A PROJECT REPORT ON

Decentralized Chit Funds: A Sidechain Approach for Scalability

Submitted by

SHANMUGASUNDARAM P

REGISTER No.: 22412034

Under the Supervision and Guidance of

DR. K. USHA

Asst Professor, Department of Banking Technology

MASTER OF BUSINESS ADMINISTRATION

IN

FINANCIAL TECHNOLOGY

DEPARTMENT OF BANKING TECHNOLOGY

SCHOOL OF MANAGEMENT

PONDICHERRY UNIVERSITY, PONDICHERRY - 14

MAY 2024

DEPARTMENT OF BANKING TECHNOLOGY

PONDICHERY UNIVERSIRY

BONAFIDE CERTIFICATE

This is to certify that this project report titled "**Decentralized Chit Funds: A Sidechain Approach for Scalability"** is the bonafide work of **"SHANMUGASUNDARAM P"** who carried out the project work under my supervision during January 2022 to May 2024.

SIGNATURE	**SIGNATURE**
Professor, DR. V. MARIAPPAN	Asst Professor, DR. K. USHA
HEAD OF THE DEPARTMENT	**Supervisor**
Department of Banking Technology	Department of Banking Technology

Submitted for the Project Viva – Voce examination held on

_____

…….	……..……
Internal Examiner	**External Examiner**

DEPARTMENT OF BANKING TECHNOLOGY

SCHOOL OF MANAGEMENT
PONDICHERRY UNIVERSITY, PONDICHERRY - 14

DECLARATION

SHANMUGASUNDARAM P

2ND YEAR MBA FINANCIAL TECHNOLOGY

DEPARTMENT OF BANKING TECHNOLOGY

PONDICHERRY UNIVERSITY

I declare that the project entitled **"Decentralized Chit Funds: A Sidechain Approach for Scalability"** is the result of a study originally carried out by me under the guidance and supervision of **DR. K. USHA**, assistant professor of Department of Banking technology, Pondicherry University. This work has not been submitted earlier, in full or in part, for any Diploma, Degree or any other award, in this or any other university.

I also declare that no part of this project is a reproduction from any other source, published or unpublished, without acknowledgement.

Place: Pondicherry **SHANMUGASUNDARAM P**

Date:

ABSTRACT

Chit funds are typically operated among a trusted network of people, by a foreman, completely relying on the trust and transparency of the transactional data audited through the network. The cost involved in this ledger keeping or audit procedures for ensuring trust and transparency is the major institutional overhead for running a chit fund. To overcome these issues, Blockchain based Chit funds were developed and implemented successfully. Even though this innovative idea was a success, there are some drawbacks aroused like “scalability”. Scalability refers to a system's ability to handle an increasing amount of data or users without a significant decline in performance. When the number of users and transactions increases, the size of the blockchain ledger also increases. This can make it more difficult and time-consuming for nodes to store and synchronize the entire blockchain. With a high volume of transactions, the blockchain network can become congested, leading to delays in transaction processing and confirmation times. This can be frustrating for chitfund participants who need timely access to their funds. This paper proposes including a new blockchain technology called “Sidechain”. In blockchain technology, a sidechain is a separate blockchain network that connects to another, main blockchain (often called the parent blockchain or mainnet). The parent chain will have high level of security and the sidechain will be for faster transactions. This is possible using “Two-way Peg” technique: A special mechanism allows users to transfer digital assets between the mainnet and the sidechain and the assets aren't physically transferred. Instead, when you move something to the sidechain, an equivalent amount gets locked on the mainnet, and a matching amount is unlocked on the sidechain. This ensures the value is maintained.

ACKOWLEDGMENT

First of all, I express my sincere thankfulness to the Almighty, for bestowing his blessings throughout this project work. I express my gratitude to my Parents for their care, support, prayers and love.

I wish to record my thanks to the honourable Dean, School of Management (SOM),

DR. MALABIKA DEO for his constant support, great enthusiasm and perpetual motivation.

I would like to express my sincere gratitude to **DR. V. MARIAPPAN**, Head of the Department & my project guide **DR. K. USHA**, Department of banking Technology, SOM, Pondicherry University, for his inspiring guidance and sincere advice throughout this project.

I express my sincere and heartiest thanks to all the staffs of Department of banking technology for their advice, encouragement and guidance throughout this project.

I sincerely wish to express my thanks to my friends for their valuable support during this project work. I would also like to thank the authors of various journals and books whose works and results are used in this project.

Finally, I thank all the persons who have directly or indirectly contributed in preparing this project.

With Regards,

SHANMUAGASUNDARAM P

TABLE OF CONTENTS

CHAPTER-1
INTRODUCTION

Chitfunds are a type of financial institution in India that combines the goodness of credit and savings in a single scheme. Chitfunds are operated among a group of individuals, termed subscribers. It is organised by a Foreman, who could be a registered company or a trusted individual.

Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

Traditional chit funds, despite their usefulness, have some drawbacks. There can be a lack of trust in the system since a central figure, the foreman, manages the money. This can lead to worries about mismanagement of funds. Additionally, record-keeping is often manual and paper-based, making it difficult to track transactions and identify discrepancies. There's also the risk of fraud, as the foreman or participants could disappear with the money.

Blockchain technology offers a solution to these issues. By recording all transactions on a secure, shared ledger, blockchain can increase security and transparency. This builds trust among participants because everyone can see the complete history of the chit fund.

Furthermore, automation can streamline operations and reduce administrative costs. Blockchain-based chit funds also have the potential to reach a wider audience and open doors for new features within the chit fund system.

As there are several blockchain based chitfunds system already implemented, one of the important challenges for blockchain-based chit funds is scalability. As the number of users and transactions grows, the main blockchain can become congested, leading to slow transaction processing and increased fees. Imagine a chit fund with hundreds of participants, each contributing

and receiving payments regularly. This high volume of transactions could overwhelm the blockchain, causing delays and making the chit fund cumbersome to use.

Sidechain technology can be a solution to scalability issues in blockchain-based chit funds. A sidechain is a separate blockchain that interacts with the main blockchain. Chit fund transactions can occur on the sidechain, reducing congestion on the main blockchain and improving transaction speed and cost-effectiveness. Think of it as having a dedicated lane for chit fund transactions, keeping the main road (the main blockchain) free-flowing for other activities. Additionally, sidechains can offer more flexibility for implementing new features specific to chit funds, such as automated rule enforcement or reputation scoring for participants. This allows chit fund creators to tailor the system to their specific needs.

1.2 Problem Statement:

This high volume of transactions could overwhelm the blockchain, causing delays and making the chit fund cumbersome to use. How can we enhance scalability in blockchain-based chit fund systems while maintaining trust and transparency.

1.3 Objectives:

- To implement side chain technology In this system and investigate how side chain reduces the scalability issues.
- To elaborate why side chain technology and the other alternatives available for it.

1.4 Chitfund:

1.4.1 What is Chitfund:

"Chit" means a transaction (whether called chit fund, chit, kuri or by any other name), by which the foreman enters into an agreement with a number of subscribers that each of them shall subscribe a certain sum for a certain period and each subscriber in his turn as determined by lot or by auction, shall be entitled to a prized amount.

Chitfunds are a type of financial institution in India that combines the goodness of credit and savings in a single scheme. Chitfunds are operated among a group of individuals, termed

subscribers. It is organised by a Foreman, who could be a registered company or a trusted individual. Foreman brings the group together and regulates the activities of the chit group as defined in Chit Funds Act, 1982, which regulates the Chit Funds in India. As reported in Sect. 2(b) of the Chit Fund Act, 1982: ‘‘Chit means a transaction whether called chit, chit fund, chitty, Kuri or by any other name by or under which a person agrees with a specified number of persons that every one of them shall subscribe a certain sum of money (or a certain quantity of grain instead) by way of periodical instalments over a definite period and that each such subscriber shall, in his turn, as determined by lot or by auction or by tender or in such other manner as may be specified in the chit agreement, be entitled to the prize amount’’. The organizer or the foramen is offered compensation every month or at the time of withdrawal of prize money. The organizer will be responsible for adhering to the chit policy while collecting, managing, and dispensing money and other related decision processes regarding the chit-fund. In the South Indian States of Kerala and Tamil Nadu, chitty (chit fund) is a common phenomenon practised by all sections of society and played a significant role in providing better access to credit and financial wellbeing of the people.

1.4.2 How To Choose a Chit Fund Company:

Verify company registration:

- Check the company's registration with the Registrar of Companies (ROC).
- Confirm the company's registration with the Registrar, Chit Funds, Delhi (RCF).

Review the chit agreement:

- Ensure that the chit group has previous sanction from RCF Delhi.
- Go through the clauses of the chit agreement carefully.

Assess financial capability:

- Make sure you are financially capable of subscribing to the chit group.

Verify directors' credentials:

- Ask for a list of the company's directors.
- Assess the financial soundness of the directors and the company.
- Check for the directors' sincerity towards the subscribers.

Confirm company's good standing:

- Check the list of registered chit fund companies.

- Verify with the RCF that the company is functioning and there are no complaints or court cases pending against the company.

1.4.3 Key Responsibilities:

As a member of a chit fund company, you are obligated to fulfill three main responsibilities as outlined in the chit agreement: making subscription payments on time, providing sufficient surety (guarantor) when you win the prize money, and adhering to all the terms and conditions laid out in the agreement.

1.4.4 Non-Payment Of Prized Money:

As soon as the prized subscriber furnishes sufficient security for the due payment of future subscription(s), the foreman shall be bound to pay him the prized amount or the prized subscriber shall be entitled to demand immediate payment of prize amount after deducting all future subscription without furnishing any security.

1.4.5 Receipt Of Prized Money:

If owing to default of the prized subscribers, the prize amount due in respect of any draw remains unpaid before the next succeeding draw, the foreman shall deposit the same forthwith in an approved bank mentioned in the chit agreement and intimate in writing the fact of such deposit and the reasons therefore to the prized subscriber and the Registrar. Provided that where any prized subscriber does not collect the prize amount in respect of any instalment of a chit within a period of two months from the date of the draw, it shall be open to the foreman to hold another draw in respect of such instalment. The foreman shall not draw any excess amount from that account for any purpose except for further monthly instalments due form the subscriber.

1.4.6 Rights Of A Subscriber:

- To get a proper receipt for payment of subscription from the foreman company.
- To get a copy of chit agreement in respect of the concerned chit group before the date of first auction.
- All subscribers are entitled to attend the auction and non-prized subscribers or their authorised agents can bid during the auction.

- To get the chit amount after the chit is prized in his/her favour before the next auction, subject to the condition that the requisite surety has been furnished in accordance with the chit agreement duly registered with the Chit Fund Department.
- To inspect the chit record and registers etc. at the premises of the chit fund company after payment of requisite fee as mentioned in the chit agreement.
- To seek arbitration in case of any dispute with the chit fund company regarding the chit in the office of the Registrar after paying the arbitration fee prescribed in the Delhi Chit Fund Rules, 2007.

1.4.7 Who Can Become A Member:

- Person having regular sources of income.
- Person of sound mind, who is solvent and has not been convicted in any case.

The fund generally starts at an announced date and carries on for a certain number of months which may be equal to or less than the number of subscribers. Every month subscribers contribute monthly instalments into the chit. An open auction is conducted every month to distribute the prize money. This is to determine the subscribers who are willing to agree to the lowest assured prize money, for that month. If multiple subscribers are bidding for the same prize money, the winner will be selected based on the lot. Some of the prominent advantages offered by a chit fund are:

• The main attraction of chit funds among the households is the early access to money. It offers hassle-free access to money compared to complex banking documentation procedures for availing of loans. Prized customers have early access to money at zero interest and need to bear only a nominal auction discount.

• Prized customers could invest the amount in the chitfund organization and could harvest better interes rates. Also investing the amount in the chit organizing institution would enable the prized customer in producing documents related to proof of security investment, for availing credit or services elsewhere.

• Prized customers could fund microfinance initiatives and harvest returns on the prize money.

• For non-prized customers, soft-loan options are available for interim emergencies with proof of their invested amount.

1.5 BLOCKCHAIN TECHNOLOGY:

Bitcoin, the decentralized network, allows users to transact directly, peer to peer, without a middle man to manage the exchange of funds.

The digital asset, bitcoin, is used like other assets in exchange for goods and services. Unlike traditional currencies and assets, bitcoin is easily portable, divisible, and irreversible.

Bitcoin increases system efficiency and enables the provision of financial services at a drastically lower cost, giving users more power and freedom.

Peer to Peer Network – You must be aware of BitTorrent and Tor. Both of these are built on peer-to-peer network design. A peer to peer network is a distributed application architecture that consists of computing devices connected to each other, without a central server.

In centralised networks, the security is dependent on a single entity. If that central server is attacked, the security of the overall network is compromised. But a peer to peer network is more secure as there is no single point of failure.

Distributed Ledger – A ledger is a system containing all the records of a input and output of a process. A distributed ledger is a data structure which is spread across different computing devices. DLT (Distributed Ledger Technology) is the technology that distribute records across all the users. DLT consists of 3 components – Data Model (current state of ledger), Language of transactions (which changes ledger state) and Protocol (used to build consensus). Blockchain is a type of DLT. This way the data is shared among all its users increasing transparency and avoiding corruption.

Consensus – Consensus is a process of ensuring that all the different users in a blockchain come to an agreement regarding the current state of blockchain. There are several consensus mechanisms that are used by different blockchains to achieve consensus. For example, Bitcoin uses Proof-of-Work while Ethereum is moving from Proof-of-Work to Proof-of-Stake algorithm.

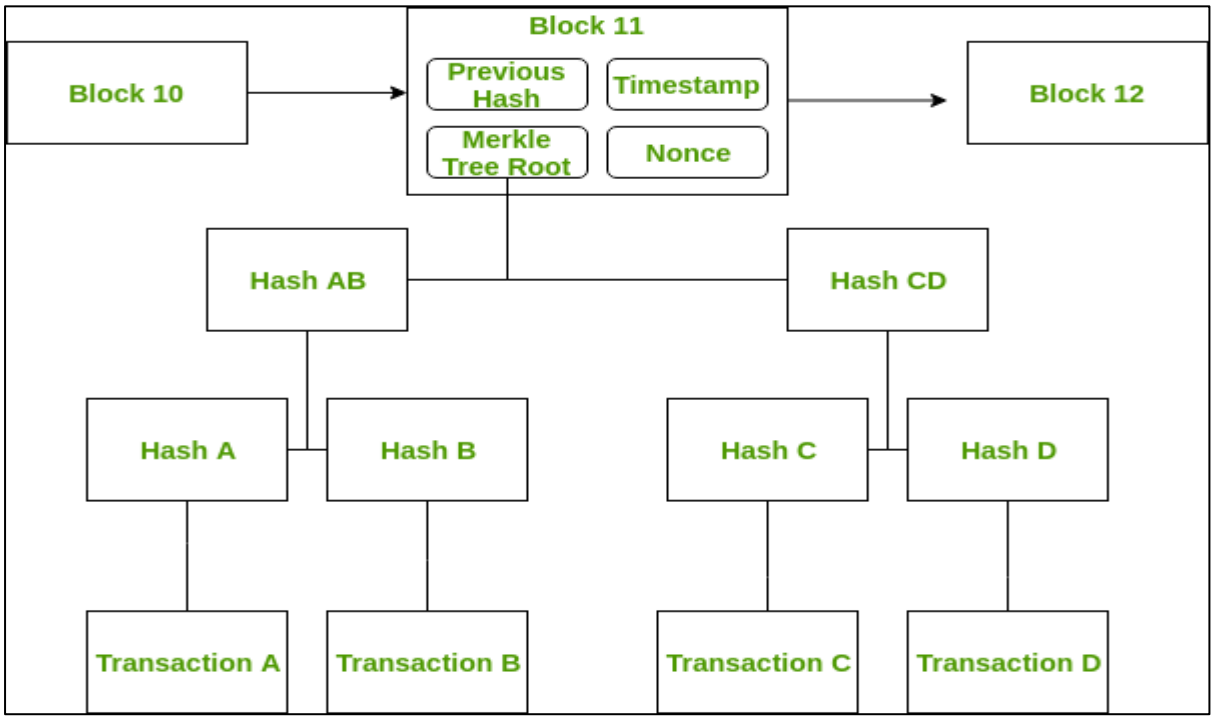
Smart Contracts – Forget smart contract and blockchain for a moment. Think about contracts in general. These contain some conditions which need to be fulfilled in order for some transaction (eg; money exchange) to occur. For example, if you are selling me a laptop, a contract will contain that I will be responsible to pay you only if the laptop works properly. Similarly, smart contracts are pre-requisite conditions which need to be fulfilled for transactions to happen in a blockchain.

1.6 What is inside a blockchain?

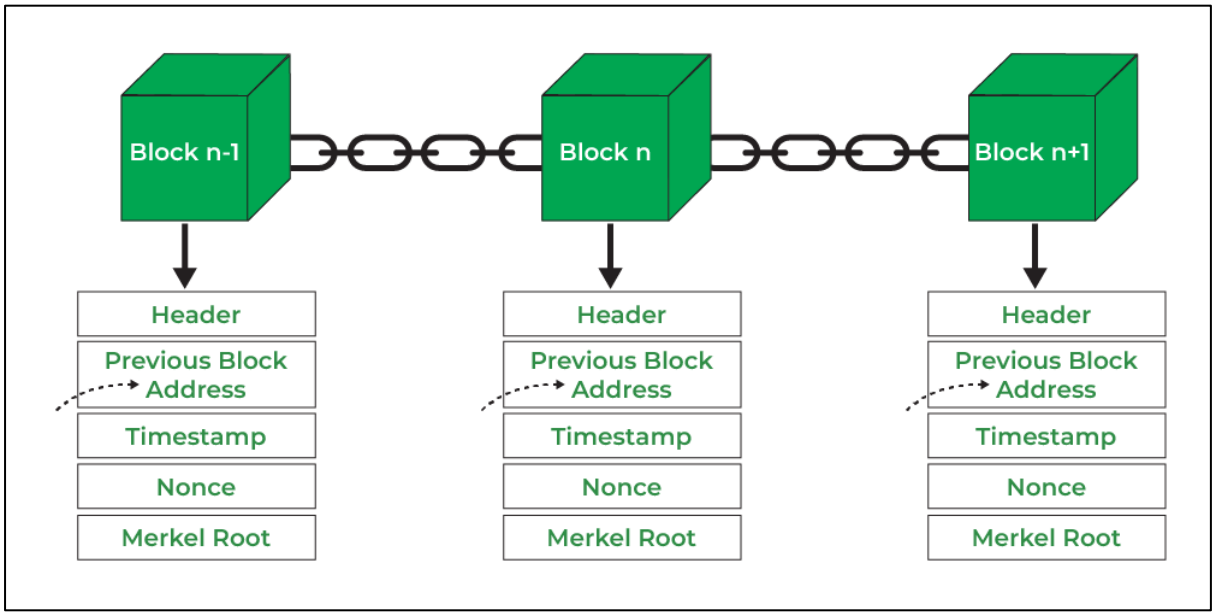
A blockchain is a chain of blocks connected to each other. A block consists of four parts:

I. Previous Hash
II. The timestamp
III. Nonce
IV. Merkle tree root

1.6.1 A block in a blockchain:



1.6.2 How blocks are connected:



1.6.3 Why should I use it?

- Bitcoin was named the top performing currency four of the last five years.
- As a global currency you can send bitcoin to anyone, anywhere in the world without worrying about cross border remittance fees.
- Keeping your bitcoin safe in a non-custodial wallet (like Blockchain's) means there is no entity that can lock you out of your funds.
- It's globally inclusive -- bitcoin is enabling millions across the globe to transact, save, and hedge their way to a better financial future.

Parameters	Blockchain Architecture	Database
Control	Blockchain is decentralized because there is no single point of failure and there is no central authority to control the blockchain.	The database is Centralized.
Operations	Blockchain has only an Insert operation.	The database has Create, Read, Update, and Delete operations.
Strength	It is robust technology.	The database is not fully robust technology.
Mutability	Blockchain is immutable technology and we cannot change it back or we cannot go back.	The database is a fully mutable technology, The data can be edited in the database.
Rights	Anyone with the right proof of work can write on the blockchain.	In the database reading and writing can do so.
Speed	It is slow in speed.	It is faster as compared to blockchain.

1.7 Benefits of Blockchain:

I. It is safer than any other technology.
II. To avoid possible legal issues, a trusted third party has to supervise the transactions and validate the transactions.
III. There's no one central point of attack.
IV. Data cannot be changed or manipulated, it's immutable.

CHAPTER-2

LITERATURE REVIEW

2.1 Literature Review:

1. “ChitChain: A Blockchain-Based Technology Framework for Trust Enablement in Decentralized Chit Funds” by H. S. Jennath, V. S. Anoop, S. Asharaf, and Gopinath Saji (2021).

This study introduces ChitChain, a blockchain framework enhancing trust in decentralized chit funds, focusing on secure data handling and transaction transparency.

2. “Blockchain-Based Chit Fund System: A Financial Inclusion Tool” by Pawan Kumar and Amrit Lal Sanga (2020).

This research explores blockchain's role in chit fund systems, emphasizing financial inclusion through transparent transactions and secure participant interactions.

3. “ChitChain: A Blockchain-Powered Framework for Decentralized Chit Fund Management”.

This paper discusses the ChitChain framework's application in decentralized chit fund management, emphasizing efficiency, security, and trust in chit fund operations.

4. “Blockchain Technology for Chit Fund Management: A Comparative Study” Authors: K. S. Sreejith, K. S. Sreehari, and K. S. Sreelekshmi. (2020).

This comparative study evaluates blockchain's effectiveness in chit fund management, analyzing benefits such as transparency, security, and operational efficiency.

5. “Blockchain-Based Chit Fund Management System: A Case Study” Authors: R. S. Sabeenian, S. S. Sreeja, and S. S. Sreehari (2019).

this research highlights the implementation of a blockchain-based chit fund management system, emphasizing its practical applications and benefits in real-world scenarios.

CHAPTER-3

3.1 Decentralized chitfund system:

Blockchain is the underlying technology of the celebrated Bitcoin and other cryptocurrencies which is redefining the erstwhile model of centralized financial architecture. It is a decentralized, replicated ledger technology that provides an immutable datastore managed by some consensus mechanisms, which offers a potential alternative to traditional models to organize modern finance. The blockchain offers various potential application areas in the finance domain namely securities bond issuance, asset management, payments and settlement, clearing and settlement, trade repositories, credit bureaus, corporate governance, etc. Even though the Blockchain has the potential to build a trusted infrastructure in the financial domain, there are many, legal, regulatory, institutional, and commercial challenges that need to be addressed to ensure effective implementation.

There are attempts reported such as ChitMonk, which uses a platform that uses blockchain technology to bridge the gap inflow of information from chit fund companies to regulators and such platforms are being adopted in the Government. But the same has notyet been used in its full potential due to various bottlenecks such as the operational cost, transaction speed issues, and other issues related to regulatory and compliances. In some states in India such as Andhra Pradesh and Telangana, the chit industry growth has been reported somewhere between 25 and 35 percentage annually. In the last few years in Telegana alone, the total count for the chit fund subscribers has been reported as close to one million. This clearly shows the need for digitized, decentralized, and regulated platform chit fund management.

Decentralization is seen as the perfect solution to problems requiring complex coordination across heterogeneous stakeholders. Hoffman et al., analyze the potential of blockchain-mediated decentralization and try to capture the meaning of decentralization and its salient features, by exploring the commonalities and differences between them and explaining the concepts such as distribution, disintermediation, and peer-to-peer networks and transactions. Osmani et al., explore various potential and benefits blockchain technology could offer for banking and financial sector managers and decision-makers and develop strategies to overcome the identified challenges

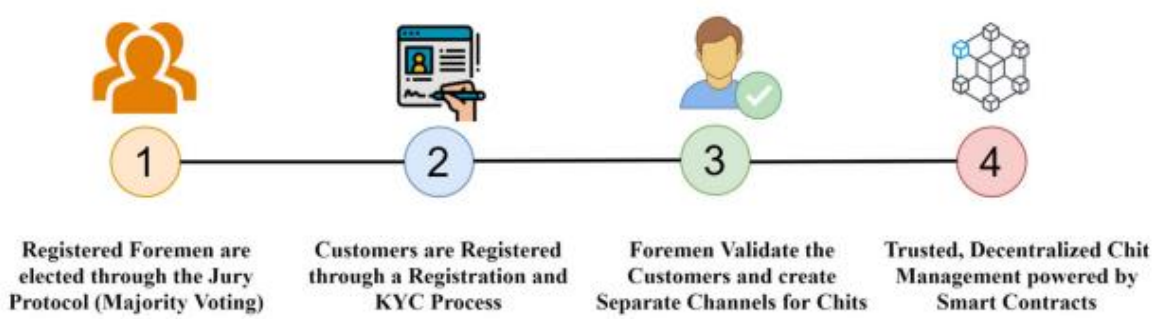
.

The study underlines the need for appreciating various aspects of cost, benefits, risk, and opportunities to design blockchain applications that work for banking and other finance sectors. Scha¨r et al., propose an alternative financial infrastructure built on the top of the Ethereum blockchain, termed decentralized finance (DeFi). DeFi employs smart contracts to design and develop protocols that replicate current financial services in a better interoperable, and transparent way. The article also studied various opportunities and potential risks associated with the DeFi ecosystem.

This work proposed a multi-layered framework for decentralized finance, leveraging the potential of various DeFi building blocks like decentralized exchanges, decentralized token standards, and other asset governance protocols. Faircent is a leading peer-to-peer lending platform in India that is built out a full-fledged loan analytics platform by bringing onboard lenders and borrowers by providing them online tools to discover each other and transact. However, Chitchain is not a mere lending infrastructure or a financial service aggregator rather a microfinance institution capable of instrumenting the peer-to-peer lending opportunity as an added advantage over the chit management platform.

While applications of Blockchain technology in the formal financial sector is well-studied n the literature, the possibility of their extension to the vast informal finance sector is scanty. Identifying the disruptive potential of Blockchain technology in this sector, this paper proposes a decentralized framework powered by blockchain for chit fund management. The proposed framework provides a decentralized platform for transactions and enables trust in the whole ecosystem that offers many advantages for the stakeholders over the traditional centralized finance ecosystem channels and schemes.

3.2 How Blockchain Based Chitfunds Works:



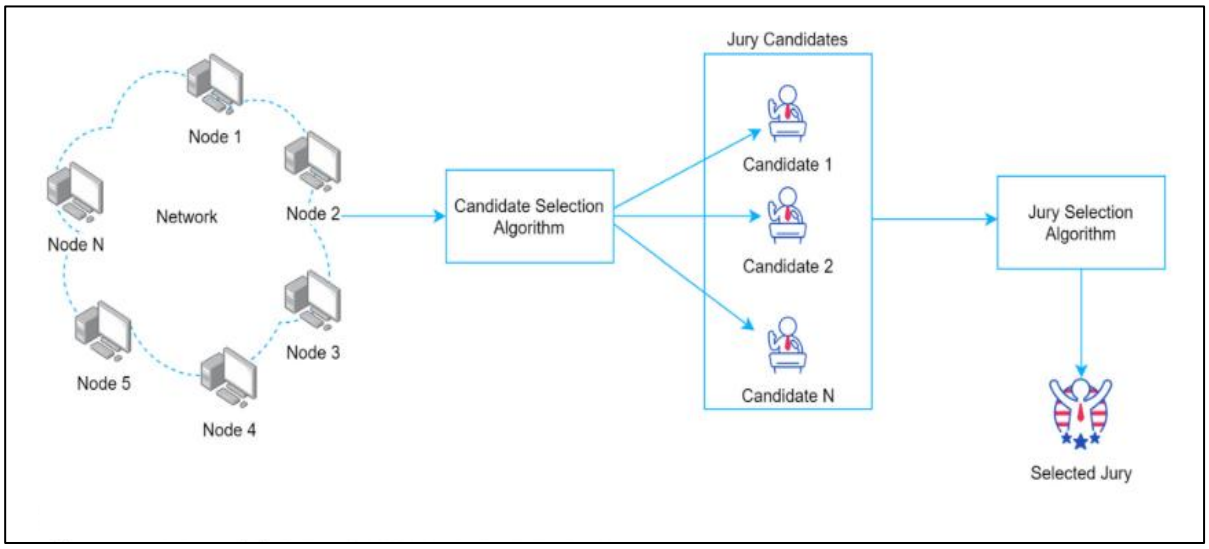
I. **Registered Foremen are Elected:** Foremen, who manage chit funds, are chosen through a jury voting process.

II. **Customers Register:** Customers go through a standard registration process that likely includes KYC (Know Your Customer) verification to confirm their identity.

III. **Foremen Validate Customers:** Once registered, customers are validated by the foremen. This step might involve additional verification or approval by the foremen.

IV. **Trusted Chit Fund Management:** The system creates separate channels for each chit fund, presumably to manage transactions and maintain privacy for each fund. Smart contracts, which are self-enforcing programs on the blockchain, are used to automate chit fund operations.

3.2.1 How Jury Selection Process Works:



I. **Candidate Selection:** Potential jurors are identified from a pool, likely based on criteria such as location and voter registration.

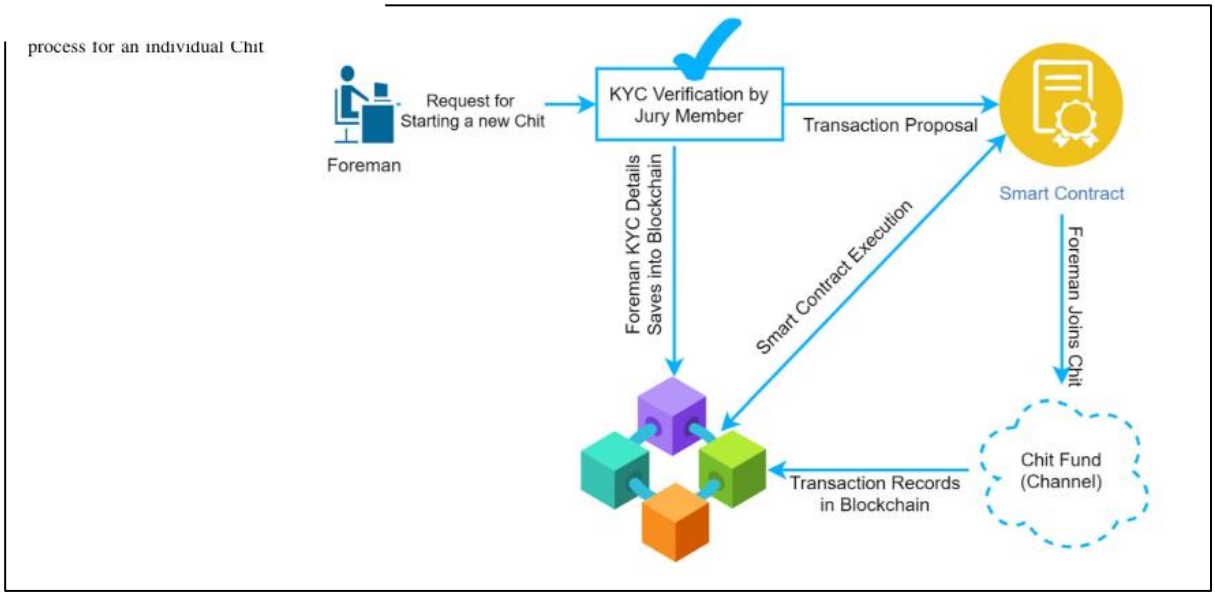
II. **Node 1** This node might represent a verification step where the candidate's eligibility to serve as a juror is confirmed.

III. **Network Algorithm:** A blockchain algorithm is applied, potentially to randomly select jurors from the verified candidates.

IV. **Node 2 (Candidate Selection Algorithm):** This node could indicate that another algorithm is involved in selecting jurors based on specific requirements of the trial.

V. **Selected Jury:** The final outcome shows the chosen jurors for the trial.

3.2.2 How Blockchain Based Chitfund System Works:



I. **Request for KYC Verification by Jury Member:** The process begins with a jury member, presumably someone who vouches for the foreman's identity, requesting Know Your Customer (KYC) verification for the foreman.

II. **Foreman Joins Chit:** The foreman joins the chit fund.

III. **Foreman KYC Details Saves into Blockchain:** The foreman's KYC details are then saved onto the blockchain ledger.

IV. **Transaction Proposal:** A transaction proposal is likely submitted, perhaps by the foreman or the jury member, to initiate the foreman's onboarding process.

V. **Smart Contract Execution:** A smart contract, a self-executing program on the blockchain, is then executed to facilitate the onboarding process.

VI. **Transaction Records in Blockchain (Channel):** The transaction records are stored on the blockchain, likely within a specific channel designated for chit fund transactions.

VII. **Chit Fund (Channel):** This represents the chit fund itself, potentially depicted as a channel on the blockchain network.

3.3 Why Blockchain Can’t Perform well in Chitfund System:

Slow Transactions: Users would experience delays in their transactions, impacting the usability and efficiency of the chit fund system. Imagine waiting days or even weeks for your chit fund contribution to be reflected.

High Transaction Fees: As the network becomes congested, transaction fees might surge due to increased competition for limited block space. This could make chit funds less accessible for participants with limited resources.

Disrupted Workflow: Delayed transactions and high fees could disrupt the smooth operation of the chit fund, potentially hindering timely payouts and creating friction among participants.

CHAPTER-4

4.1 Sidechain based decentralized chitfund system:

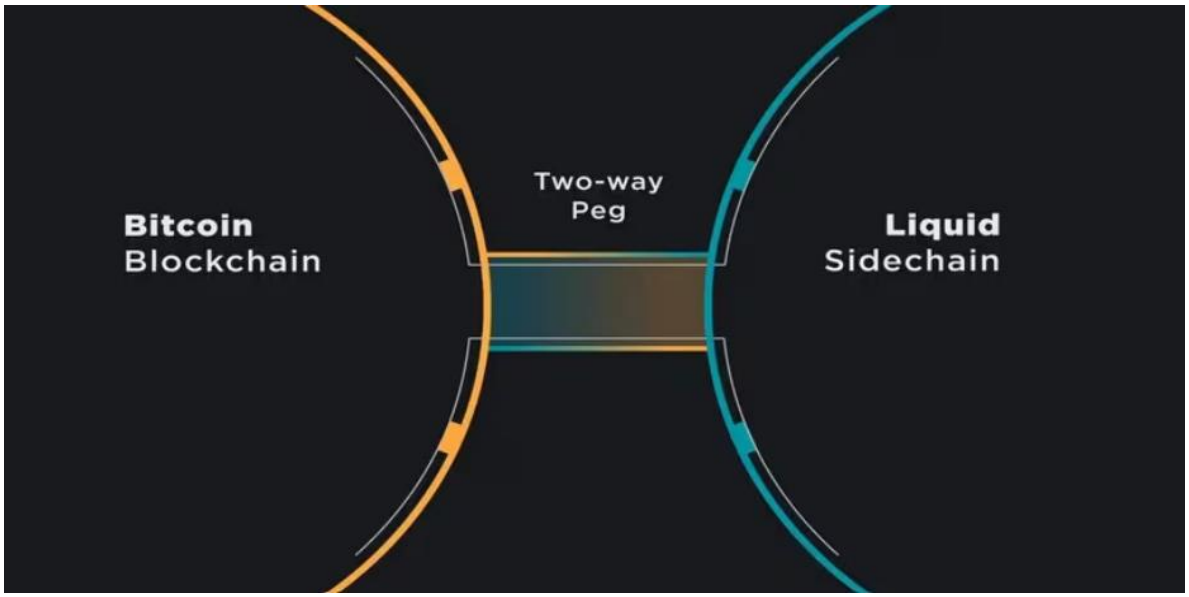
4.1.1 What is a sidechain?

A sidechain is a separate blockchain network that connects to another blockchain – called a parent blockchain or mainnet – via a two-way peg.

These secondary blockchains have their own consensus protocols allowing a blockchain network to improve its privacy and security, and minimize the additional trust required to maintain a network.

A key component of sidechains is their ability to facilitate a smoother asset exchange between the mainnet and the secondary blockchain. This means that digital assets such as tokens can be securely transferred between blockchains – allowing projects to expand their ecosystem in a decentralized manner.

In practical terms, an individual using the Bitcoin mainnet needs to send bitcoin to an output address. This address could be a hard wallet, a hot wallet or a sidechain. Once the transaction is confirmed, a notice of the completed transaction is broadcasted across Bitcoin's network.



4.2 Two-way peg:

Sidechains were developed to facilitate the transfer of digital assets between blockchains, regardless of who is the holder of the assets. Digital assets should be able to be moved without any counterparty risk – meaning that no secondary actor should be able to stop the transfer of the asset from occurring.

To facilitate this transfer back and forth between blockchains, a two-way peg is required. You can think of this as a two-way tunnel with cars driving in both directions.

According to the sidechain white paper, a two-way peg is defined as:

"The mechanism by which coins are transferred between sidechains […] a pegged sidechain is a sidechain whose assets can be imported from and returned to other chains."

4.2.1 Advantages of two-way pegs:

There are two major advantages of using a centralized two-way peg design: 1) Centralized two-way pegs are easy to visualize and implement due to their simplistic design which involves just one entity to oversee the transfer of assets between blockchains. 2) the design could provide extremely fast transfer of funds from the parent blockchain to its sidechain and vice versa as the central entity generally requires a simple proof of locked funds in the lockbox, which they can verify themselves at any given time.

4.3 Smart contracts:

To transfer digital assets between a sidechain and its mainnet, an off-chain process – transactions occurring outside of the parent blockchain – that transfers data between the two blockchains must be built.

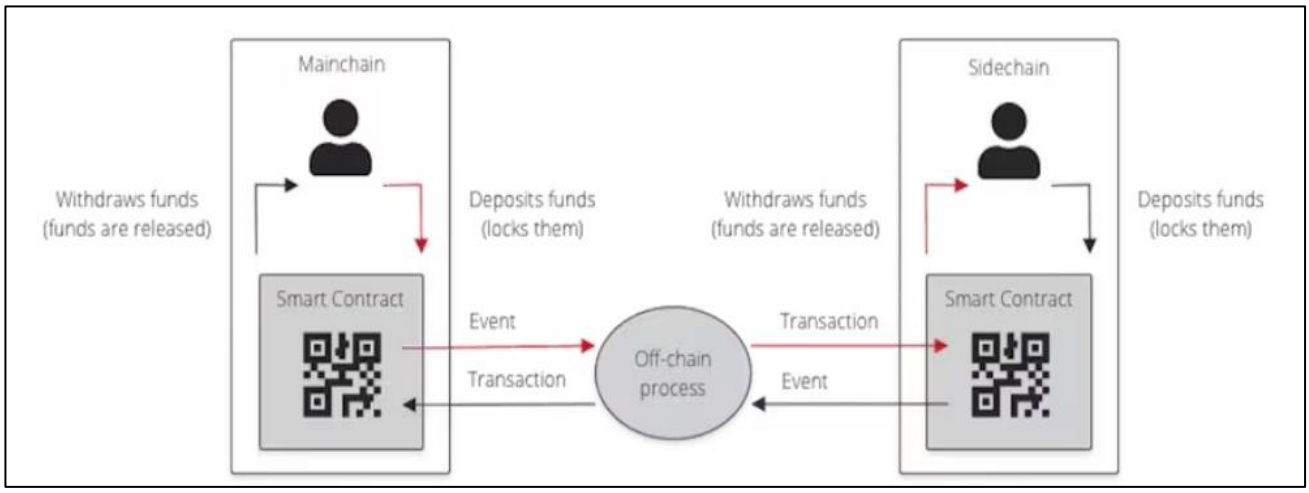
As mentioned above, because the transfer of digital assets between a parent chain and sidechain are imaginary, digital assets are locked in and released on either end of the two blockchains once the transaction has been validated via a smart contract.

Smart contracts are used to ensure that foul play is minimized by enforcing validators on the mainnet and sidechain to act honestly confirming cross-chain transactions. Once a transaction has occurred, a smart contract will notify the mainnet that an event has happened.

Sidechains are used to enhance the scalability and functionality of blockchains like Ethereum or Bitcoin. Popular examples include:

- **Liquid Network** (built on Bitcoin): Aims for faster transactions and more privacy.
- **Polygon** (connected to Ethereum): Offers faster and cheaper transactions compared to the Ethereum mainnet.

You wouldn't directly interact with these sidechains on a platform. Instead, you'd use wallets or applications that support the specific sidechain and the main blockchain it's connected to.



4.4 The potential of sidechains

Sidechains have great potential to expand the scope, scale and dynamics of blockchain technology, allowing previously secluded blockchain networks to become integrated into one common ecosystem.

Taking a macro perspective, imagine a universal blockchain network consisting of numerous blockchains, each with its own consensus mechanism, governance rules and vision yet they all remain independent from one another.

The cross-chain interoperability facilitated by sidechains would allow users to seamlessly navigate across these various projects. This is the fundamental value proposition of sidechains.

As we are going to implement this **Sidechain Technology in Ethereum**, lets discuss how it is going to be implemented in Polygon technology

4.5 Why Polygon Technology:

Polygon PoS is a widely-adopted EVM-compatible sidechain designed for low transaction costs and fast transaction times.

4.5.1 Scalability:

Polygon provides a high-performance scaling solution for Ethereum networks, offering significantly higher throughput and faster transaction speeds compared to the main Ethereum chain. This scalability enhancement enables the processing of a larger number of transactions at lower costs, making it ideal for applications requiring high transaction volumes, like chit funds.

4.5.2 Cost-Effectiveness:

By leveraging Polygon, you can benefit from lower transaction fees and reduced gas costs compared to the Ethereum mainnet. This cost-effective solution makes it more affordable for users to participate in chit fund activities and interact with smart contracts on the sidechain.

4.5.3 Interoperability:

Polygon is designed to be compatible with Ethereum, ensuring seamless interoperability with the Ethereum ecosystem. This compatibility allows for easy integration of existing Ethereum projects and decentralized applications (dApps) with the Polygon sidechain, enhancing the overall ecosystem's connectivity and functionality.

4.5.4 Fast Confirmation Times:

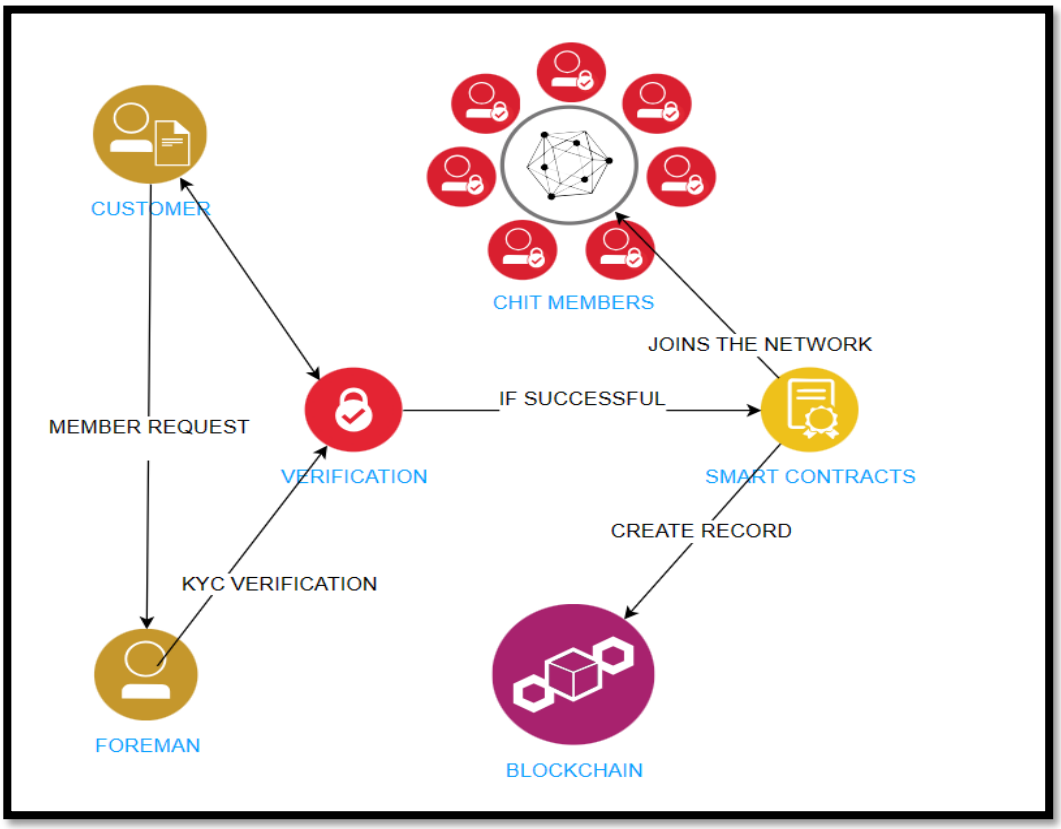
Transactions processed on Polygon sidechains typically have faster confirmation times compared to the Ethereum mainnet. This quick transaction finality ensures that chit fund activities, such as loan sanctioning and jury selections, can be executed promptly, providing users with a seamless and efficient experience.

4.5.5 Security:

Polygon employs a Layer 2 scaling solution that benefits from the security of the Ethereum mainnet. By anchoring sidechain transactions to the Ethereum mainnet, Polygon ensures a high

level of security for chit fund operations, mitigating concerns related to data integrity and asset protection

4.6 How Side chain-based block chain works in chit fund system:



4.7 Steps involved in the selection process:

1. Customer:

When a customer is willing to join the chits, the first step performed by the foreman before including them in the chit members. This process will be done on the basis of how much amount can be contributed from him.

As per his willingness, the foreman will allot the accordingly. If the verification process was not executed. The KYC verification includes Facial recognition and Signature identification etc.

2. Foreman agrees:

Once the verification completed successfully, the foreman will add the member into the chits and includes all the relevant details in the blockchain.

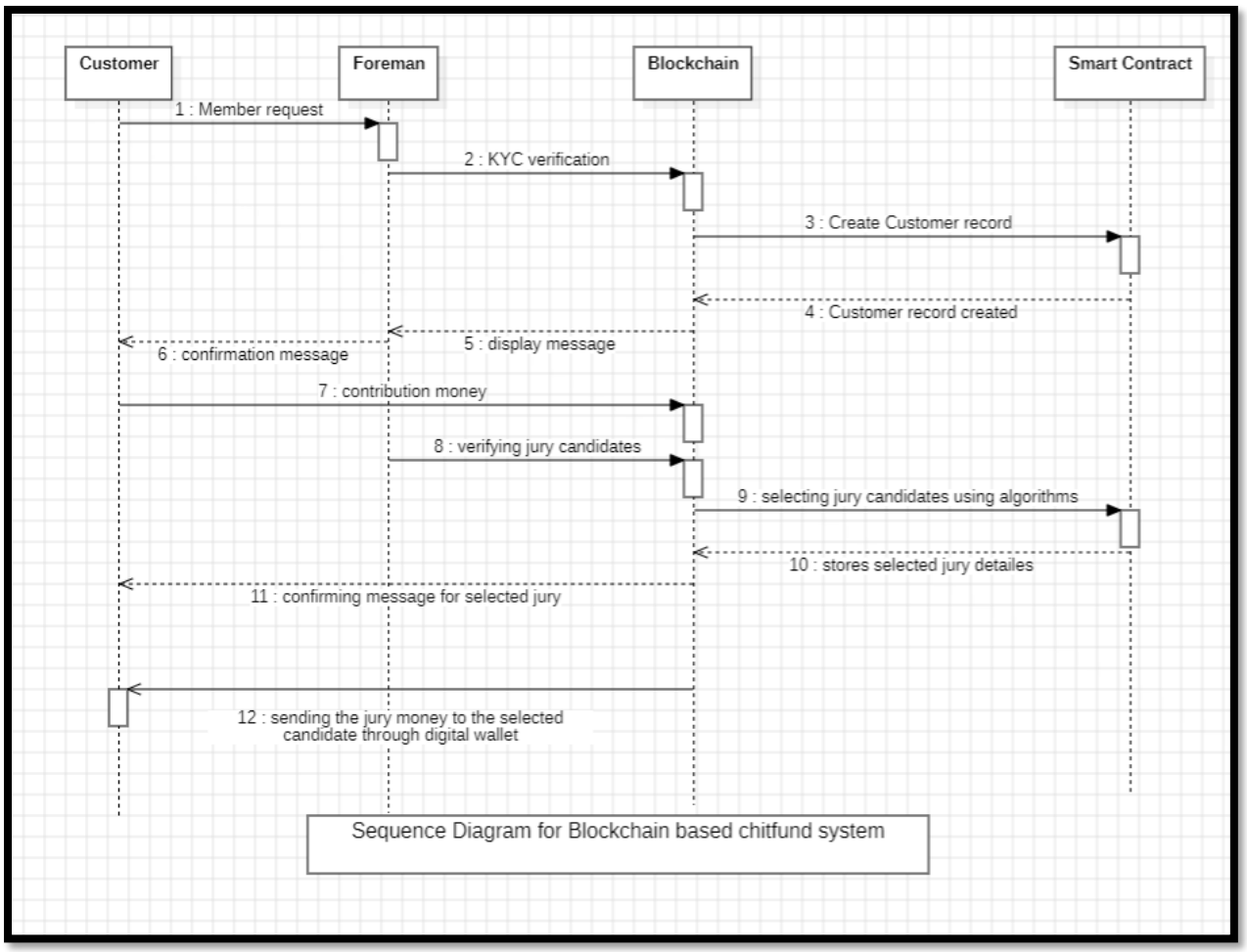
This process involves implementing Smart contracts which can work on its own when it is triggered. Smart contracts are created by high level programming language like: solidity.

3. Joins the Network:

After the completion of the blockchain registration, the member will be allowed to participate in the jury loan and the chits.

The blockchain does not prefer to join the participants who already received in the jury loan and who are default in the monthly contribution.

4.8 Sequence Diagram of how the blockchain model will interact with customer:



1. Entities:

In this case, I have taken Four entities:

Customer / Web User: The person who is going to receive loan or paying contribution in the chits.

Foreman: The person who is going to monitor the chit group by verifying members, verifying candidates for jury loan. The foreman some amount of commission for his job.

Blockchain: A network which is decentralized inorder to minimize the fraud risk involved and to be more transparent.

Smart contract: A set of high-level Programming language (Solidity) which will perform several operations inside the blockchain when the criteria is triggered.

2. Lets discuss about the Candidate verification and Candidate selection process:

A. Member request: The first step will be a participant who is interested in joining the chit funds group requests the foreman to add him.

B. KYC Verification: Now the foreman will check the candidate details meets the criteria for being a member in the chitfund system.

C. Create Customer Record: After all the documents are verified successfully, and the foreman created the account in blockchain which triggers the smart contracts to store the data in the blockchain.

D. Recorded notification: After the customer details were recorded successfully, the blockchain will send notification for the foreman and the customer through broad channels.

E. Making Contribution: Once the customer receiver confirmation message from Blockchain, he should pay the minimum amount (contribution aoumt for the upcoming jury).

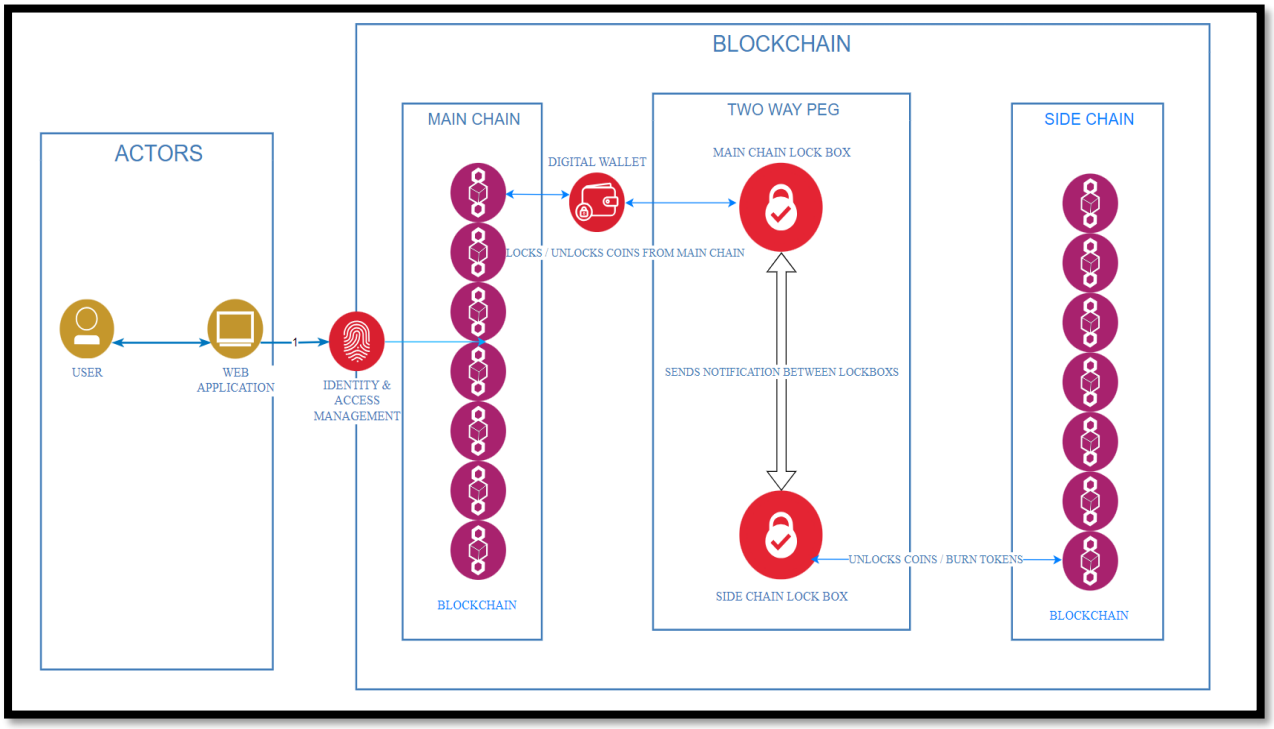
F. Verifying jury candidates: After all customers have to pay their contribution amount to the blockchain, the foreman will check how customers are allowed to get jury loan amount (it won't be provided to the people who already received loans).

G. Selecting Jury candidate using algorithms: After the jury are verified by foreman, the smart contract will be triggered and select the candidate using some random algorithm.

H. Stores data and send notification: As the jury is selected by the smart contract, now the smart contract will store the details of the jury in the blockchain and the notification will send to the customer.

I. Sending Loan amount: After these steps have been completed, the jury loan amount will be sent to the selected customers digital wallet.

4.9 Architecture for sidechain integrated blockchain system:



To understand the fundamentals and design implemented in this two-way peg enabled sidechain, we need to discuss a trivial example in this section. Let us assume a sidechain is attached to a public and permisionless primary blockchain with a two-way peg.

4.10 The primary blockchain:

1) operates a cryptocurrency called MainCoin

2) cannot execute non-trivial smart contracts due to the absence of a Turing complete Virtual Machine.

4.10.1 The sidechain:

1) operates its own cryptocurrency of named SideCoin,

2) has the capability of executing non-trivial smart contracts

3) offers significantly higher transaction rate (i.e. higher transactions per second) than the mainchain. For the sake of simplicity in such multi-blockchain environment, the primary blockchain is called the parent blockchain (or mainchain) and the sidechain attached to it is called a secondary chain (the terms sidechain and secondary chains will be used interchangeably throughout the rest of this paper).

In our example, a two way peg allows the transfer of MainCoins from the mainchain to the sidechain and vice versa at a fixed rate of 1 MainCoin ¼ 1 SideCoin. Suppose a user wishes to transfer 5 MainCoins from the mainchain to the sidechain to play a rock, paper and scissor game with another random user based on a smart contract (where winner takes all and a draw result in no exchange of coins) implemented on the sidechain, then this system could work in the following abstract manner:

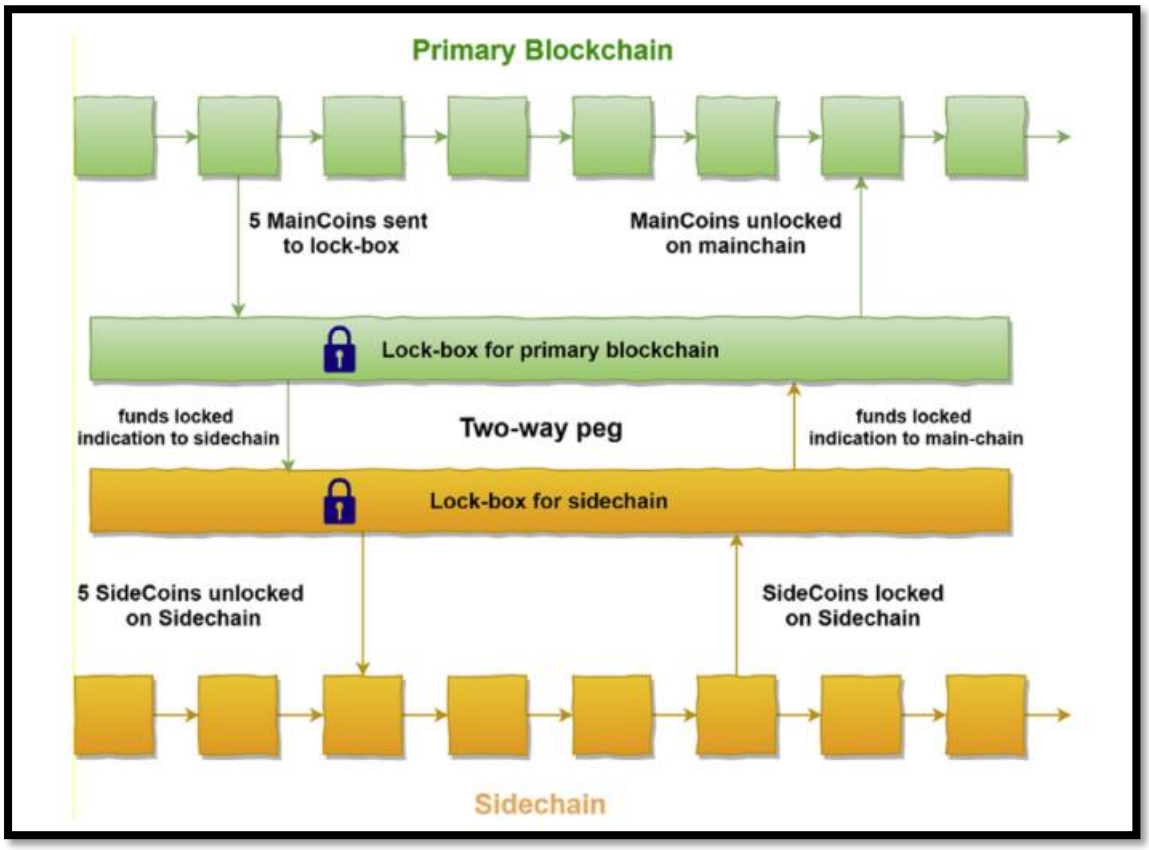
1. The user sends 5 MainCoins to a special address (also known as a lockbox) where the coins are locked and can only be unlocked once funds on sidechain are locked and transferred back to the mainchain.

2. Once the funds locked on the mainchain, 5 SideCoins are created on the sidechain.

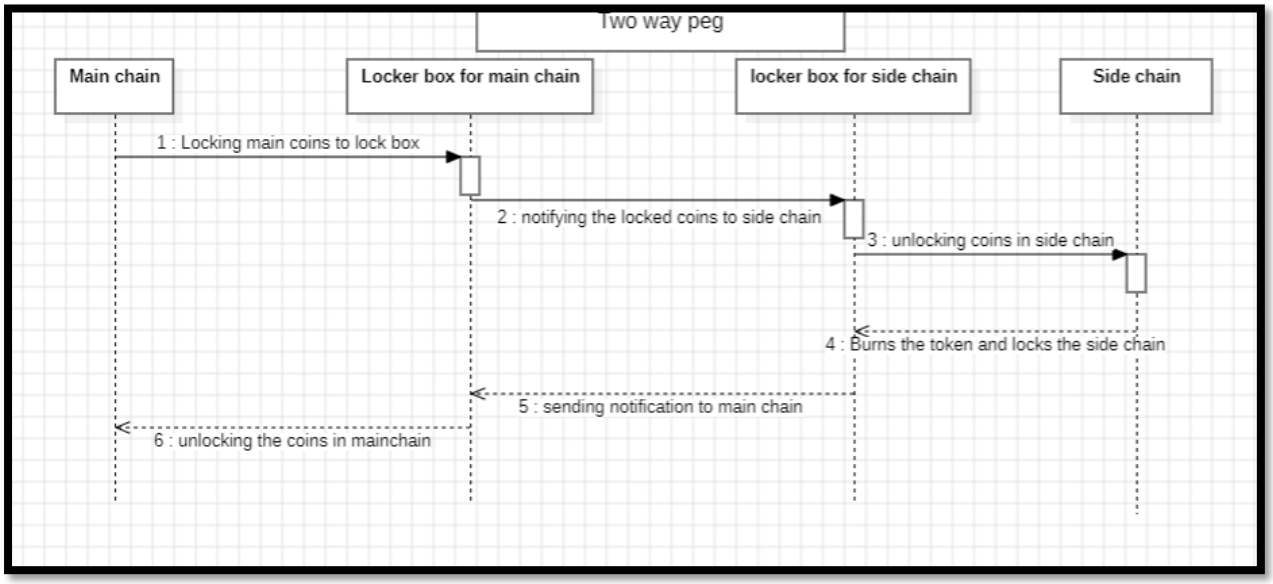
3. The user can now use these SideCoins to play the game of rock, paper and scissors with another random user who is willing to bet the same amount of SideCoins.

4. Depending on the outcome of the game, 10 SideCoins are transferred to the winner or 5 SideCoins are transferred back to their respective owners (in case of a draw).

5. The user(s) can then transfer their funds back to the mainchain, which essentially means that the SideCoins will be locked/destroyed on the sidechain and an equivalent number of MainCoins will be unlocked on the mainchain from the lock box.



4.11 Sequence diagram for the transaction process:



Lets discuss abouts the process in currency transaction through side chain:

1. Locking main coins: In this step, as the user wants to make the transaction faster, he uses sidechain. For accessing your digital coins in the side chain, you need to lock the equal lent amount of digital coins from main chain to lock box.
2. Notifying to sidechain: Once you lock the coins inside the mainchain lock box, it will send the notification to the side chain lock box about the amount of coins locked.
3. Unlocking the sidechain coins: After receiving the notification from the main chain lock box, the sidechain lock box will also unlocks the equal lent amount of coins with same token number.
4. Burns / Locks the side coins: When the user wants the coin to switch to main chain, he can simply burn the side coin which will unlock the main coins from the lock box. Burning the side coin is to make sure that the coin with unique token is existing in only one place.
5. Notifying to mainchain: Once the coins in sidechain burns, it will send notifications to the mainchain lockbox regarding how much coins have been burned along with the token number.
6. Unlocking the coins from mainchain lock box: After receiving the notification from the side chain lock box, the main chain lock box will unlock the locked coins and transfer it to the main blockchain.

4.12 Suggestions:

To enhance the efficiency and effectiveness of the sidechain integration, transaction verification, data storage, smart contracts, and operations within your blockchain-based chit fund system, we can also introduce the sidechain technology in:

4.12.1 Improving Transaction Verification:

- Implement Multi-Signature Verification: Require multiple approvals for critical transactions to enhance security and mitigate risks of unauthorized transactions.
- Utilize Zero-Knowledge Proofs: Employ zero-knowledge proofs for transaction verification to ensure privacy while maintaining the integrity of transactions.
- Integrate Real-time Monitoring: Implement real-time transaction monitoring tools to detect anomalies and suspicious activities for prompt resolution.

4.12.2 Enhancing Data Storage:

- Utilize Distributed File Systems: Implement distributed file systems for scalable and secure data storage, ensuring efficient handling of large volumes of chit fund data.
- Implement Data Encryption: Encrypt sensitive data stored on the sidechain to enhance security and prevent unauthorized access.
- Regular Data Auditing: Conduct regular audits of data storage practices to ensure compliance with data protection regulations and maintain data integrity.

4.12.3 Optimizing Smart Contracts:

- Automate Contract Deployment: Develop automated processes for deploying and managing smart contracts to streamline contract execution and reduce manual errors.
- Implement Upgradeable Contracts: Design smart contracts with upgradability features to easily introduce improvements or fix issues without disrupting ongoing operations.
- Include Error Handling Mechanisms: Integrate error handling mechanisms within smart contracts to gracefully handle exceptions and prevent contract failures.

4.12.4 Streamlining Operations:

Implement Automated Workflows: Utilize automated workflows for routine operations such as user onboarding, reward distributions, and asset transfers to increase operational efficiency.

Utilize Oracles for External Data: Integrate oracles to securely fetch external data required for chit fund operations, enhancing the accuracy and reliability of information.

Regular Performance Testing: Conduct regular performance testing of operational processes to identify bottlenecks and optimize resource utilization for smoother operations.

CHAPTER-5

5.1 Conclusion:

In conclusion, the integration of a sidechain in a blockchain-based chit fund system presents a significant opportunity to enhance scalability, efficiency, data storage and security within the decentralized finance landscape. By designing a system where users request to join chits, undergo KYC verification, and have their details securely stored on the main blockchain, followed by efficient jury selection through smart contracts on the sidechain, and subsequent loan disbursement to digital wallets—all while ensuring data integrity and transparency—the project showcases a thoughtful and innovative approach to revolutionizing traditional chit fund practices.

The architecture diagrams and step-by-step breakdown provided a clear visualization of how the main blockchain and sidechain interact, leveraging a two-way peg mechanism for asset transfers, smart contract interoperability, and seamless user experiences. By incorporating security measures, consensus mechanisms, and robust data storage capabilities, the system ensures a trustworthy environment for chit fund participants while optimizing transaction processing speed and overall performance.

This project not only demonstrates a deep understanding of blockchain technology but also highlights a practical application in the realm of financial services, specifically chit funds. By prioritizing user experience through intuitive interfaces and efficient processes, your project sets a strong foundation for creating a secure and scalable decentralized chit fund ecosystem. The comprehensive integration of the main blockchain and sidechain components showcases a holistic approach to modernizing financial systems, paving the way for greater transparency, accessibility, and reliability in chit fund operations.

Overall, the project's innovative approach to incorporating smart contracts, sidechains, and blockchain technology in the chit fund system underscores your commitment to leveraging cutting-edge technology for financial inclusion and operational efficiency. It sets a benchmark for future advancements in decentralized finance and stands as a testament to the vision for enhancing traditional financial practices through blockchain innovation.

Reference

1. “ChitChain: A Blockchain-Based Technology Framework for Trust Enablement in Decentralized Chit Funds” by H. S. Jennath, V. S. Anoop, S. Asharaf, and Gopinath Saji (2021).

2. “Blockchain-Based Chit Fund System: A Financial Inclusion Tool” by Pawan Kumar and Amrit Lal Sanga (2020).

3. “ChitChain: A Blockchain-Powered Framework for Decentralized Chit Fund Management”.

4. “Blockchain Technology for Chit Fund Management: A Comparative Study” Authors: K. S. Sreejith, K. S. Sreehari, and K. S. Sreelekshmi. (2020).

5. “Blockchain-Based Chit Fund Management System: A Case Study” Authors: R. S. Sabeenian, S. S. Sreeja, and S. S. Sreehari (2019).

6. “Sidechain technologies in blockchain networks: An examination and state-of-the-art review”. Amritraj Singh a, Kelly Click a, Reza M. Parizi a, Qi Zhang b, Ali Dehghantanha 3, Kim-Kwang Raymond Choo 4,

7. Bitcoin, 2011. Bitcoin improvement proposals (BIP) [Online]. Available: https://github.com/bitcoin/bips. (Accessed 4 July 2019).

8. “Liquid.” [Online]. Available: https://blockstream.com/liquid/. [Accessed: 30-Jan2019].

9. BlockStream, “Elements.” [Online]. Available: https://elementsproject.org/. [Accessed:11-Jan-2019].

10. Buterin, V., 2014. A Next-Generation Smart Contract and Decentralized Application Platform. Etherum [Online]. Available: http://buyxpr.com/build/pdfs/EthereumWhitePaper.pdf. (Accessed 5 March 2018)