ENSURING TRUST AND SECURITY IN BLOCKCHAIN-BASED FINANCIAL TRANSACTIONS: A COMPREHENSIVE ANALYSIS AND IMPLEMENTATION

A Capstone Project report submitted
in partial fulfillment of requirement for the award of degree

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE & ENGINEERING
by

SANA ARJUMAN	**2003A53019**
RASAMALLA SAI GANESH	**2003A53018**
PAKA VAMSHI	**2003A53008**
VEMUGANTI SAI CHANDRA	**2003A51243**

Under the guidance of
Mr. P. Chakradhar
Assistant Professor, School of CS&AI.

SR University, Ananthsagar,Warangal,Telagnana-506371

SR University

Ananthasagar, Warangal.

SR
UNIVERSITY

CERTIFICATE

This is to certify that this project entitled **“ENSURING TRUST AND SECURITY IN BLOCKCHAIN-BASED FINANCIAL TRANSACTIONS: A COMPREHENSIVE ANALYSIS AND IMPLEMENTATION"** is the bonafied work carried out by **SANA ARJUMAN, RASAMALLA SAI GANESH, PAKA VAMSHI, VEMUGANTI SAI CHANDRA,** as a Capstone Project phase-1 for the partial fulfillment to award the degree **BACHELOR OF TECHNOLOGY** in **School of Computer Science and Artificial Intelligence** during the academic year 2023-2024 under our guidance and Supervision.

Mr. P. Chakradhar
Asst. Prof.,
SR University
Anathasagar,Warangal

Dr. M.Sheshikala
Professor & Head (CSE),
School of CS&AI,
SR University
Ananthasagar, Warangal.

External Examiner

ACKNOWLEDGEMENT

We owe an enormous debt of gratitude to our Capstone project phase-1 guide **Mr. P. Chakradhar, Asst. Prof.** as well as Head of the School of CS&AI , **Dr. M.Sheshikala, Professor** for guiding us from the beginning through the end of the Capstone Project Phase-1 with their intellectual advices and insightful suggestions. We truly value their consistent feedback on our progress, which was always constructive and encouraging and ultimately drove us to the right direction.

We express our thanks to project co-ordinators **Mr. Sallauddin Md, Asst. Prof., and R.Ashok Asst. Prof.** for their encouragement and support.

Finally, we express our thanks to all the teaching and non-teaching staff of the department for their suggestions and timely support.

ABSTRACT

Our research focuses on a particular use case: blockchain-based safe friend-to-friend transactions. This application is a clear example of what blockchain can do, especially when it comes to safe financial transactions. This study investigates how the unique characteristics of blockchain technology align with the demands of open science, emphasising the potential benefits of promoting a more transparent, cooperative, and reliable research environment. We investigate the unique requirements of the open science ecosystem through a thorough analysis and show how blockchain might meet these needs. A real-world example of blockchain technology in operation is the secure friend-to-friend transactions, which demonstrate how well it works to protect the confidentiality and integrity of financial transactions.

Blockchain is a distributed and decentralized data ledger characterized by essential features such as transparency, immutability, security, and reliability. This innovative technology integrates a peer-to-peer (P2P) protocol, digital encryption techniques, consensus mechanisms, and the utilization of smart contracts. It departs from the traditional reliance on centralized entities for data management, instead opting for shared maintenance by multiple users. This collaborative approach ensures the credibility and integrity of the data contained within the blockchain. Moreover, the blockchain ecosystem is classified into three distinct types: public chains, offering open participation with nodes freely joining or leaving; confidential chains, imposing stringent participation restrictions; and consortium chains, jointly administered by a group of institutions.

Blockchain Technology

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION

Numerous sectors like finance, medicine, manufacturing, and education harness blockchain's distinct features. Blockchain technology (BT) offers gains in trust, collaboration, organization, identification, credibility, and transparency. Our project examines how open science can profit from these aspects. We assess open science ecosystem needs against BT traits, demonstrating its fit as infrastructure. Our use case involves secure friend-to-friend transactions using Blockchain. The application of blockchain for secure financial transactions serves as a pertinent illustration of its capabilities.

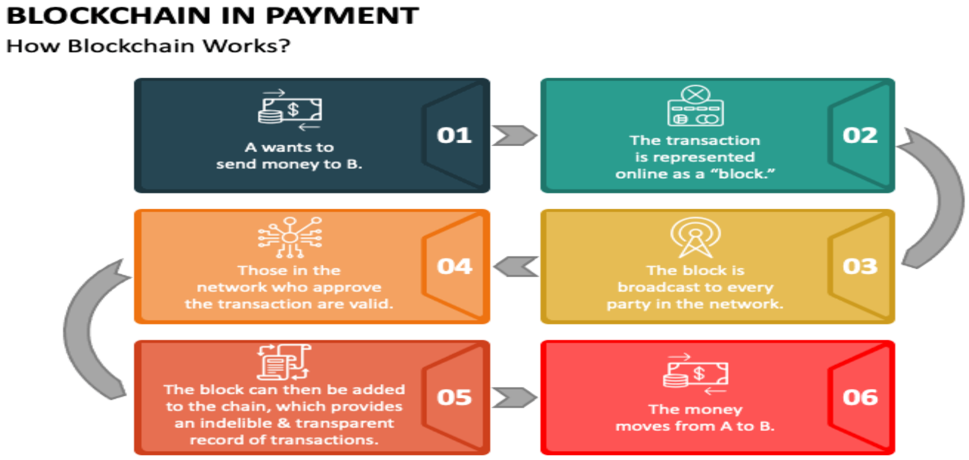

BLOCKCHAIN IN PAYMENT
How Blockchain Works?
01
A wants to send money to B.
02
The transaction is represented online as a "block."
03
The block is broadcast to every party in the network.
04
Those in the network who approve the transaction are valid.
05
The block can then be added to the chain, which provides an indelible & transparent record of transactions.
06
The money moves from A to B.

Fig-1, Working of Blockchain in Money Transaction

As a representative of distributed databases, blockchain stores all user transaction information on the blockchain, which has high requirements for the security performance of blockchain. Blockchain is a decentralised peer-to-peer network. Nodes do not need to trust each other and there is no central node. Therefore, transactions on the blockchain also need to ensure the security of transaction information on unsecured channels and to maintain the integrity of transactions. In blockchain, cryptography technology is mainly used to protect user privacy and transaction information, and ensure data consistency, etc. This paper briefly introduces the cryptographic techniques such as hash algorithm, asymmetric encryption algorithm and digital signature, also elaborates the blockchain infrastructure, the blockchain structure, bitcoin address, digital currency trading and other technologies of blockchain, and also explains how cryptography technology protects privacy and transaction maintenance in the blockchain in detail.

TYPES OF BLOCKCHAINS:

1. **Public Blockchain:** A blockchain that anybody on the planet can peruse, can send transactions to and hope to see them included assuming they are legitimate. This implies anybody can turn out to be important for the organization and partake in the agreement cycle making them permissionless. It is basically impossible to blue pencil exchanges on the organization nor change exchanges reflectively. The substance of the blockchain can be relied upon to be right. Public blockchains are, nonetheless, exceptionally wasteful. The more com-putting power is expected to help trust. In this way, an aggressor would have to obtain 51% of the organization's processing ability to change a section in the blockchain. (e.g., Bitcoin, Ethereum).

2. **Private Blockchain:** A blockchain where access consents are all the more delicately controlled, where privileges to change or try and read the blockchain state are confined to a couple of clients, where just realized hubs are permitted to take part in the organization. Preferably, it is inner for an association. The composes authorizations are kept unified to one association. Private blockchain diminishes counterparty risk by empowering the trading of information without the intermediation of outsiders.

3. **Consortium Blockchain:** It is a blockchain where pre-chosen set of hubs control the agreement interaction.

4. **Permissioned Blockchain:** It is a blockchain where we can permit explicit activities to be performed exclusively by unambiguous addresses. The members in the organization can limit who can partake in the agreement system and who can make a savvy agreement and give the expert for certain members to give the approval of blocks of exchanges. A control access layer into the blockchain hubs is utilized. Nonetheless, bring up their issues, Who has the position to allow authorization? A consent blockchain may cause its proprietors to have a solid sense of reassurance, giving the information base thorough security and protection capacities yet should be

visible as disregarding the possibility of blockchain on the grounds that main a few members have more control, and that implies they can make changes whether other organization members concur.

HASH AND BLOCK STRUCTURE:

The hash calculation is a capability that maps a succession of messages of any length to a more limited fixed-length esteem, and is described by weakness, unidirectionality, crash opposition, and high responsiveness. Hash is generally used to guarantee information uprightness, that is to say, to check the information has been illicitly messed with. At the point when the information tried changes, its hash esteem likewise changes correspondingly. In this manner, regardless of whether the information is in a hazardous climate, the trustworthiness of the information can be identified in light of the hash worth of the information.

SHA is a kind of cryptographic hash capability gave by the Public Foundation of Guidelines and Innovation (NIST) with the overall qualities of a cryptographic hash capability. The SHA256 calculation is a class of the SHA-2 calculation bunch, which produces a 256-bit message digest. The calculation's computation interaction incorporates two phases: message preprocessing and primary circle. In the message preprocessing stage, parallel cycle filling and message length filling are performed on the data of any length, and the filled message is separated into a few 512-digit message blocks. In the principal circle stage, each message block is handled by a pressure capability. The contribution of the ongoing pressure capability is the result of the past pressure capability, and the result of the last pressure capability is the hash worth of the first message.

For blockchain, hash capabilities can be utilized to perform block and exchange trustworthiness check. In the blockchain, the hash worth of the data of the past block is put away in the header of each block, and any client can contrast the determined hash esteem and the put away hash esteem. Thus, the trustworthiness of the data of the past block is identified. Likewise, the hash capability can be utilized to produce public-private key matches.

The hash pointer is an information structure that contains, notwithstanding the standard pointers, a few information data and secret key hashes related with the data. A typical pointer is utilized to recover data, and a hash pointer is utilized to check that the data has been altered. The blockchain is a rundown of hash pointers, every one of which is associated by utilizing a hash esteem. It is confirmed by the hash esteem whether the information contained in the block is changed, in this way guaranteeing the respectability of the block data.

SECURITY OF BLOCKCHAIN:

Before we make a plunge blockchain, let us ponder momentarily the blockchain itself. It essentially alludes to a dispersed information base that offers the highlights of decentralization, security, detectability, dependability, and unchanging nature. Blockchain removes the requirement for conventional methodologies for keeping up with focal hubs and presents the new methodology for common support of hubs by numerous clients.

Thus, it can share data management with different gatherings and guarantee wanted degrees of validity and information honesty. Another significant angle relating to blockchain alludes to the three unmistakable sorts of blockchain stages. The kinds of blockchain stages incorporate public chain, confidential chain, and partnership chain. Every one of the hubs in a public chain could undoubtedly partake or pull out from the blockchain as per their inclinations.

Then again, private blockchains force explicit circumstances to decide the qualification of the taking an interest hubs. The partnership chain works under the administration of various partaking associations working closely together. Throughout the long term, blockchain has been to a great extent connected with the monetary business. Nonetheless, it has exhibited the promising potential for enhancing various areas close by reshaping the basic principles of our general public.

Anyway, what is the connection among blockchain and cryptography? The blockchain fills in as a delegate of circulated data sets by putting away all the exchange data of clients on the blockchain. Hence, it is sensible to distinguish a significantly more popularity for security execution in the blockchain.

Since blockchain works with a decentralized, distributed network model, there is no single hub, and hubs don't need to trust each other. Thus, blockchain should likewise guarantee fitting protections for exchange data on unstable channels while keeping up with exchange trustworthiness. Consequently, cryptography turns into a fundamental prerequisite for blockchain to defend client exchange data and security close by guaranteeing information consistency.

CRYPTOCURRENCY: RISE OF BLOCKCHAIN TECHNOLOGY

Blockchain's most notable use (and perhaps generally disputable) is in digital currencies. Cryptographic forms of money are computerized monetary standards (or tokens), like Bitcoin, Ethereum or Litecoin, that can be utilized to purchase labor and products. Very much like a computerized type of money, crypto can be utilized to purchase everything from your lunch to your next home. In contrast to cash, crypto utilizes blockchain to go about as both a public record and an improved cryptographic security framework, so online exchanges are constantly recorded and gotten.

BEYOND BITCOIN : ETHEREUM BLOCKCHAIN

Initially made as the super straightforward record framework for Bitcoin to work on, blockchain has for some time been related with cryptographic money, however the innovation's straightforwardness and security has seen developing reception in various regions, quite a bit of which can be followed back to the improvement of the Ethereum blockchain.In late 2013, Russian-Canadian engineer Vitalik Buterin distributed a white paper that proposed a stage joining customary blockchain usefulness with one key distinction: the execution of PC code. Hence, the Ethereum Task was conceived.

Ethereum blockchain allows engineers to make refined programs that can speak with each other on the blockchain.

2. RELATED WORK

1. “Bitcoin: A Peer-to-Peer Electronic Cash System (Nakamoto, 2008)”: This seminal work by Satoshi Nakamoto introduced the concept of blockchain and cryptocurrency. It serves as the foundation for the entire blockchain ecosystem, and its principles are at the core of many blockchain projects.

2. “Security Research in Key Technologies of Blockchain (Zhu, Gan, Deng, 2016)”: Zhu, Gan, and Deng's research provides valuable insights into the security aspects of blockchain technology. It explores various key technologies and their security implications, which is crucial in understanding the challenges and solutions in the blockchain domain.

3. “Research on Blockchain Performance Improvement of Byzantine Fault-Tolerant Consensus Algorithm Based on Dynamic Authorization (Liu, 2017)”: Liu's research focuses on improving the performance of blockchain through Byzantine fault-tolerant consensus algorithms and dynamic authorization. This work is relevant for understanding how consensus mechanisms impact the efficiency and security of blockchain networks.

4. “Cryptanalysis of the Hash Functions MD4 and RIPEMD (Wang, Lai, Feng, 2005)”:Wang, Lai, and Feng's work is significant for understanding the vulnerabilities of hash functions used in blockchain technology. Cryptanalysis of hash functions is essential for assessing the security of blockchain systems.

5. “Cryptography in Blockchain (Wang, Wu, 2017)”: Wang and Wu's paper explores the role of cryptography in blockchain technology. This is relevant for understanding the cryptographic techniques used to secure data and transactions in blockchain systems.

6. “Current Status and Prospects of Blockchain Technology Development (Yuan, Wang, 2016)”: Yuan and Wang's work provides an overview of the current status and future prospects of blockchain technology. It offers insights into the evolution and trends in the blockchain industry.

7. “Elliptic Curves Suitable for Cryptosystems (Miyaji, 1994)”: Miyaji's research on elliptic curves is relevant to blockchain technology, as elliptic curve cryptography (ECC) is widely used for securing blockchain transactions. Understanding ECC is essential for comprehending blockchain security.

8. “Prospective Review of Blockchain Technology and Application (He, Yu, Zhang, 2017)”: He, Yu, and Zhang's work offers a forward-looking perspective on blockchain technology and its applications. It provides insights into potential future developments and use cases for blockchain.

9. “The Data Block Chain of the Key Technologies Consistency (Zhai, Li, 2018)”: Zhai and Li's research delves into data consistency in blockchain technology. Consistency is a critical aspect of blockchain databases, and this work can shed light on how to maintain data integrity in distributed ledgers.

10. “Research and Application of Key Technologies for Decentralized Transactions Based on Blockchain (An, 2017)”: An's research focuses on the key technologies for decentralized transactions in blockchain. Understanding how blockchain enables secure and transparent transactions is fundamental to comprehending its real-world applications.

3. PROBLEM STATEMENT

The contemporary financial and transactional landscape is burdened with a host of inefficiencies and vulnerabilities that impede the seamless exchange of assets and data. In light of this, there is a pressing need for a solution that addresses these issues and propels us toward a more accurate, efficient, and secure transaction ecosystem. This problem statement encapsulates the overarching aim to rectify the following challenges:

Firstly, the problem of improved transaction accuracy must be tackled. Current transaction systems are prone to errors and discrepancies, primarily due to fragmented databases and lack of synchronized verification. Blockchain technology presents a promising avenue for resolving this problem by necessitating validation from multiple nodes, minimizing the likelihood of inaccuracies. In case one node's database contains errors, the collaborative network ensures that discrepancies are swiftly detected and rectified, thereby enhancing overall transaction accuracy.

Secondly, the challenge of enhanced transfer efficiency necessitates attention. Conventional international financial and asset transfers often suffer from protracted delays, subject to manual confirmations by banks and authorities operating within specific working hours. The implementation of blockchain, functioning around the clock, stands as a solution to this issue. It streamlines cross-border transactions, rendering them significantly swifter, and reduces reliance on intermediaries, thus eliminating unnecessary waiting times.

Furthermore, the elimination of intermediaries presents a paramount concern that must be addressed. Intermediaries, such as banks, introduce complexities, time constraints, and additional costs to the transaction process. Blockchain technology has the potential to empower direct transaction confirmation between involved parties, circumventing the need for third-party involvement and, in turn, saving time and resources.

Lastly, the imperative problem of heightened security cannot be understated. Traditional transaction systems are susceptible to fraudulent activities, compromising the integrity of exchanges. Blockchain's decentralized network architecture acts as a robust solution in this regard, substantially reducing the possibility of fraudulent transactions and ensuring a higher level of security.

In summation, the challenges of transaction accuracy, transfer efficiency, intermediary involvement, and security deficiencies within contemporary financial and asset exchange systems necessitate a comprehensive solution that embraces blockchain technology to usher in a more precise, efficient, and secure transactional environment.

4. REQUIREMENT ANALYSIS

The project necessitates essential resources: skilled knowledge for both front-end (HTML page). Utilize various HTML elements like headings, paragraphs, links, images, and lists to structure and present content. CSS can be used for styling, enhancing the page's visual appeal. Finally, save the file with a ".html" extension and open it in a web browser to view the rendered page and back-end (Visual Studio Code), suitable hardware, software like Visual Studio Code, and blockchain tools.

Software Requirements:

IDE - Visual Studio Code

Hardware Requirements:

Any Hardware as Mobile, Laptop or Desktop.

5. RISK ANALYSIS

Market Volatility:

The inherent volatility in the cryptocurrency market can pose a significant risk to the project's financial stability. Fluctuations in the value of cryptocurrencies, which may be used within the blockchain system, can impact budgetary considerations, affecting both revenue and expenses. Prudent risk mitigation strategies, such as hedging or diversifying currency holdings, need to be explored to minimize the potential impact of market volatility on the project's financial health.

Interoperability Challenges:

Integration with existing systems and technologies poses another potential risk. Incompatibility issues with legacy systems or other blockchain platforms may hinder smooth operations. Comprehensive testing and compatibility assessments are essential to identify and address interoperability challenges. Strategic planning for phased implementations and potential system upgrades may be necessary to ensure seamless integration with existing infrastructures.

Scalability Concerns:

As the project gains traction and the volume of transactions increases, scalability becomes a critical consideration. Inadequate scalability could lead to performance issues, slower transaction processing times, and increased costs. Scalability challenges may emerge both in terms of technological infrastructure and operational processes.

Data Privacy and Confidentiality:

While blockchain is inherently designed to ensure data integrity, ensuring privacy and confidentiality remains a concern. The decentralized nature of the technology can make it challenging to manage access control and protect sensitive information. Robust encryption methods, compliance with data protection regulations, and continuous monitoring are necessary

6. FEASIBILITY ANALYSIS

Technical Feasibility:

The technical feasibility analysis delves into the capabilities and readiness of the technology required for the blockchain-based friend-to-friend transactions. This involves assessing the availability of necessary hardware, software, and skilled personnel. It explores whether the existing infrastructure can support the implementation of blockchain, ensuring that the technology is scalable, secure, and can handle the anticipated transaction volume. Additionally, considerations for interoperability with existing systems and the ability to integrate with other technologies are crucial aspects of the technical feasibility assessment.

Financial Feasibility:

The financial feasibility analysis is pivotal in determining the economic viability of the blockchain project. It scrutinizes the cost considerations associated with the implementation, including hardware and software acquisition, development, maintenance, and operational expenses. A detailed budget is constructed, outlining both initial and ongoing costs. Moreover, potential revenue streams and return on investment (ROI) are evaluated, taking into account market demand and competition. This financial scrutiny ensures that the project aligns with the available budgetary resources and offers a sustainable economic model.

Market Feasibility:

Market feasibility assesses the demand and acceptance of the blockchain-based friend-to-friend transactions within the targeted user base. This involves studying the market dynamics, potential user adoption, and competition in the realm of secure peer-to-peer transactions. Understanding customer needs, preferences, and expectations is crucial for tailoring the blockchain solution to meet market requirements effectively. Furthermore, the analysis examines potential partnerships, collaborations, or alliances that could enhance market penetration and contribute to the project's success in the competitive landscape.

Legal and Operational Feasibility:

Legal feasibility examines the project's compliance with existing laws and regulations related to financial transactions, data protection, and blockchain technology. It ensures that the implementation adheres to legal standards and mitigates potential risks associated with regulatory frameworks. Operational feasibility, on the other hand, focuses on the day-to-day execution of the blockchain project. This includes evaluating the impact on current workflows, assessing scalability for future growth, and identifying potential bottlenecks. Stakeholder support is crucial in both legal and operational aspects, emphasizing the need for clear communication and collaboration to address any challenges that may arise during implementation.

7. PROPOSED SOLUTION OR APPROACH OR TECHNIQUE

Existing: FIFO is a straightforward method to implement in traditional centralized systems, requiring minimal additional infrastructure. FIFO alone does not inherently provide the same level of security as blockchain, making it more vulnerable to tampering and fraud.

1. Paytm using a checksum signature: This is a common practice to ensure the integrity of API requests and responses. Checksums, often generated using hashing algorithms like SHA256, help verify that the data has not been tampered with during transit.

2. Google using ECDSA with NIST P-256 and SHA-256: This is accurate as per the provided information. Google uses strong cryptographic algorithms for signing messages to ensure their authenticity and integrity.

3. Google Pay and Host Card Emulation (HCE): This is also accurate. Google Pay uses HCE, which allows card data to be stored in the cloud rather than a physical secure element. Android's open-source nature and the diversity of device versions make HCE a practical solution for mobile payments.

Proposed: Block Hash

A Block Hash is basically a reference number for a block in the blockchain.This lets us create one-way encrypted messages. Cryptography techniques like hashing make Blockchain create secure transactions.

A hash function is an algorithm that takes some data (usually an encoded string) and returns a unique identifier, often named “digest” or “signature.” This last part is vital; with a hash function, a slight difference in the input produces a radically different identifier as an output.

Blockchain technology can be highly beneficial for an electronic money transaction project. Blockchain offers several key features that can enhance the security, transparency, and efficiency of such a system. Here are some ways blockchain can be helpful:

Decentralization: Blockchain operates on a decentralized network of computers, known as nodes. This removes the need for a central authority to manage transactions, reducing the risk of single points of failure and increasing resilience.

In this project we are using Sha-256 Algorithm for security reasons instead of using many algorithms which has its own functionalities to save the maintainance cost which will be charged to the customers in the form of transaction fee and which will be efficient for the updating/modification in the code.

8. ARCHITECTURE DIAGRAM/FLOW CHART

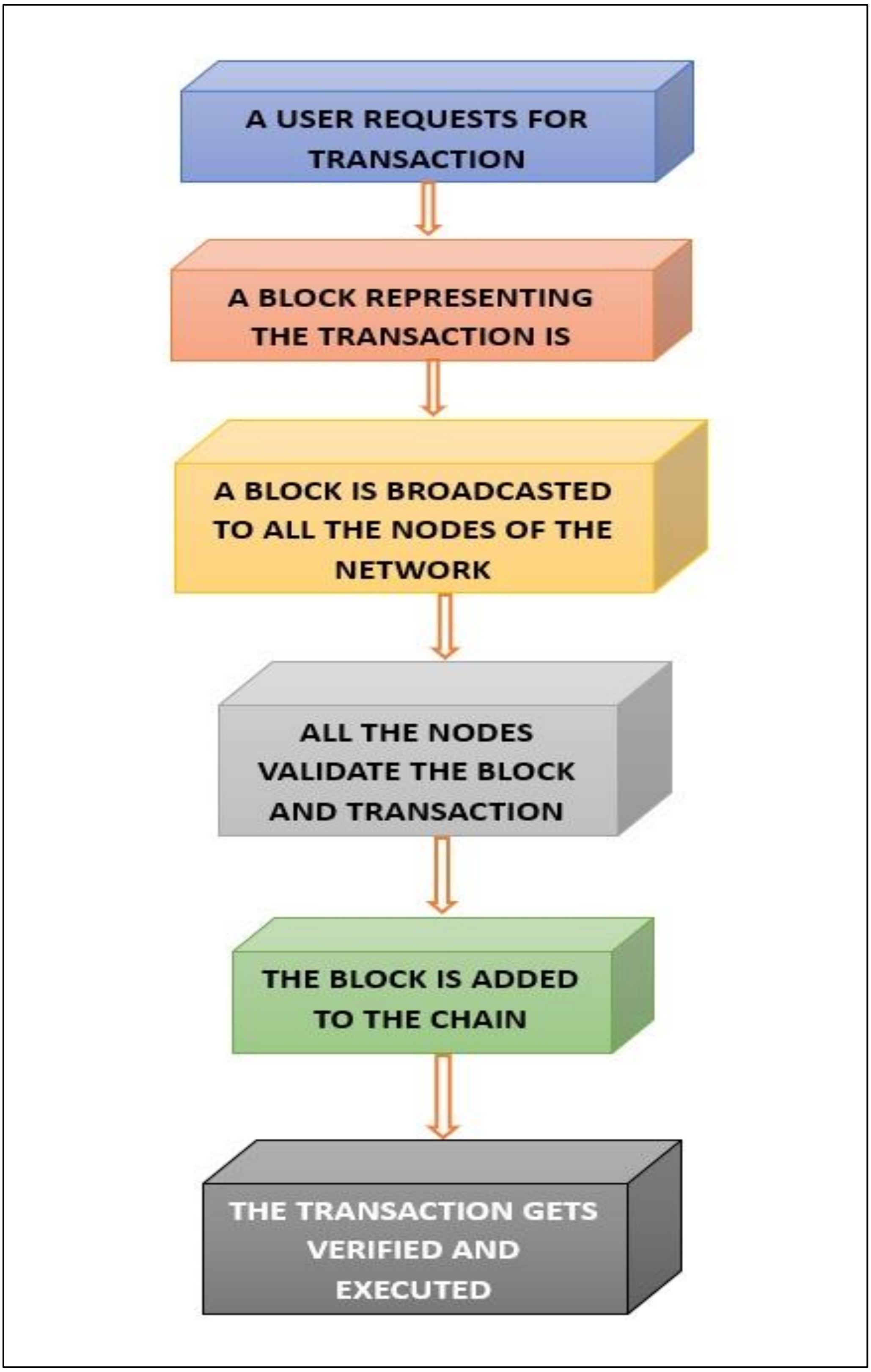

A USER REQUESTS FOR TRANSACTION
A BLOCK REPRESENTING THE TRANSACTION IS
A BLOCK IS BROADCASTED TO ALL THE NODES OF THE NETWORK
ALL THE NODES VALIDATE THE BLOCK AND TRANSACTION
THE BLOCK IS ADDED TO THE CHAIN
THE TRANSACTION GETS VERIFIED AND EXECUTED

Fig-2, Working Architecture of Blockchain Technology

WORKING OF BLOCKCHAIN:

The name blockchain is not really incidental: The computerized record is frequently portrayed as a "chain" that is comprised of person "blocks" of information. As new information is intermittently added to the organization, a new "block" is made and joined to the "chain." This includes all hubs refreshing their form of the blockchain record to be indistinguishable.

How these new blocks are made is vital to why blockchain is viewed as exceptionally secure. A larger part of hubs should check and affirm the authenticity of the new information before another block can be added to the record. For a cryptographic money, they could include guaranteeing that new exchanges in a block were not fake, or that coins had not been spent at least a few times. This is not quite the same as an independent data set or calculation sheet, where one individual can make changes without oversight.

"When there is agreement, the block is added to the chain and the fundamental exchanges are kept in the dispersed record," says C. Neil Dark, accomplice in the fintech practice regions at Duane Morris LLP. "Blocks are safely connected together, framing a protected computerized chain from the outset of the record to the present."

Exchanges are normally gotten utilizing cryptography, meaning the hubs need to tackle complex numerical conditions to deal with an exchange.

"As a compensation for their endeavors in approving changes to the common information, hubs are ordinarily compensated with new measures of the blockchain's local money — e.g., new bitcoin on the bitcoin blockchain," says Sarah Shtylman, fintech and blockchain counsel with Perkins Coie.

USAGE OF BLOCKCHAIN:

Blockchain innovation is utilized for the overwhelming majority various purposes, from offering monetary types of assistance to directing democratic frameworks.

1. Cryptocurrency:

The most well-known utilization of blockchain today is as the foundation of cryptographic forms of money, as Bitcoin or Ethereum. At the point when individuals purchase, trade or spend digital money, the exchanges are recorded on a blockchain. The more individuals use digital money, the more inescapable blockchain could turn into.

"Since digital forms of money are unstable, they are not yet utilized a lot to buy labor and products. However, that is changing as PayPal, Square and other cash administration organizations make computerized resource benefits extensively accessible to merchants and retail clients," notes Patrick Daugherty, senior accomplice of Foley and Lardner and lead of the company's blockchain team.

2. Banking:

Past digital money, blockchain is being utilized to handle exchanges in government issued money, similar to dollars and euros. This could be quicker than sending cash through a bank or other monetary foundation as the exchanges can be checked all the more rapidly and handled beyond typical business hours.

3. Supply Chain Monitoring:

Supply chains include monstrous measures of data, particularly as merchandise go from one area of the planet to the next. With conventional information stockpiling strategies, following the cause of issues, similar to which seller low quality merchandise came from can be hard. Putting away this data on blockchain would make it simpler to return and screen the production network, for example, with IBM's Food Trust, which utilizes blockchain innovation to follow food from its gather to its utilization.

4. Voting:

Experts are looking into ways to apply blockchain to prevent fraud in voting. In theory, blockchain voting would allow people to submit votes that couldn’t be tampered with as well as would remove the need to have people manually collect and verify paper ballots.

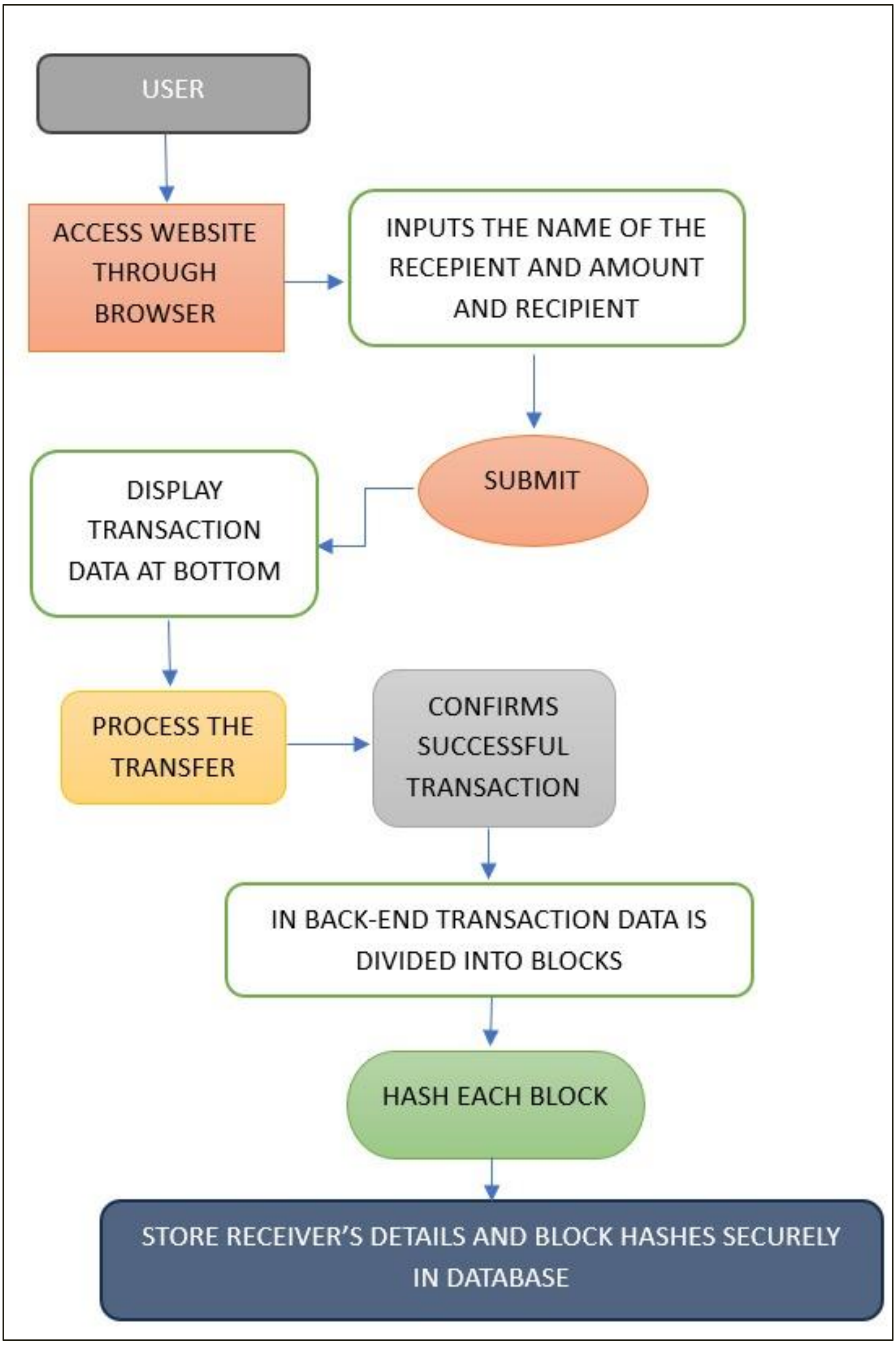

USER
ACCESS WEBSITE THROUGH BROWSER
INPUTS THE NAME OF THE RECEPIENT AND AMOUNT AND RECIPIENT
SUBMIT
DISPLAY TRANSACTION DATA AT BOTTOM
PROCESS THE TRANSFER
CONFIRMS SUCCESSFUL TRANSACTION
IN BACK-END TRANSACTION DATA IS DIVIDED INTO BLOCKS
HASH EACH BLOCK
STORE RECEIVER'S DETAILS AND BLOCK HASHES SECURELY IN DATABASE

Fig-3, Flowchart of approach.

ADVANTAGES OF BLOCKCHAIN:

1. High Accuracy:

Since a blockchain exchange should be checked by different hubs, this can diminish blunder. On the off chance that one hub has a misstep in the data set, the others would see it's unique and catch the blunder.

Conversely, in a customary data set, in the event that somebody commits an error, it could be bound to go through. Furthermore, every resource is separately distinguished and followed on the blockchain record, so there is no way of twofold spending it (like an individual overdrawing their financial balance, in this manner burning through cash two times).

2. Extra Security:

Hypothetically, a decentralized organization, as blockchain, makes it almost unthinkable for somebody to make fake exchanges. To enter in fashioned exchanges, they would have to hack each hub and change each record. While this isn't really unimaginable, numerous digital money blockchain frameworks utilize proof-of-stake or proof-of-work exchange confirmation strategies that make it troublesome, as well as not to members' greatest advantage, to add false exchanges**.**

3. More Efficiency:

Since blockchains work every minute of every day, individuals can make more effective monetary and resource moves, particularly universally. They don't have to hang tight days for a bank or an administration office to affirm everything physically.

DISADVANTAGES OF BLOCKCHAIN:

1. Limit on Transactions per second:

Considering that blockchain relies upon a bigger organization to endorse exchanges, there's a cutoff to how rapidly it can move. For instance, Bitcoin can handle 4.6 exchanges each second versus 1,700 every second with Visa. Furthermore, expanding quantities of exchanges can make network speed issues. Until this improves, versatility is a test.

2. Risk of asset lose:

A few computerized resources are gotten utilizing a cryptographic key, similar to digital money in a blockchain wallet. You really want to monitor this key cautiously.

"Assuming the proprietor of a computerized resource loses the confidential cryptographic key that gives them admittance to their resource, presently it is basically impossible to recuperate it — the resource is gone for all time," says Dark. Since the framework is decentralized, you can't call a focal power, similar to your bank, to request to recapture access.

9. SIMULATION SETUP

Software Requirements: Visual Studio Code for front-end and back-end development

Hardware Requirements: Any Hardware as Mobile, iPad, Laptop or Desktop

Programming: Front-End: HTML (To Design Web Page), Back-End: Python (Flask)

- Python: Ensure that you have Python installed on your system. You can download and install Python from the official website: Python Downloads.
- Flask: You'll need to install the Flask web framework to run the web application. You can install Flask using pip: pip install Flask
- Web Browser: To interact with the web application, you'll need a web browser.
- HTML and CSS: Your front-end code is in HTML and CSS. No additional installations are required for these, as they are standard web technologies.
- Jinja2 (Optional): Flask uses Jinja2 as a template engine for rendering HTML templates. It's typically included with Flask, but ensure that it's available.
- Bootstrap (Optional): Your HTML code includes Bootstrap CSS classes, which enhance the styling of the web application. You don't need to install Bootstrap separately; your code references it from a CDN (Content Delivery Network).
- Save the Python code in a file with a .py extension (e.g., blchain.py).
- Save the HTML code in a file with an .html extension (e.g., index.html).
- Run the Python application by executing: python blchain.py
- You should see output indicating that the Flask web server is running. It will provide a URL (usually, http://127.0.0.1:5000/) where your application is accessible.
- Open a web browser and enter the provided URL to access the blockchain-based money transfer system.

10. IMPLEMENTATION

- We will Write code in Visual Studio Code.
- Will use libraries like import hashlib,json,sys.
- Create a function to generate exchanges between friends.
- We'll construct our transactions to always be between the two users of our system, and make sure that the deposit is the same magnitude as the withdrawal- i.e. that we're neither created nor destroying money.
- Now we will construct blocks
- Next step: making our very own blocks! We'll take the first k transactions from the transaction buffer, and turn them into a block. Before we do that, we need to define a method for checking the validity of the transactions we've pulled into the block. We'll define our own, very simple set of rules which make sense for a basic token system: The sum of deposits and withdrawals must be 0 (tokens are neither created nor destroyed) A user's account must have sufficient funds to cover any withdrawals If either of these conditions are violated, we'll reject the transaction.
- Each block contains a batch of transactions, a reference to the hash of the previous block (if block number is greater than 1), and a hash of its contents and the header
- For each block, we want to collect a set of transactions, create a header, hash it, and add it to the chain
- Now that we know how to create new blocks and link them together into a chain, let's define functions to check that new blocks are valid- and that the whole chain is valid.

Methodology:

1. Development Environment and Libraries:

Utilize Visual Studio Code as the primary integrated development environment.

Employ essential libraries such as hashlib, json, and sys for cryptographic operations, data serialization, and system-level interactions.

2. Transaction Generation Function:

Create a Python function to generate secure exchanges between friends within the system.

Ensure that transactions are consistently between two users, maintaining a balance by matching withdrawal and deposit magnitudes.

3. Block Construction:

Develop a block creation process to convert transactions from the buffer into blocks.

Define a method for validating transactions within a block using a set of simple rules:

Ensure the sum of deposits and withdrawals is 0, adhering to the principle that tokens are neither created nor destroyed.

Verify that a user's account has sufficient funds to cover any withdrawals.

Reject transactions that violate these conditions.

4. Block Structure:

Define the structure of each block, encompassing:

A batch of transactions.

A reference to the hash of the previous block (if the block number is greater than 1).

A hash of the block's contents and header.

5. Block Addition to the Chain:

Implement a mechanism to collect transactions, create a header, hash it, and add the block to the blockchain.

Ensure the integrity and consistency of the blockchain by properly linking new blocks to the previous ones.

6. Validation Functions:

Define functions to check the validity of new blocks and ensure the integrity of the entire blockchain.

Validate individual blocks by verifying the consistency of transactions and adherence to defined rules.

Check the entire blockchain for consistency, confirming that each block's reference to the previous block is accurate.

7. Testing and Debugging:

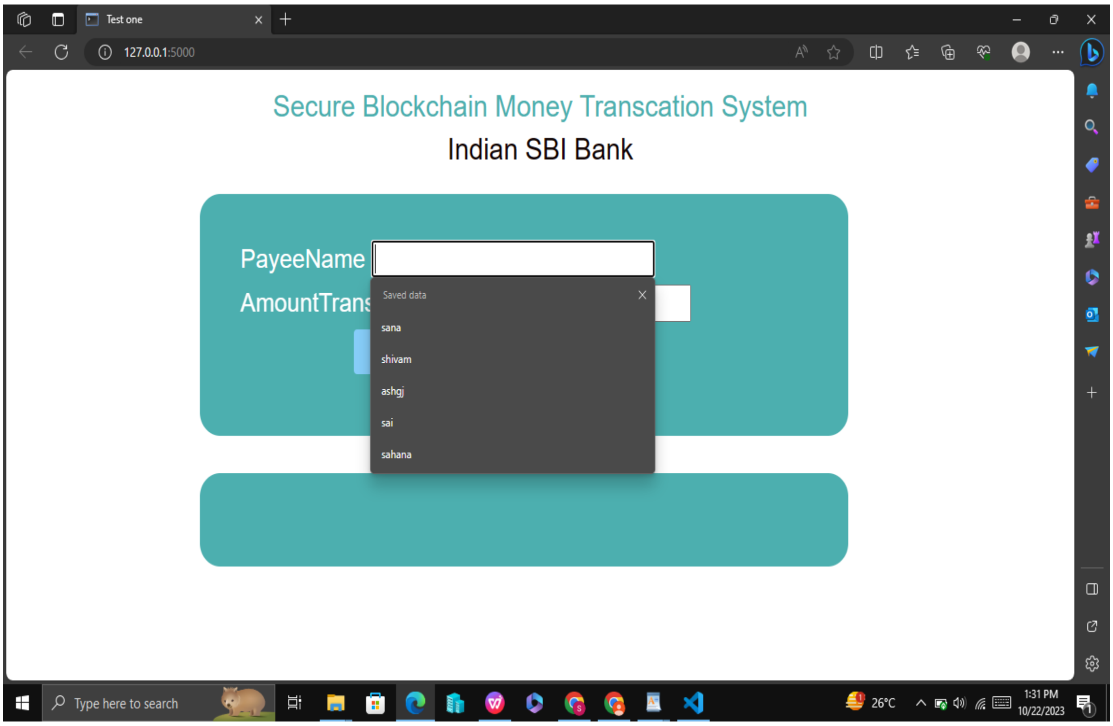
Conduct thorough testing to ensure the functionality and security of the blockchain-based system. Debug the code to identify and rectify any issues, paying close attention to the validity checks and the creation of blocks.

8. Security Measures:

Implement cryptographic techniques provided by the hashlib library to secure transactions and block contents.

Regularly update and review security protocols to adapt to emerging threats and vulnerabilities.

11. RESULTS AND DISCUSSIONS



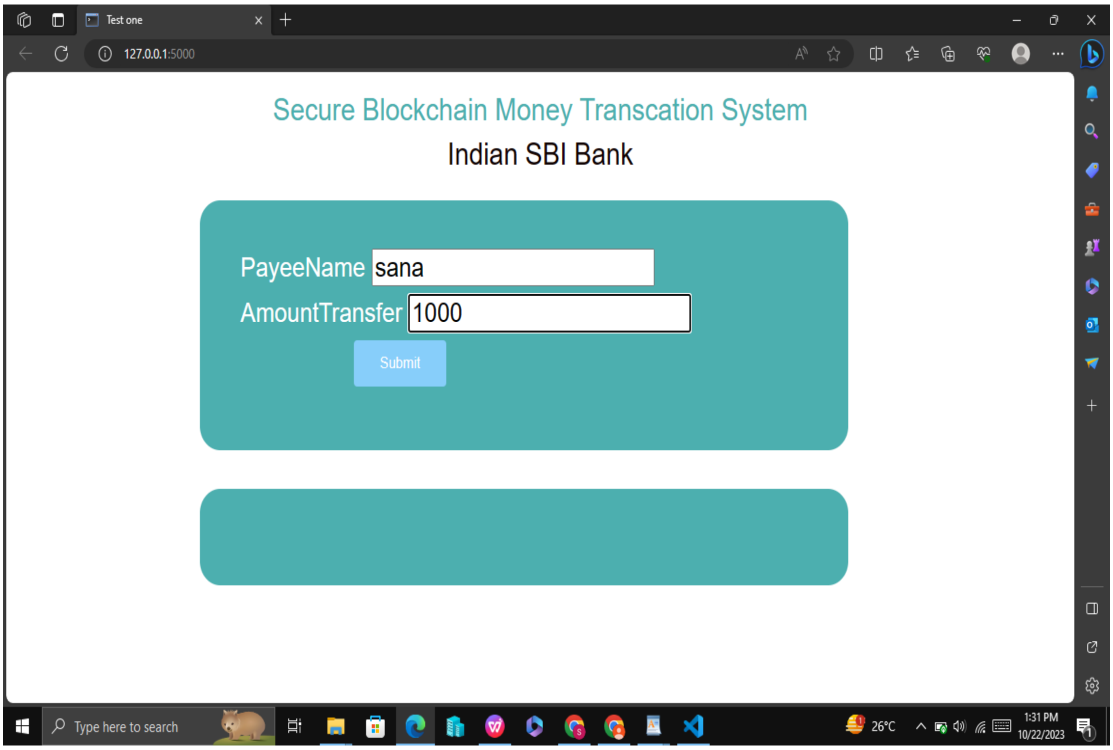
Secure Blockchain Money Transcation System

Indian SBI Bank

PayeeName

AmountTrans

Fig-4, Initial step to access the website



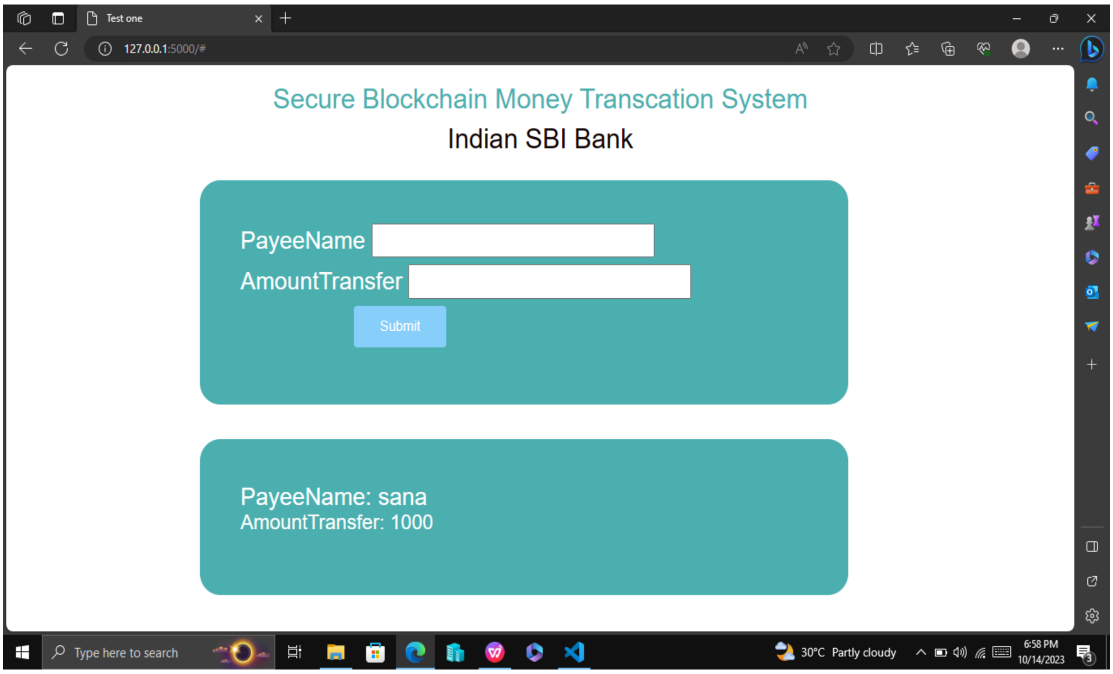
Secure Blockchain Money Transcation System

Indian SBI Bank

PayeeName sana

AmountTransfer 1000

Fig-5, Entering Name & Amount to transfer



Secure Blockchain Money Transcation System

Indian SBI Bank

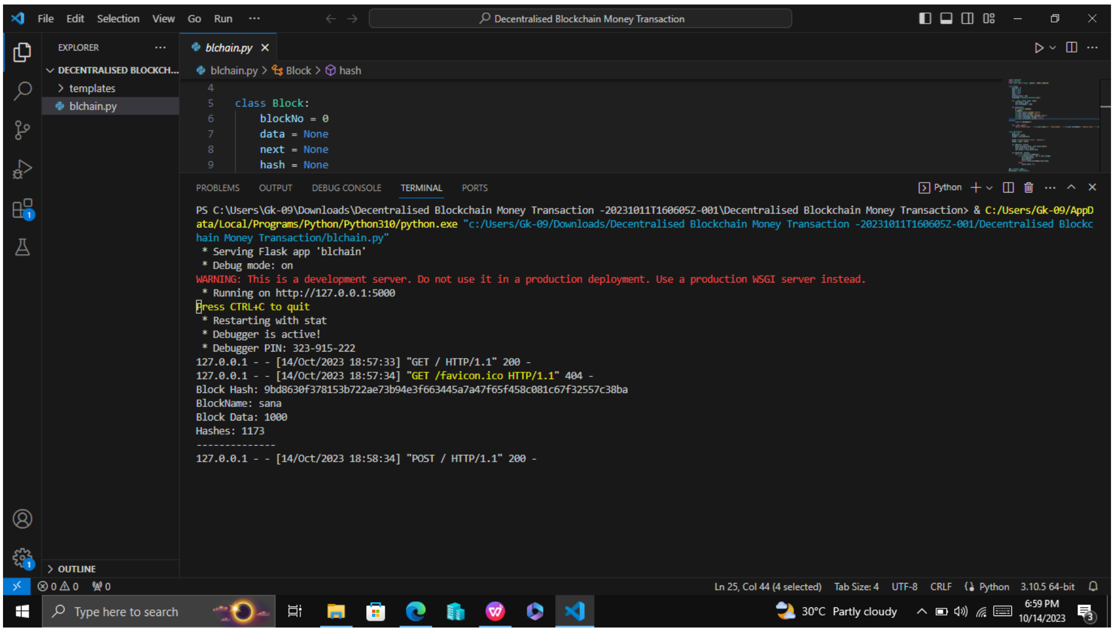
PayeeName

AmountTransfer

PayeeName: sana
AmountTransfer: 1000

Fig-6, Data stored at bottom

To initiate the banking website experience, users will access the platform and proceed with a link generated during the execution to input essential information, comprising their name and the desired amount to be transferred to the intended recipient. Following the data input, a submission action via a designated button will trigger the display of this entered information at the lower section of the webpage. Simultaneously, a backend system ensures the secure storage of this transaction data within a database. This user-friendly interface combines the functionalities of data input, immediate visibility, and secure data retention, offering a seamless and efficient online banking experience for individuals seeking to perform transactions. The process maintains a balance between user convenience and data integrity, ensuring a reliable and secure financial interaction platform.



```

class Block:
    blockNo = 0
    data = None
    next = None
    hash = None
```

```
PS C:\Users\Gk-09\Downloads\Decentralised Blockchain Money Transaction -20231011T160605Z-001\Decentralised Blockchain Money Transaction> & C:/Users/Gk-09/AppD
ata/Local/Programs/Python/Python310/python.exe "c:/Users/Gk-09/Downloads/Decentralised Blockchain Money Transaction -20231011T160605Z-001/Decentralised Blockc
hain Money Transaction/blchain.py"
 * Serving Flask app 'blchain'
 * Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 323-915-222
127.0.0.1 - - [14/Oct/2023 18:57:33] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [14/Oct/2023 18:57:34] "GET /favicon.ico HTTP/1.1" 404 -
Block Hash: 9bd8630f378153b722ae73b94e3f663445a7a47f65f458c081c67f32557c38ba
BlockName: sana
Block Data: 1000
Hashes: 1173
--------------
127.0.0.1 - - [14/Oct/2023 18:58:34] "POST / HTTP/1.1" 200 -
```

Fig-7, Storing of Block Data & Block Hash

In the backend system, each transaction triggers the creation of a unique block data, accompanied by its corresponding block hash. These blocks are specifically generated for individual transactions and are subsequently preserved within the database. This approach ensures a distinct and secure record for every financial interaction, enhancing the reliability and traceability of the entire transaction history. The combination of unique block data and hash values contributes to the robustness of the backend architecture, providing a solid foundation for transaction management and data integrity.

12. LEARNING OUTCOME

The completion of a project involving the creation of a blockchain system offers several important learning outcomes. Firstly, it provides a comprehensive understanding of blockchain technology, encompassing its foundational principles like distributed ledgers, consensus mechanisms, and cryptographic security. This project allows individuals to gain insights into the intricacies of blockchain systems, from designing state transition rules to generating and validating blocks, and ultimately, how these components come together to secure and manage transactions.

Moreover, the project emphasizes the significance of decentralization in blockchain networks, which bolsters security by removing single points of failure. Learners also become adept at ensuring data integrity, a critical aspect of blockchain technology that safeguards against tampering and fraudulent activities. They acquire the ability to recognize the broader applications of blockchain technology, extending beyond cryptocurrencies to domains such as supply chain management and healthcare.

In addition to this, participants in this project are encouraged to explore methods of developing resilient systems that can withstand attacks and external interference. It serves as a practical exercise in problem-solving and critical thinking, as they address various technical challenges along the way. The project fosters innovation by introducing novel approaches to transaction security and verification, reinforcing the importance of creativity in the field. Lastly, it familiarizes individuals with the intricacies of managing complex systems, highlighting aspects of systems engineering and architecture. For those who collaborated on this project as a team, it enhances teamwork, communication, and task delegation skills. Overall, creating a blockchain system is a valuable educational journey that equips individuals with the skills and insights necessary to understand, adapt, and innovate in the rapidly evolving realm of blockchain technology.

BLOCKCHAIN AND FUTURE OF TRANSACTIONS:

Blockchain innovation is groundbreaking, and is supposed to have a gigantic monetary effect like the one the Web has had in the beyond couple of many years.

Since blockchain innovation is at the core of Bitcoin and other virtual monetary forms, it can at any rate be normal to drive significantly more important vehicles of trade from now on. Be that as it may, virtual monetary standards are only the main use instance of blockchain innovation.

FOR LONG TERM:

Blockchain innovation is still in an early, developmental stage, and digital currencies are just its most memorable significant use case. Past digital currency, blockchain innovation will change how we execute, and how we record and confirm exchanges. This will upset agreements and decrease grating in the trading of resources. Over the course of the following couple of many years, blockchain innovation will permeate through our associations and establishments, and shape how we execute with each other. Similarly, as the Web keeps on controlling developing innovations, we can hope to see new use instances of blockchain innovation across all businesses.

13. CONCLUSION

The conclusion underscores the remarkable accomplishments in constructing a robust and secure blockchain system. The project has encompassed a wide array of critical elements, including the formulation of intricate state transition rules, the strategic creation of blocks, and the implementation of mechanisms to rigorously verify the legitimacy of transactions, individual blocks, and the entirety of the blockchain. This holistic approach represents a profound understanding and mastery of the intricate workings of blockchain technology, marking a significant milestone in the realm of distributed ledger systems.

The blockchain framework that has been engineered serves as the foundational core for enabling secure financial transactions. This framework has ushered in a transformative paradigm shift in the way we conduct and secure financial exchanges, emphasizing not just innovation but also an uncompromising commitment to security. The system's resilience to external threats and vulnerabilities is a testament to the robust security features integrated into its architecture. It relies on a combination of consensus mechanisms and cryptographic techniques to create a virtually impregnable fortress against unauthorized access and tampering, thus safeguarding the integrity and immutability of data.

One of the blockchain's standout attributes is its immutability, which ensures that once data is recorded on the ledger, it becomes exceedingly difficult to alter, enhancing trust and transparency. Furthermore, the system's decentralization aspect, which eradicates the need for a central authority, bolsters trust among participants. This feature effectively eliminates the single point of control, contributing to the blockchain's reputation as a secure and tamper-resistant platform. It not only challenges external attackers but also endorses the blockchain's potential to continually adapt and evolve in response to emerging threats and challenges. In essence, the project serves as a powerful testament to the pivotal role of blockchain technology in reshaping financial and data management systems, establishing a secure and transparent foundation for transactions in the digital age.

Future Scope:

- ❖ Enhanced Security: Blockchain uses cryptographic techniques to secure transactions, making it highly resistant to fraud and hacking. Transactions are immutable and transparent, reducing the risk of unauthorized changes.

- ❖ Reduced Costs: Blockchain eliminates intermediaries in financial transactions, such as banks and payment processors, leading to lower transaction fees. This can significantly reduce the cost of financial services.

- ❖ Faster Transactions: Traditional cross-border transactions can take days or even weeks to process. Blockchain-based transactions can occur within minutes, even for international transfers, improving efficiency.

- ❖ Improved Transparency: Blockchain's ledger is visible to all participants, creating transparency and trust. This transparency can help prevent fraudulent activities and reduce disputes.

- ❖ Financial Inclusion: Blockchain can provide access to financial services for unbanked and underbanked populations, enabling them to participate in the global economy.

- ❖ Data Privacy: Blockchain can offer improved data privacy through encryption and decentralized data storage solutions.

- ❖ Reduced Fraud: The transparency and immutability of blockchain can significantly reduce the risk of fraudulent activities.

- ❖ Microtransactions: Blockchain allows for cost-effective microtransactions, opening up new possibilities for monetization and revenue generation.

- ❖ Reduced Counterparty Risk: Blockchain reduces counterparty risk by ensuring that all parties fulfill their obligations before a transaction is finalized. This can be especially valuable in complex financial transactions.

- Immutable Records: Once data is recorded on the blockchain, it cannot be altered or deleted. This feature ensures data integrity and can be valuable for record-keeping and auditing.

- Increased Trust: Blockchain's security features and transparency build trust among participants in the ecosystem. This trust can lead to increased collaboration and investment.

- Blockchain innovation is groundbreaking, and is supposed to have a gigantic monetary effect like the one the Web has had in the beyond couple of many years.

- Since blockchain innovation is at the core of Bitcoin and other virtual monetary forms, it can at any rate be normal to drive significantly more important vehicles of trade from now on. Be that as it may, virtual monetary standards are only the main use instance of blockchain innovation.

14. REFERENCES

[1] Nakamoto, S. (2008) Bitcoin: A peer-to-peer electronic cash system. Consulted., 165: 55-61.

[2] Zhu, Y., Gan, G.H., Deng, D. (2016) Security Research in Key Technologies of Blockchain.

Information Security Research., 12: 1090-1097.

[3] Liu, X.F. (2017) Research on blockchain performance improvement of Byzantine fault-tolerant

consensus algorithm based on dynamic authorization. Zhejiang University.

[4] Wang, X., Lai, X., Feng, D. (2005) Cryptanalysis of the Hash Functions MD4 and RIPEMD. Advances in Eurocrypt., 3494: 1-18.

[5] Wang, H.Q., Wu, T. (2017) Cryptography in Blockchain. Journal of Nanjing University of Posts and Telecommunications., 37: 61-67.

[6] Yuan, Y., Wang, F. (2016) Current Status and Prospects of Blockchain Technology

Development. Acta Automatica Sinica., 42: 481-494.

[7] Miyaji, A. (1994) Elliptic Curves Suitable for Cryptosystems. Ieice Transactions on Fundamentals of Electronics Communications & Computer Sciences., 77: 98-105.

[8] He, P., Yu, G., Zhang, Y.F. (2017) Prospective review of blockchain technology and application. Computer Science., 44: 1-7.

[9] Zhai, S.P., Li, Z.Z. (2018) The data block chain of the key technologies Consistency. Computer Technology and Development., 8: 1-6.

[10] An, Q.W. (2017) Research and application of key technologies for decentralized transactions based on blockchain. Donghua University.