockchain technology. The idea is great as the transactions between users are secure and require no intervention from a third party. Transactions are secure due to the use of asymmetric key encryptions present while carrying out the transaction using smart contracts; this means there is less use for the bank server, and thus, the whole system is more efficient as a whole. In addition to that, due to the use of blockchains, all transactions are stored in chronological order and with timestamps. With all transactions being authenticated properly, fraudulent activities are avoided. The only problem mentioned by the authors is that there are no methods of providing loans to the users present in the system.

Rahman et al. suggested using blockchain technology to reduce banking costs and to constantly coordinate and verify data [16]. Due to the nature of their business, banks must regularly update their data, but doing so takes a long time. Additionally, the current banking system is not ideal because customers must pay significant fees to banks. As a result, they suggested a blockchain system that increases financial system efficiency while cutting expenses. They also suggested that banks might get more income through the adoption of blockchain technology since there are new business models and goods on the blockchain. One of the main advantages of blockchain technology over traditional banking systems is the speed and low cost of transactions, particularly for international transfers and small payments. In order to minimize costs and streamline operations, it is thus possible to automate processes and also keep all operations traceable; blockchain will maintain a level of confidence among all parties.

In [17], Satoshi Nakamoto put out a concept for a peer-to-peer network and electronic money in this paper. The author essentially broke this down into a few parts, such as new transactions being broadcast to all nodes before they are collected by each node into blocks. Nodes will only accept a block if all of its transactions are genuine and have not yet been spent. The author of the paper placed a strong emphasis on security and utilized mathematical calculations to support it. Online payments can be sent directly between parties using this peer-to-peer network without going through a bank or other middleman. This establishes the framework and foundation for Bitcoin, the most popular blockchain application.

In [18], The Author discussed the value of Know Your Customer (KYC) and blockchain in the financial sector. The goal of KYC is to know each consumer thoroughly. It's crucial to ensure consumer validity in order to uphold anti-money laundering laws.

The author here introduced blockchain, which enables banks to securely share customer information across the organization and streamline administrative processes by reducing duplicate information. Blockchain also allows for the creation of a single non-editable KYC record and independent access to one client's verification by one bank by other banks. Because cryptocurrencies are decentralized and growing daily, there are more opportunities for money laundering and financial terrorism, which is where KYC comes into play.
Zhang P. et al. mentioned how we can use different methods of optimizations to make it easier for healthcare service providers to manage data more efficiently [19]. These include -

i maintaining evolvability while minimizing integration complexity,

ii minimizing data storage requirements,

iii balancing integration ease with

iv security concerns, and

v tracking relevant health changes across large patient populations

They conducted a Case Study on DASH (DApps for Smart Health) to apply the ideas. Their concepts mostly revolved around reducing the complexity between transactions and reducing data overhead for the transactions to make it easier, as this form of exchange didn't require excess information.
Li, W. et al. introduced a novel method of connecting what they call satellite chains [9]. These chains are all connected via a single larger chain, and as long as the satellite chains are satisfying the consensus enforced by the main chain, they can independently perform transactions inside the blockchain (satellite chains), and later send necessary details across the main chain. This is a revolutionary concept as this allows for the satellite chains to use any blockchain technology, which complies with the consensus requirements from the main chain and allows all cross-communication between the satellite chains.
In [5], The author Pillai, B. wrote an amazing paper mentioning the use of a theoretical two-blockchain communication system that would allow for extremely fast transactions between two blockchains containing the sender and receiver, respectively. This is achieved by allowing the two blockchain systems to communicate on a simple software level without needing consensus from each other, as it is assumed that the communication is occurring between blockchains that are completely aware of each other and trust each other (pre-verified). This allows for much faster transactions without a PoW system and allows different blockchains on different platforms (e.g. Bitcoin, Ethereum, Hyperledger Fabric, etc.) to communicate effectively.
The importance of value systems in connection to investment choices within the setting of blockchain technology is highlighted in this research [20]. The author suggests a blockchain-based automatic value system concept. User information API, Smart contract API, and Distributed Ledger API are used to categorize the model. Investors are able to estimate the stock fairly, thanks to it. Essentially, this new blockchain-based system has three layers. They are the creation of value, recording of value, and valuation of value. The investors will be guided by this approach to make rational investments and obtain the best results. This model will be highly

beneficial for investors since it will allow them to see what they are investing in and what can happen as a result, which will help them play their game more effectively. Owing to this blockchain technology concept, investors will have more faith in the banking industry.

Chapter 4

Proposal

The structural layout of the system (as shown in Fig.4.1) resembles a hierarchical tree diagram composed of three distinct layers, each intricately supported by its dedicated blockchain network. Positioned at the zenith of this hierarchy is the central bank, serving as the pinnacle of the financial infrastructure, occupying the highest stratum labeled as TIER 1. Within this top tier, exclusive access is granted solely to the central bank's management and operational entities, delineating its paramount role in overseeing the overarching financial system.
Moving down the financial hierarchy, the secondary layer, Tier 2, contains the variety of banks that operate in particular national regimes. That layer of blockchain, which is nested beneath Tier 1, acts as the link between these financial institutions, conducting financial interactions between banks along with encouraging joint ventures; this middle level is essential to coordinating the smooth movement of financial operations across specified jurisdictional constraints.
The final level, Tier 3, is located further beneath the hierarchical structure and forms the foundation of the mechanism's structure. Tier 3 consists of unique specific individuals and their respective corresponding identities. It establishes an immediate link among all users along with a single blockchain where each user acts as a distinct leaf node throughout the whole system's infrastructure. It is important to remember that banks are situated in two different tiers of the blockchain network hierarchy: they are linked to Tier 3 blockchains and are located in Tier 2. Through this framework, banks may communicate directly with particular users and execute interbank transactions while improving efficiency and making it easier for the financial environment to function as a whole.
This layered blockchain paradigm serves as a strong basis for an interconnected and sustainable banking infrastructure in addition to establishing a disciplined and systematic method for conducting financial transactions. In the end, it fosters a unified and functional financial environment by guaranteeing efficient lines of interaction, securing transactions, and optimizing the exchange of data across users, local banks, and central banks.

4.1 Threat modeling

Threat modeling is an organized process for locating as well as mitigating possible risks to a mechanism or application's vulnerability. It compromises thoroughly analyzing the system to identify any vulnerabilities and determine the probability and

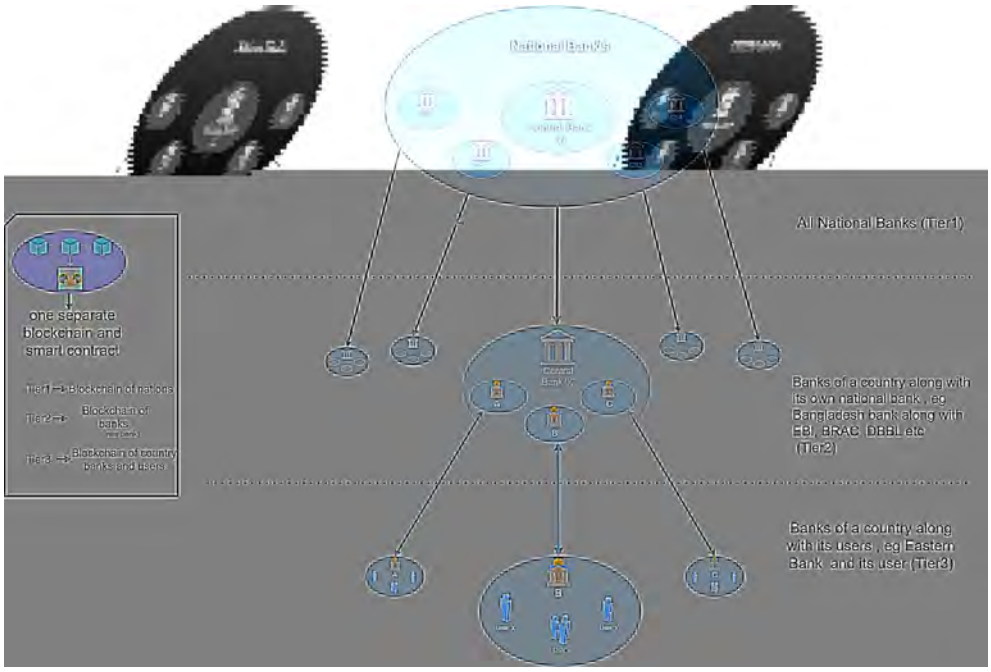

Figure 4.1: 3 Layer Bank Model

effect of different attacks. In his book "Threat Modeling: Designing for Security," Adam Shostack [21] outlines a popular method for threat modeling. The STRIDE threat detection and categorization approach is divided into six main categories: spoofing, tampering, repudiation, disclosure of information, denial of service, and elevation of privilege. Here is a brief overview of every STRIDE classification based on our model below :

4.1.1 Security Threats(T)

- **T1 - Spoofing Identity:** An attacker pretends to be a reliable user of the blockchain banking network. Spoofing is the practice of attempting to pose as an authorized user on the blockchain network, which can be detrimental. This may form attempts to change transactions or obtain confidential financial data using hacked or fake login credentials. (e.g., An attacker may try to impersonate a bank client in order to access their account or carry out illegal activities).

- **T2 - Tampering with Data :** An attacker may attempt to manipulate financial transactions to create an impact on the infrastructure's integrity and threaten the infrastructure.

- **T3 - Repudiation:** An attacker might retract their involvement in certain invalid and forbidden activities relating to a financial transaction in the banking system.

- **T4 - Information Disclosure:** Vulnerabilities in the system's security or any deficiencies while exchanging confidential information may cause the data to be released maliciously to an attacker.

- **T5 - Denial of Service(DoS):** Refers to the probability of an attacker causing disruption to the standard functioning of the system due to malicious activities to execute the transactions without the consent of authorized users.
- **T6 - Elevation of Privilege:** Elevation of Privilege refers to the potential for an unauthorized individual to attempt to gain elevated privileges within the blockchain-based banking system, potentially manipulating or accessing sensitive functions or data.
- **T7 - Replaying Transactions:** By recording an old financial transaction and transmitting it repeatedly at subsequent times, an attacker may try to execute a replay attack. As a result, the same amount of money could be transferred twice, launching a replay attack.
- **T8 - Misuse of System Resources:** Excessive and unnecessary utilization of the system's processing resources might arise in a multichain blockchain-based banking system. For instance, users may create frequent queries for insignificant targets, either accidentally or intentionally putting an undue strain on the system's computational resources.

The lack of user-executed privacy controls is the main cause of the emergence of privacy threats. The threats that have been identified in this situation can be broken down as follows:

- **T9 - Lack of control and Transparency:** This lack of control and transparency refers to the obstacle of ensuring that everyone on the network receives equivalent rights to access the data and the decision's managerial legitimacy despite ensuring the confidentiality and security of financial transactions.
- **T10 - Lack of Consent:** This means that without the consent of a user, a transaction is being carried out. For example, a transaction has occurred where someone has accessed or modified a user's private data without their consent.

By considering these STRIDE threat categories, the threat modeling process can identify potential vulnerabilities and guide the development and implementation of appropriate security measures to protect the advanced banking system using Multichain Blockchain systems.

4.2 Requirement Analysis

4.2.1 Functional requirement (FR)

Functional requirements specify the processes and actions that the system must carry out in order to fulfill the demands of users and stakeholders. This comprises account setup, cash transfer, transaction verification, smart contract execution, and secure financial data storage. Functional criteria guarantee that the system runs effectively, safely, and in accordance with banking rules, taking advantage of the possibilities of multichain blockchain technology.

- **FR1:** The system shall provide a multi-chain blockchain architecture to support the creation of interconnected blockchains.
- **FR2:** To perform interbank transactions, each regional bank in Tier 2 will have its own blockchain.
- **FR3:** To facilitate regional activities and transactions, all local banks in the Tier 3 layer will have their own blockchain.
- **FR4:** To facilitate secure and reliable processing for transactions, the infrastructure will employ Proof of Work (PoW), methods, and smart contracts designed on top of Hyperledger Fabric.
- **FR5:** A reliable credential management framework that utilizes KYC procedures over authentication will allow users in the blockchain system to authorize participation.
- **FR6:** Transaction processing functionalities shall include funds transfer, account management, transaction history, and balance inquiries.

4.2.2 Security Requirements (SR)

Security requirements in an advanced banking system using multichain blockchain entail measures to protect sensitive information, prevent unauthorized access, ensure transaction integrity, and comply with regulations. They include user authentication, data encryption, secure key management, transaction auditability, fraud protection, and adherence to regulatory standards. Security requirements are essential for maintaining system security, building user trust, and safeguarding the banking ecosystem.

- **S1:** This should be ensured by the system that whenever the users try to access the data in the blockchain, they should be authorized, and only then can they access the data; otherwise, it will not allow them to access the system. This mitigates T1 and T6 threats.
- **S2:** To establish a layer of isolation between distinct users, a secure process will be preserved for every signed-in user.So that any user will not be able to access another user's data. This mitigates T1 and T2 threats.
- **S3:** To discourage users from DoS, the system must implement precautionary steps regarding potential DoS attacks that might occur. This mitigates the threat of T5.
- **S4:** The framework must implement preventative assessments concerning replay attacks of any. This mitigates T7 threat.

4.2.3 Privacy Requirements(PR)

- **P1:** The infrastructure is obligated to make sure that no transaction will be completed without the user's consent. This mitigates the T10 threat.

- **P2:** It must be ensured by the system that the absolute authority throughout each and every transaction of theirs will be the user's. This mitigates the T9 threat.

4.3 Architecture

Our proposed bank architecture follows a three-layer structure, depicted in Fig.1, which was created to support various transaction types. We identify three distinct transaction scenarios within this architecture:

- Transactions between users within the same bank.
- Domestic transactions between two different banks in the same country
- International transactions spanning multiple countries

Three distinct tiers make up the architecture, each of which has specific functional levels. The central banks' blockchain infrastructure is located at the top tier, also known as TIER 1. When we reach TIER 2, a national bank that is also a policymaker is present. Finally, in TIER3, each bank has its own blockchain network.

i In Fig.4.2, we see transactions between users within the same bank.

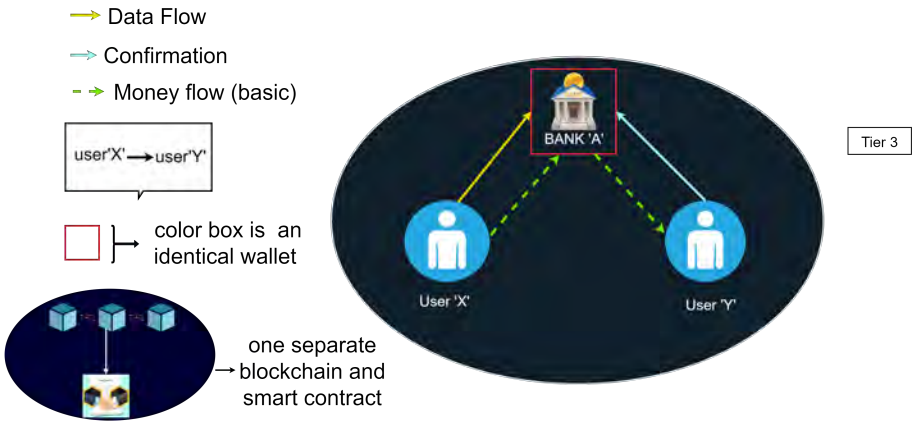

Figure 4.2: Same bank transaction

In this transaction architecture, we take into account a scenario in which Users X and Y are both customers of the same bank. The procedure used in this transaction is reasonably simple and effective. User "X" requests the transaction from their respective bank to start the transaction. The bank then carefully examines and validates this request to make sure User Y is the rightful recipient. Upon confirmation of validity, the bank either authorizes or rejects the transfer of funds from User "X" 's account to User "Y" 's account. The internal systems and protocols of the bank facilitate quick and secure execution of everything.

ii In Fig.4.3, we see Domestic transactions between two different banks in the same country

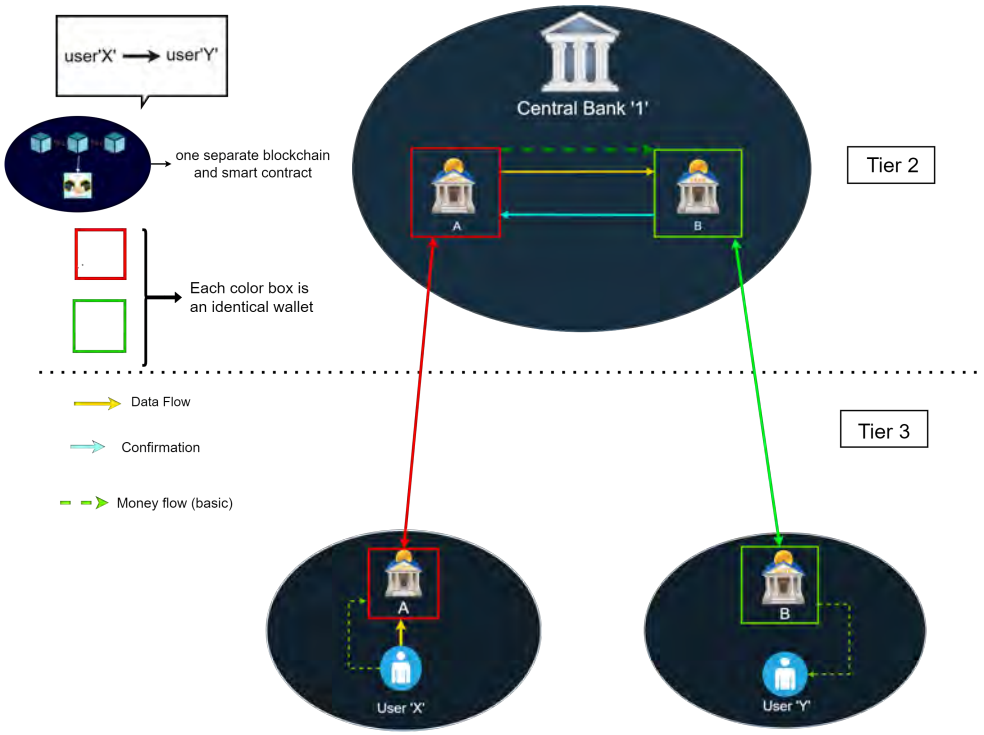

Figure 4.3: National transaction

We take into account a scenario where User X wants to send money to User Y within the same nation when analyzing the domestic transaction architecture. The transaction is started by User X sending a request to their respective bank, which we will refer to as "Bank A". When "Bank A" receives a transaction request, it transfers it to "Bank B". As the recipient bank, "Bank B" receives the transaction details from "Bank A" and verifies the transaction's validity and the recipient's accuracy as needed. Then, using the same network of middlemen, "Bank B" transmits a confirmation signal back to "Bank A". The money is either transferred or rejected after the transaction is completed in accordance with the confirmation that was received.

iii In Fig.4.4, we see International transactions spanning multiple countries:

In the international transaction architecture, we consider the case of a money transfer between users X and P, who are situated in different nations. The process starts when User X, who is located in a Country, requests a money transfer through their local bank, "Bank A" Following receipt of the request, "Bank A" transmits the transaction information to the nation's central bank (referred to as "Central Bank 1"). By sending the request to the central bank of User P's nation (referred to as "Central Bank 2"), Central Bank 1 serves as an intermediary and makes the transfer possible. The transaction details are then forwarded by Central Bank 2 to User P's local bank, designated as "Bank D." After confirming the legitimacy and authenticity of the request, Bank D sends a confirmation signal back to Bank A via the same chain of intermediaries.

The transaction is carried out in accordance with the confirmation received, and the money is either transferred or rejected. It's important to remember that this

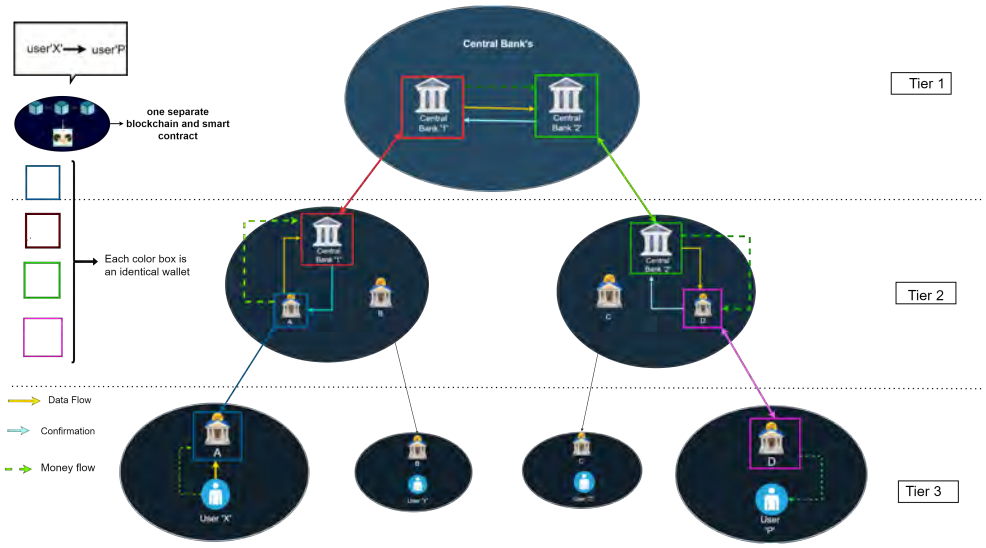

Figure 4.4: International transaction

architecture allows for the existence of identical banks in different blockchains, each with its own particular wallet. Through the use of wallets, these identical banks are linked together, facilitating safe and easy communication and transaction execution.

Chapter 5

Implementaion

Our main focus on this proposal is to implement such a system under blockchain that can seamlessly transfer money in any place; for that, we have used smart contracts. Then again we have both intra-banking(within the same financial institution) and inter-banking(between different financial institutions) transactions to smoother the transfer. This system is flexible for banks at different levels to make distinct policies, which include local, regional, or global policies, regardless of their position within a hierarchy. They can make their own policies like maximum transactions allowed for a single transaction, account type restrictions, transaction frequency limits, and so on. While implementation of these specific policies might not have been explicitly implemented in our current system, the architecture supports the inclusion of these features. As we have said, due to the nature of the chain code and hierarchical structure, this is a highly scalable system. Moving on, we can integrate new chain codes to ensure more precise, detailed, and certain controls over various aspects of transactions. This system is implemented in a modular fashion, which means that its components are built separately, which makes them independent units or modules. In addition, this system maintains a hierarchical structure, meaning it's organized in a structured manner. Due to the nature of the proposed implementation, the modularity paired with a straightforward hierarchical approach allows for a system where it can be adopted and accepted by any organization across the globe.

5.1 Protocol Flow

5.1.1 Frontend

For the front end, we have used Express JS [renderer] as a base, and we have implemented it using mostly HTML and CSS with some use of bootstrapper code to beautify the site, as seen in Fig.5.2. As for the majority of the front-end logic, it has been applied with JavaScript scripts incorporated in the *.ejs files. The front end currently starts off with a landing page that consists of 2 buttons allowing the user to either log in or sign up. Both login and signup pages allow the user to go to the other page if needed. Upon login, a new user will be redirected to the KYC Verification page, where the user must enter KYC-related information to verify their identity (discussed further in the backend section). Once the user is verified, they now have access to the profile page showing the user's KYC data (this is just a filler page to show/demonstrate the stored data and is not functionally necessary).

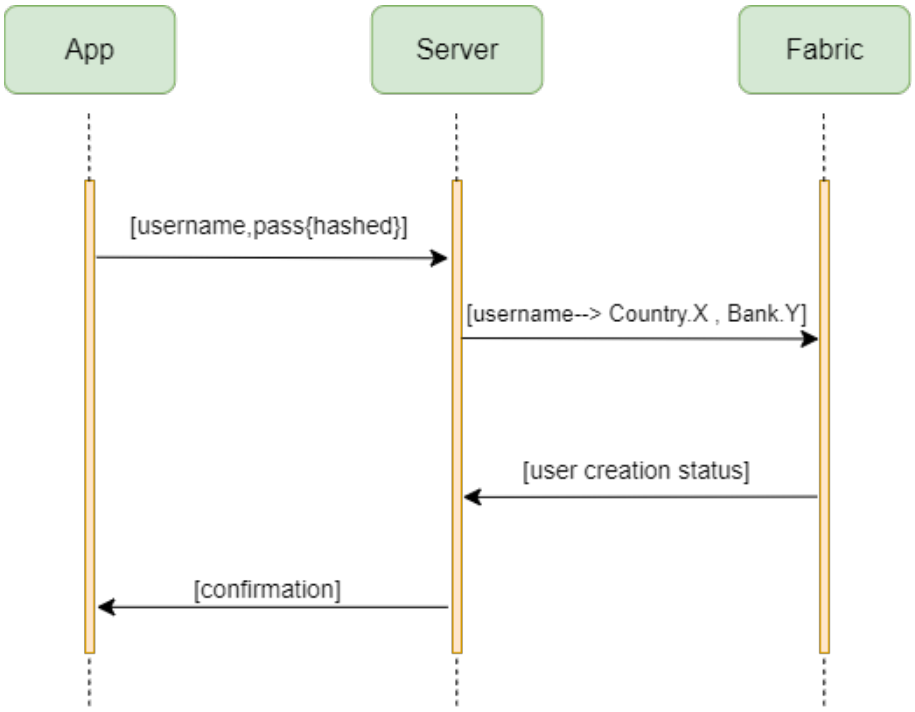

Figure 5.1: Protocol flow for signup

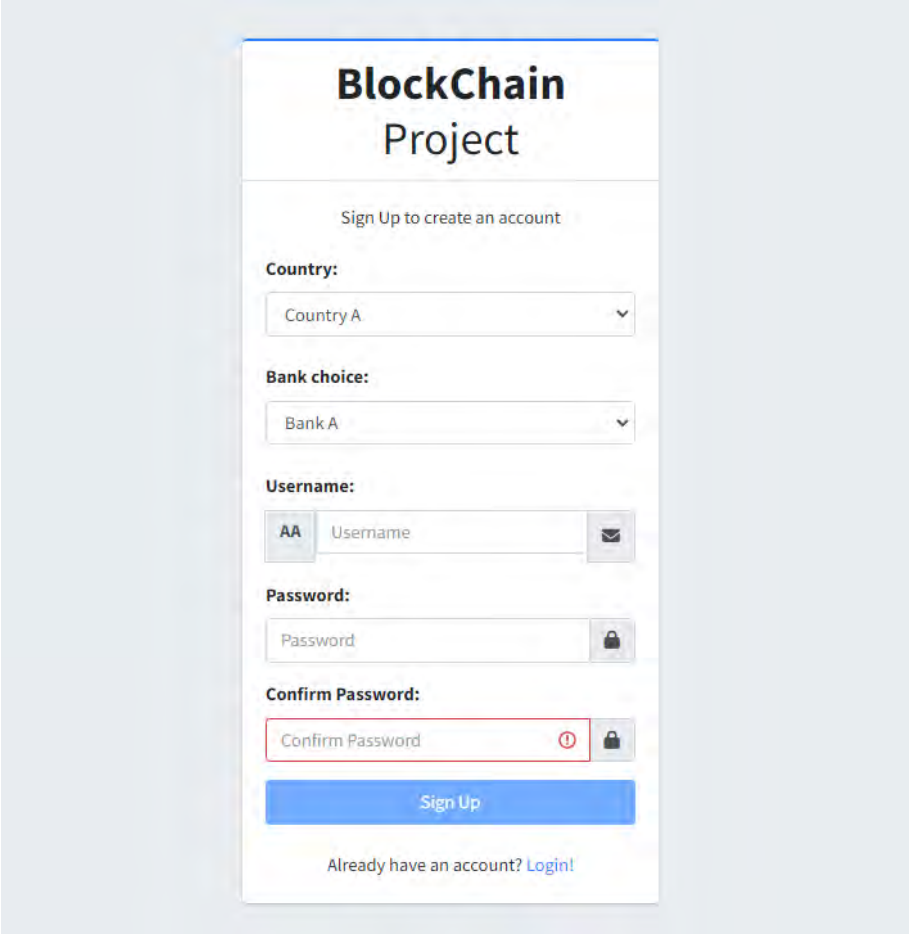

Figure 5.2: Signup page

i Here (Fig. 5.1), a new user will see the sign-up option where they need to fill out the username and password (including the confirm password field). Then, the password will be hashed

ii After the server receives the information, it will break the username's first two characters into country code and bank code. (country code and bank code can be extended to 3-4 characters)

iii Upon fabric receiving the information, it will create a user entity and send its status back to the server

iv Lastly, the server will send confirmation back to the system

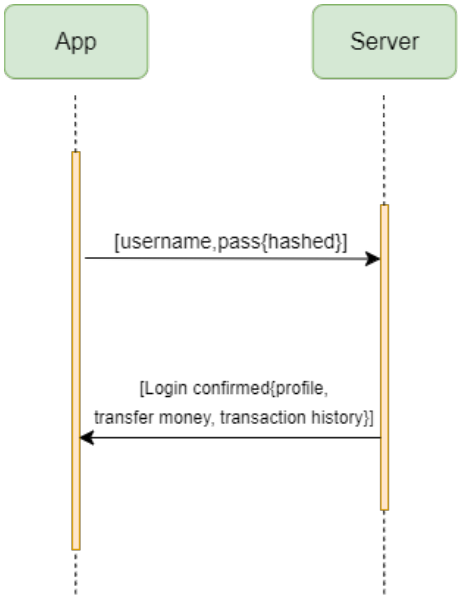

Figure 5.3: Protocol flow for login

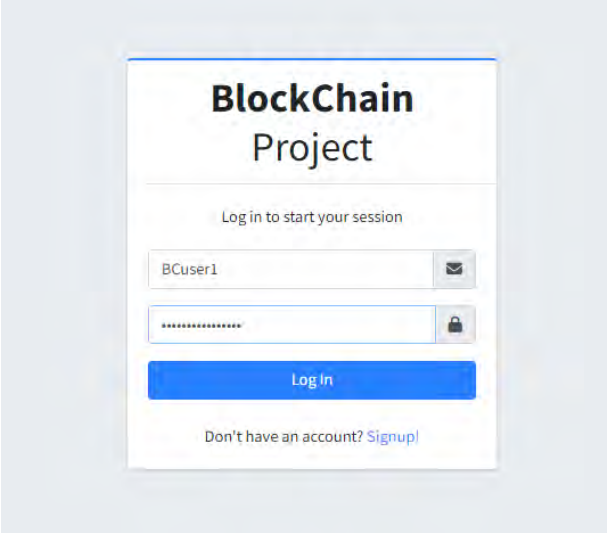

Figure 5.4: Login page

i Here (Fig 5.4,5.3), the user will see the login option where they need to fill out the username and a password (including the confirm password field), and then the password will be hashed.

ii Server will reply back with a confirmation of successful login.

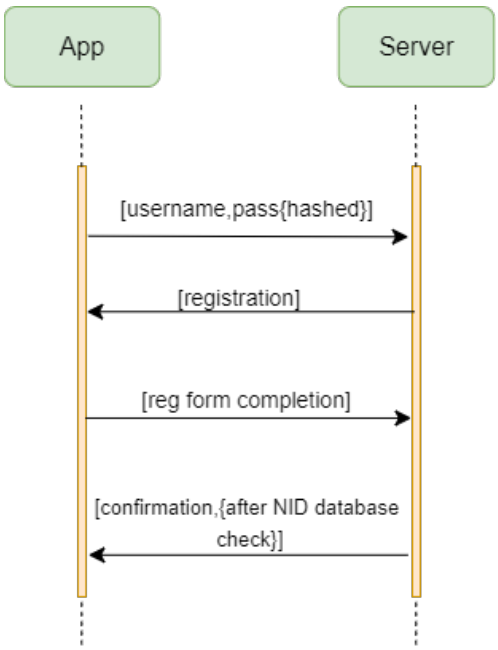

Figure 5.5: Protocol flow for login(Unregistered user)

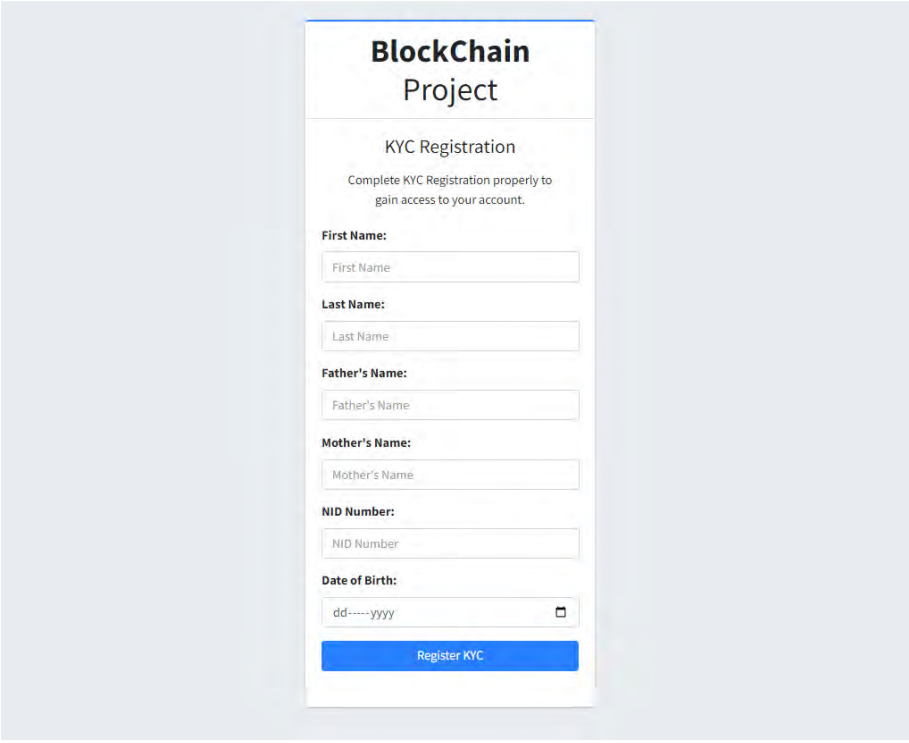

Figure 5.6: KYC Registration Page

i Here (Fig 5.5,5.6), the user will see the Login option where they need to fill out the username and a password (including the confirm password field), and then the password will be hashed.

ii Upon receiving the information, the server will send a KYC registration form to the system

iii The User will fill out the registration form, and then the server will reply back with confirmation.

5.1.2 Backend

The backend consists of a JavaScript server using the Express framework. For storing user-related data, we have set up a MongoDB server (Fig.5.7) using Mongoose inside a Docker container. Passport has been used for user authentication, such as login and signup authentication; this has been incorporated into the MongoDB server using passport-local-mongoose. In addition, this backend connects to the fabric network to perform necessary transactions utilizing the chain codes integrated into the network. The backend is also responsible for selecting which chain code has to be executed and what methods are to be used to handle responses after execution. We have 2 collections present in our MongoDB database, one for NID information and another for storing user-related data. Here, the NID collection acts as a source of information for automatic KYC verification.

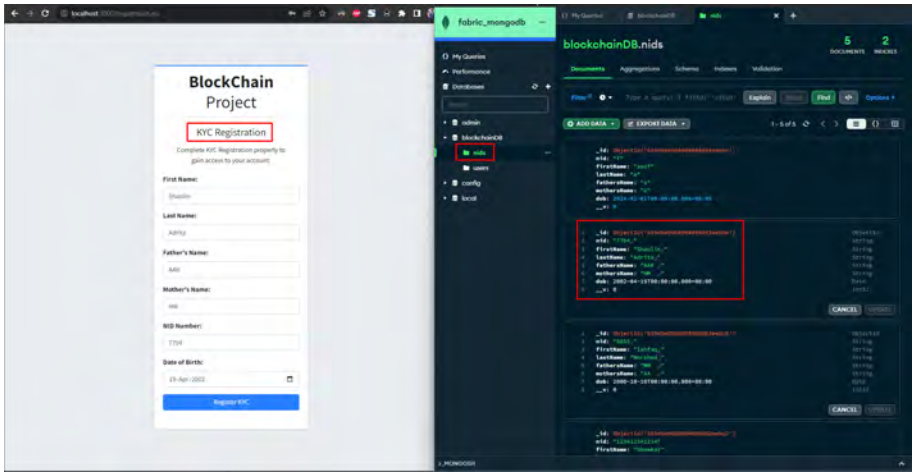

Figure 5.7: KYC Verification [including MongoDB]

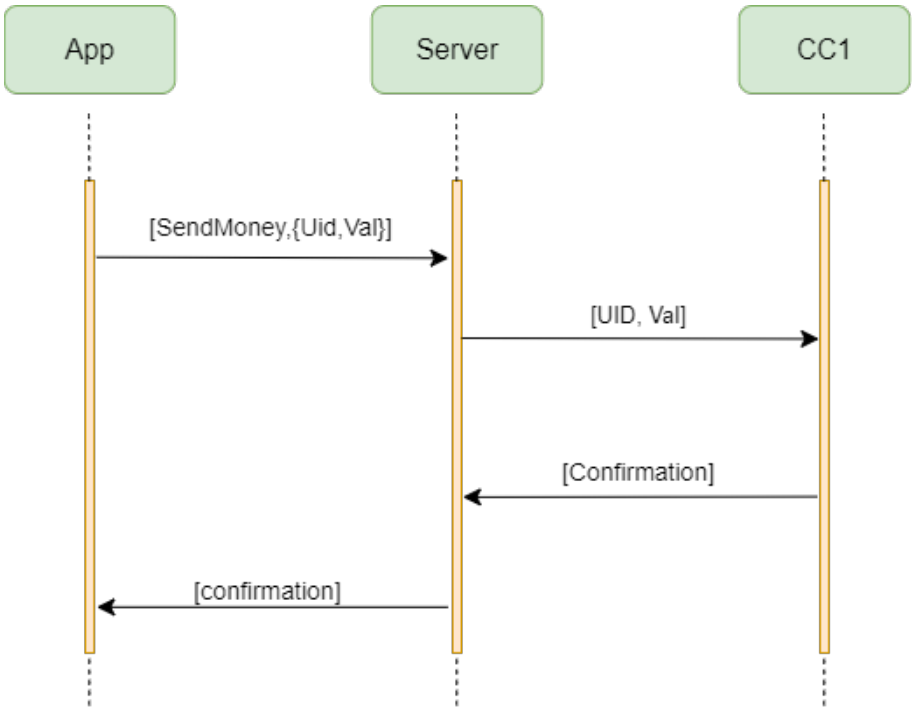

Figure 5.8: Protocol flow for peer-to-peer transaction

i In peer-peer transaction (Fig.5.8), the user will fill out the receiver user ID and amount to be transferred

ii Server will send the user ID and amount value to chaincode1

iii Then chaincode1 will send back a confirmation message to the server, and the server will pass it to the system

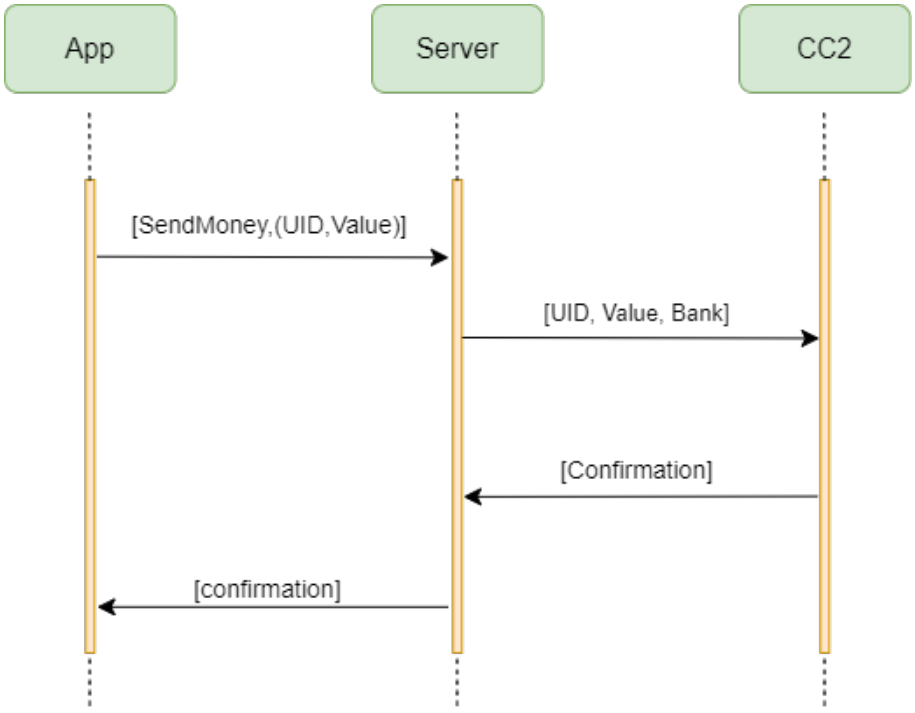

Figure 5.9: Protocol flow for bank-to-bank transaction

i For bank-to-bank transactions, (Fig.5.9) everything will remain the same where, as usual, the user will fill out the receiver's user ID and value

ii Here, the server will send the user ID, amount value, and additional bank address to chaincode2

iii After that, chaincode2 will send a confirmation message to the server

iv Lastly, the server will show a readable success message to the system

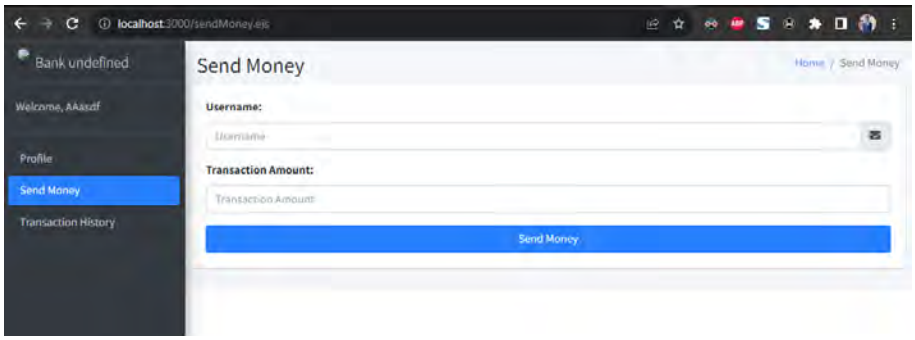

Figure 5.10: Send Money page

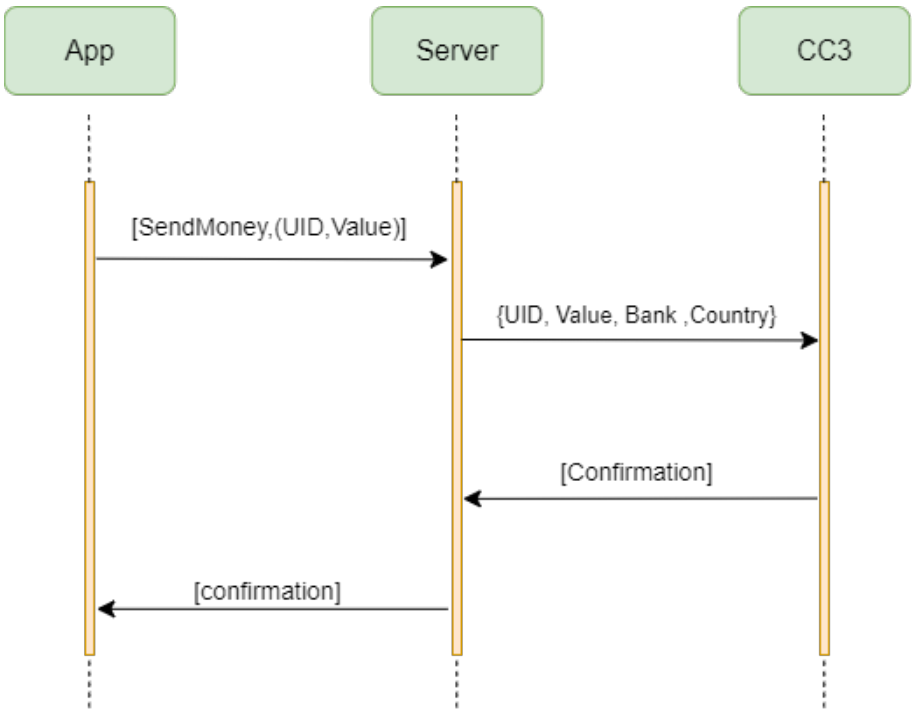

Figure 5.11: Protocol flow for cross border transaction

i For cross-border transactions (Fig.5.10, 5.11), everything remains the same except the server will send the user ID, value, bank address, and country address to chaincode3

5.1.3 The Blockchain Network.

The Blockchain Network (Fig.5.12) is essentially a HyperLedger Fabric network using a series of network configurations and chain codes. The Fabric network consists of docker images made for each Certificate Authority, Orderer, and Peer in the network. The transactions are maintained via CouchDB databases in Docker containers. After initializing the network, we just need to start up the backend, which can then seamlessly connect to the Fabric network using the Fabric API.

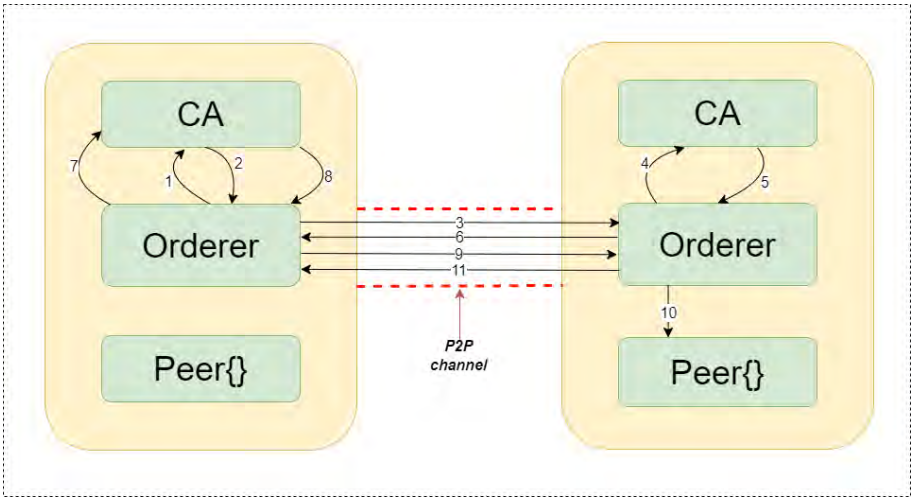

Figure 5.12: Hyperledger fabric network

5.2 Activity Diagram

This activity diagram (Fig.5.14) basically shows the flow of our proposed system it has been described below

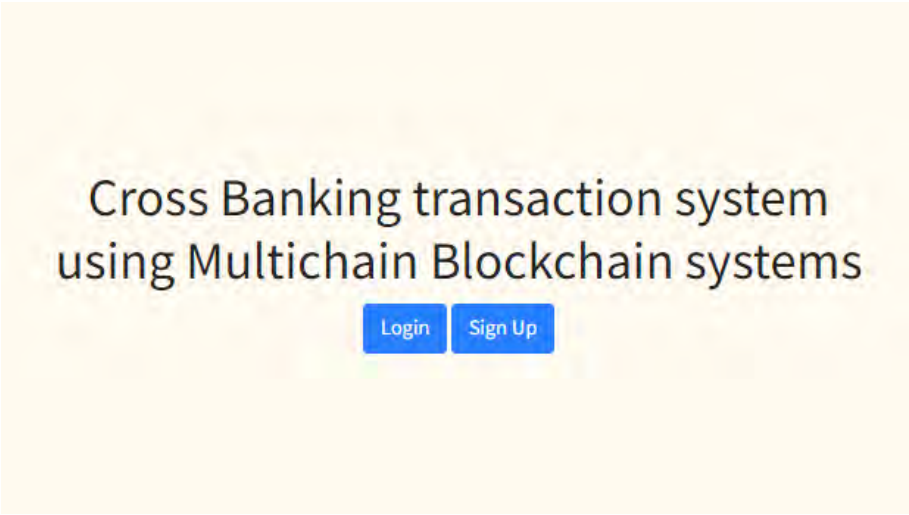

Figure 5.13: Signup page

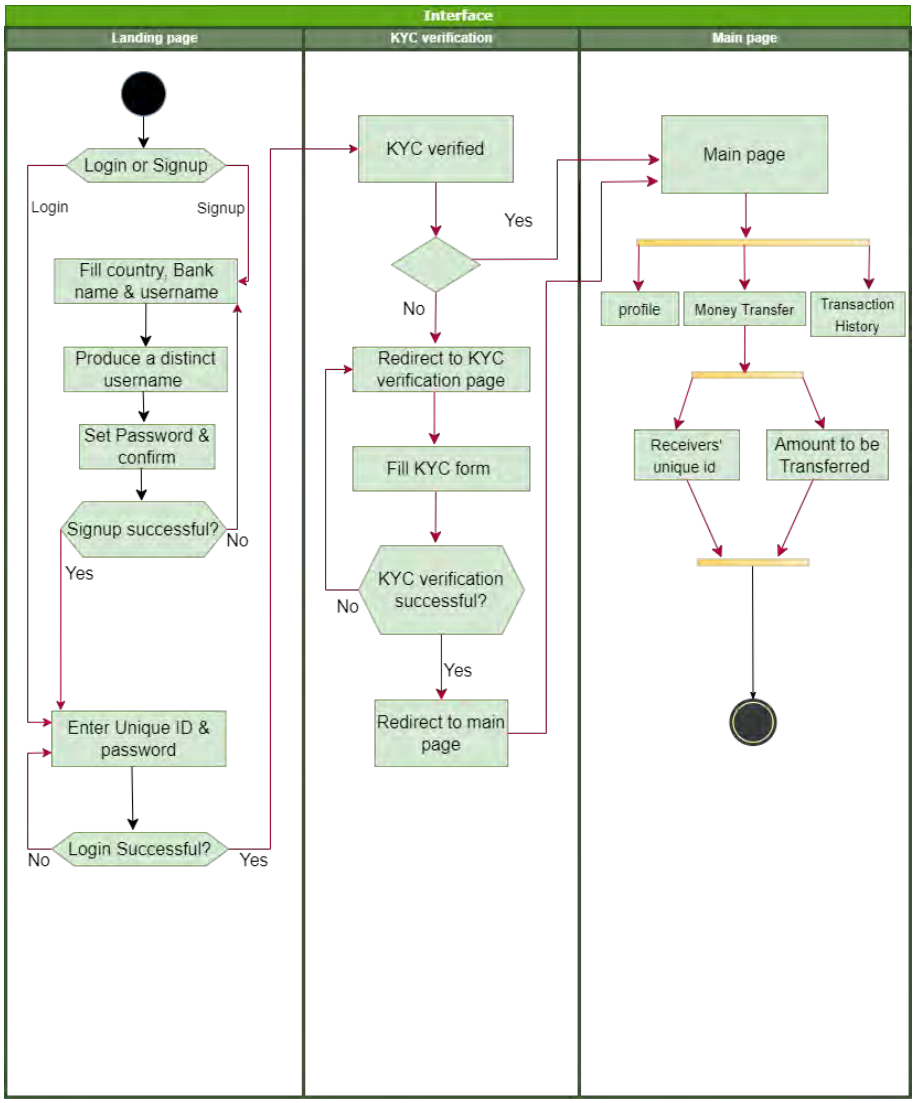

Figure 5.14: Activity Diagram

i Landing Page:

(a) Login (Fig.5.13):

i. Registered users can input their unique ID and password for authentication.

ii. The unique ID comprises the first two characters(it can be scaled up to 3+3=6 characters) denoting the country code and bank code, followed by the user's chosen username.

(b) Signup:

i. Unregistered users must click on "Signup" to initiate the registration process.

ii. On the signup page, users need to provide their country, bank name, and username.

iii. The system automatically generates a unique username by combining the country code and bank code with the user-provided username.

iv. Users must set a password and confirm it.

v. The signup button remains inactive until all required fields are filled correctly.

ii KYC verification:

(a) After a user logs in the system detects whether they have undergone KYC verification.

(b) If KYC verification is pending or not completed, users are automatically directed to the KYC verification page.

(c) Users are required to provide their first name, last name, father's name, mother's name, National ID (NID) number, and date of birth for identity verification.

(d) The system checks the provided information against the KYC requirements, ensuring accuracy and completeness.

(e) If the provided information is accurate, the KYC verification process is marked as complete, and users are redirected to the main page where users gain full access to the main page, featuring their profile, transaction history, and money transfer capabilities.

(f) If KYC is already done, the user gets redirected to the Main page

iii Main User Page:

(a) Profile:

i. Users can view their profile information, including personal details provided during KYC.

ii. Everything here remains fixed and cannot be altered by the user.

(b) Transaction History:

i. Users can review a comprehensive transaction history that includes details of all previous transactions.

(c) Money Transfer:

i. To transfer money, users navigate to the money transfer section.

ii. They fill in two fields - the receiver's unique ID and the amount to be transferred.

iii. The receiver's unique ID is created in the same manner as the sender's, ensuring secure and validated transactions.

Chapter 6

Discussion

6.1 Research Objectives Analysis

The system fulfills the research objectives in the following way:

- **R1** - We have implemented a system that uses hyper ledger fabric, and as we are using smart contracts for transfer, it reduces the transfer cost to a minimum. Moreover, hyper ledger fabric ensures security at an advanced level by mitigating the counterfeiting problem. This is how we are completing the R1 requirement.

- **R2** - we have implemented a system that has a multichain blockchain system. As previously mentioned, each bank has its own blockchain, and all of them are interconnected. It includes intra-bank transactions, inter-bank transactions, and also cross-border transactions. So it fulfills R2.

- **R3** - As we are using a blockchain system within the banking infrastructure, it ensures the security of each transaction as hyper ledger fabric is used for smart contracts. By this, R3 is achieved.

- **R4** - As the current banking system has some limitations, we proposed this system, which has overcome some of them now. By future work, research, and implementation, our system will be able to overcome all the limitations of traditional banking techniques.

6.2 Comparative Analysis

In this section, we've conducted a comparative analysis (Table 6.1) between our current proposal and existing research. Table 6.3.1 displays a comparison across several criteria, indicating whether each work met (with a "✔") or did not meet (with an "✘") the specific criterion.

Table 6.1: Comparative Analysis

Criteria	Our Work	Hassani (2018) [18]	Bakaul (2020) [4]	Golubey (2020) [16]	Lance (2018) [1]	Paliha-pitiya (2020) [22]	Khan (2021) [6]	Belchior.R (2021) [23]
HF	✔	✘	✘	✘	✔	✘	✘	✔
Smart Contract	✔	✔	✔	✘	✔	✔	✔	✔
Cross Communi-cation	✔	✘	✘	✘	✘	✔	✘	✔
Crypto-currency	✘	✔	✔	✔	✔	✔	✔	✔
KYC	✔	✔	✘	✘	✘	✔	✘	✔
Threat Modelling	✔	✘	✘	✘	✘	✘	✘	✘

6.3 Fulfillment of Requirements

6.3.1 Functional Requirements (FR):

This system fulfills the specified functional requirements. We used blockchain technology in each layer. Also, every bank obtains its own blockchain, and all of these blockchains are interconnected, which achieves FR1-FR3. We used a hyper ledger fabric network, which can directly connect to our server and provide necessary data; by this, FR4 is achieved. In the system, if a user is not KYC verified, they are asked to fill out a form to be KYC verified, which fulfills FR5. FR6 is achieved as in the system, users can transfer funds, manage accounts, and see transaction history.

6.3.2 Security Requirements (SR):

Our proposed system ensures that before requesting any money transaction, users should have to be authorized. This satisfies S1. Moreover, after the authentication, user can access their data. To keep separate the information of different authorized users, there will be a secure session that will maintain this so that no user will be able to access other users' data. This ensures S2. As a decentralized blockchain technology, Hyperledger Fabric provides good security against DoS attacks. To ensure dApp services stay functional through a DoS attack, a decentralized network of dApp can be established, thereby satisfying S3.In order to safeguard against replay attacks, we propose using nonces at every level of our protocol so that it will ensure security, prevent replay attacks, and maintain uniqueness; this satisfies S4.

6.3.3 Privacy Requirements (PR):

If there is any monetary transaction, e.g., balance transfer, or balance inquiry, there should be the consent of the user. The user needs to ensure the transaction by using a confidential passcode. However, if the user does not give consent and use the key, the transaction will be considered an invalid transaction and will be discarded. So,

the full consent and control for any financial transaction will be authorized by the user. Consequently, all this satisfies or fulfills P1 and P2.

6.4 Advantages

i Our proposal ensures a secure verification mechanism that will protect user's security and data. However, no one will be able to get any data or information of any user except the user.

ii The transactions are now happening between users; there is a third party handling this system so that they can have or access all their information, and also, users have to rely on these third parties. Our proposal ensures that the transactions will be only between users, and no third party will be there to control these transactions.

iii With the current banking system, the transactions take time to transfer money for one or more days; our proposal is to solve this, and it will not take too much time for banking. It will improve efficiency and provide a seamless transaction between users.

iv For doing transactions internationally, there are a lot of processes to complete in the recent banking system and also in between nationally with different banks. So, in an emergency, users face many difficulties in doing transactions. Our system offers to solve this and provides solutions that will make it possible to do these transactions between users with their banking data. Users can directly communicate with any other users.

6.5 Limitations

i Ensuring all banks/countries will agree to use the system is uncertain. This system will only be available to organizations agreeing to participate.

ii Complete decentralization can never be achieved

iii For now, our implementation enables us to store data in a password-protected database, which is unencrypted.

6.6 Future Work

In the future, we look forward to working on the following:

i We should explore the possibilities of implementing a multichain blockchain system in banking environments. Let's work together with financial institutions to deploy and test the system on a scale.

ii We should conduct studies involving users to gather feedback on how usable and accepted the implemented blockchain system is. Based on this feedback, we can continuously. Enhance the system.

iii It's important to examine the landscape for blockchain in the banking sector. We need to ensure that our implemented system complies with existing and future regulations

iv Let's look into how we can integrate our multichain system with emerging technologies like intelligence and the Internet of Things (IoT). By assessing synergies, we can identify opportunities for enhancing our system. Global Collaboration and Standardization: we should collaborate with organizations and standardization bodies to establish standards for multichain systems in banking. Contributing to the development of practices and protocols will be crucial in this process.

v Security audits should be implemented to identify any vulnerabilities that need attention.

vi We must stay updated on cybersecurity threats to ensure that our system remains resilient against evolving risks.

Chapter 7

Conclusion

The proposed system's design presents a promising framework poised to revolutionize financial infrastructure, offering enhanced efficiency, security, scalability, and user-friendliness. Its architecture as a permissioned ledger introduces efficiency by significantly reducing maintenance overheads. The structure of this ledger system enhances the utilization of resources, makes simpler procedures, and provides an environment that is more efficient. Its fundamental scalability is one of its significant achievements. By utilizing advanced interoperability techniques, including notary schemes, sidechains, and relays, the system is prepared to deal with rising transaction quantities and user requirements without compromising efficiency. Such flexibility is vital for making sure that the system remains able to evolve to transform the needs or demands of a growing percentage of individuals and expand the financial environment. In order to sum up, the integration of a permissioned ledger, a hierarchical blockchain framework as well as advanced interoperability approaches is an innovative move into a financial ecosystem that is more effective, sustainable yet secure. This framework's combined efforts aspire to establish an intuitive, accessible, and robust financial infrastructure that stays in procedure with the evolving demands of the digital marketplace, besides simplifying existing financial activities.

Bibliography

[1] X. Wang, X. Xu, L. Feagan, S. Huang, L. Jiao, and W. Zhao, "Inter-bank payment system on enterprise blockchain platform," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018, pp. 614–621. DOI: 10.1109/CLOUD.2018.00085.

[2] H. T. Vo, Z. Wang, D. Karunamoorthy, J. Wagner, E. Abebe, and M. K. Mohania, "Internet of blockchains: Techniques and challenges ahead," *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1574–1581, 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:174801874.

[3] "Hyperledger fabric," 2020. [Online]. Available: https://www.hyperledger.org/use/fabric.

[4] M. Bakaul, N. R. Das, and M. A. Moni, "The implementation of blockchain in banking system using ethereum," *International Journal of Computer Applications*, vol. 177, no. 38, pp. 50–54, Feb. 2020, ISSN: 0975-8887. DOI: 10.5120/ijca2020919895. [Online]. Available: http://www.ijcaonline.org/archives/volume177/number38/31159-2020919895.

[5] B. Pillai, K. Biswas, and V. Muthukkumarasamy, "Cross-chain interoperability among blockchain-based systems using transactions," *The Knowledge Engineering Review*, vol. 35, e23, 2020. DOI: 10.1017/S0269888920000314.

[6] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2901–2925, Sep. 2021, ISSN: 1936-6450. DOI: 10.1007/s12083-021-01127-0. [Online]. Available: https://doi.org/10.1007/s12083-021-01127-0.

[7] *Bangladesh Bank — bb.org.bd*, https://www.bb.org.bd/en/index.php/financialactivity/paysystems, [Accessed 23-01-2024].

[8] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, Sep. 1997. DOI: 10.5210/fm.v2i9.548. [Online]. Available: https://firstmonday.org/ojs/index.php/fm/article/view/548.

[9] W. Li, A. Sforzin, S. Fedorov, and G. O. Karame, "Towards scalable and private industrial blockchains," ser. BCC '17, Abu Dhabi, United Arab Emirates: Association for Computing Machinery, 2017, pp. 9–14, ISBN: 9781450349741. DOI: 10.1145/3055518.3055531. [Online]. Available: https://doi.org/10.1145/3055518.3055531.

[10] C. P. Gilbert Verdian Paolo Tasca and G. Mondelli, "Quant overledger whitepaper v0.1. technical report," 2018. [Online]. Available: http://objects-us-west-1.dream.io/files.quant.network/Quant%5C_Overledger%5C_Whitepaper%5C_v0.1.pdf.

[11] A. Larsen, "A primer on blockchain interoperability," 2020. [Online]. Available: https://medium.com/blockchain-capital-blog/a-primer-on-blockchain-interoperability-e132bab805b.

[12] S. A. Back, M. Corallo, L. Dashjr, *et al.*, "Enabling blockchain innovations with pegged," 2014. [Online]. Available: https://api.semanticscholar.org/CorpusID:18659636.

[13] P. Gaži, A. Kiayias, and D. Zindros, *Proof-of-stake sidechains*, Cryptology ePrint Archive, Paper 2018/1239, https://eprint.iacr.org/2018/1239, 2018. [Online]. Available: https://eprint.iacr.org/2018/1239.

[14] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," *2018 IEEE Symposium on Security and Privacy (SP)*, pp. 583–598, 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:29885138.

[15] A. Zamyatin, N. Stifter, A. Judmayer, P. Schindler, E. R. Weippl, and W. J. Knottenbelt, "(short paper) a wild velvet fork appears! inclusive blockchain protocol changes in practice," *IACR Cryptol. ePrint Arch.*, vol. 2018, p. 87, 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:4026352.

[16] A. Golubev, O. Ryabov, and A. Zolotarev, "Digital transformation of the banking system of russia with the introduction of blockchain and artificial intelligence technologies," *IOP Conference Series: Materials Science and Engineering*, vol. 940, no. 1, p. 012 041, Sep. 2020. DOI: 10.1088/1757-899X/940/1/012041. [Online]. Available: https://dx.doi.org/10.1088/1757-899X/940/1/012041.

[17] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," May 2009. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf.

[18] X. H. Hossein Hassani and E. Silva, "Banking with blockchain-ed big data," *Journal of Management Analytics*, vol. 5, no. 4, pp. 256–275, 2018. DOI: 10.1080/23270012.2018.1528900. eprint: https://doi.org/10.1080/23270012.2018.1528900. [Online]. Available: https://doi.org/10.1080/23270012.2018.1528900.

[19] P. Zhang, J. White, D. C. Schmidt, and G. Lenz, "Applying software patterns to address interoperability in blockchain-based healthcare apps," *arXiv preprint arXiv:1706.03700*, 2017.

[20] X. Liu and T. Yu, "An automatic pattern recognition value system with listed banks based on blockchain," in *2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, 2018, pp. 1850–1854. DOI: 10.1109/IAEAC.2018.8577773.

[21] A. Shostack, "Threat modeling: Designing for security. hoboken," 2014.

[22] T. Palihapitiya, "Blockchain in banking industry," Oct. 2020.

[23] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Comput. Surv.*, vol. 54, no. 8, Oct. 2021, ISSN: 0360-0300. DOI: 10.1145/3471140. [Online]. Available: https://doi.org/10.1145/3471140.