

## ENHANCING MONEY TRANSACTION SECURITY THROUGH BLOCKCHAIN TECHNOLOGY AND CRYPTOGRAPHY

Ms. P. Yamuna<sup>1</sup>, Pakala Manisha<sup>2</sup>, Rohith Gundeboina<sup>3</sup>,  
Boji Vaishali<sup>4</sup>, Mohammed Inkeshaf<sup>5</sup>

<sup>1</sup>Assistant. Professor, CSE Dept, ACE Engineering College, Hyderabad, India.

<sup>2,3,4,5</sup>Student, CSE Dept, ACE Engineering College, Hyderabad, India.

DOI: <https://www.doi.org/10.58257/IJPREMS34088>

### ABSTRACT

In the realm of financial transactions, security is paramount, and blockchain technology coupled with cryptography emerges as a transformative force. Blockchain, a decentralized ledger, ensures resilience against single points of failure by distributing transaction data across a network. Cryptographic hash functions link each block securely, creating an immutable transaction history resistant to tampering. Consensus mechanisms, like Proof of Work or Proof of Stake, add layers of security by requiring agreement among participants, thwarting potential malicious activities.

Cryptography plays a pivotal role in securing transactions within the blockchain. Digital signatures, enabled by public-key cryptography, authenticate and preserve the integrity of transactions. Smart contracts, self-executing code, automate and enforce transaction terms, reducing reliance on intermediaries and enhancing operational efficiency. Privacy-enhancing cryptography, such as zero-knowledge proofs, protects sensitive information by masking transaction details while still providing verifiable proof of validity. Blockchain's influence extends to decentralized identity management, offering a tamper-resistant solution that reduces the risk of identity theft and ensures only authorized users engage in financial transactions. Cross-border transactions benefit from blockchain's transparency, eliminating the need for traditional intermediaries and enhancing security. However, challenges like scalability and evolving regulatory landscapes persist. Ongoing innovation is required to address emerging threats and vulnerabilities. As blockchain technology and cryptography evolve, the financial landscape stands poised for increased efficiency, transparency, and security in money transactions. This synergy not only addresses current security concerns but also lays the foundation for a dynamic and secure future in financial ecosystems.

### 1. INTRODUCTION

Blockchain is a distributed database with decentralised, traceable, non-tamperable, secure and reliable features. It integrates P2P (Peer-to-Peer) protocol, digital encryption technology, consensus mechanism, smart contract and other technologies together. Abandoning the maintenance mode of the traditional central node and adopting the method of mutual maintenance by multiple users to realise the information supervision among multiple parties, thereby ensuring the credibility and integrity of the data. The blockchain platform can be divided into public chain, private chain and alliance chain. All nodes in the public chain can join or withdraw freely; the private chain strictly limits the qualification of participating nodes; the alliance chain is jointly managed by several participating institutions. Bitcoin was proposed by Nakamoto in 2008, which is the most successful case of digital currency, and is also the most typical application of blockchain. In addition, the blockchain has expanded its unique application value in many aspects and has shown its potential to reshape society. 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. It can be seen that cryptography technology occupies the most central position in the blockchain. In blockchain, cryptography technology is mainly used to protect user privacy and transaction information, and ensure data consistency, etc.[2] 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.

#### Blockchain infrastructure

According to Melanie Swan, founder of the Blockchain Science Institute, blockchain technology has experienced two phases, the first one is the blockchain 1.0 phase of multi-technology portfolio innovation represented by Bitcoin, the second one is the blockchain 2.0 phase represented by Ethereum, which is transferred by digital assets. Typical

applications of blockchain technology mainly include Bitcoin, Ethereum, Hyper Ledgers, etc. Although the implementations are different, there are many commonalities in the overall architecture. As shown in Table 1, the blockchain platform can be divided into five levels: network layer, consensus layer, data layer, contract layer and application layer.

The data layer mainly uses the block data structure to ensure the integrity of data storage. Each node in the network encapsulates the data transactions received over a period of time into a time-stamped data block and links the block to the current longest main blockchain for storage. This layer involves the main techniques of block storage, chain structure, hash algorithm, Merkle tree, time stamp and so on.

The consensus layer mainly includes a consensus mechanism, which enables each node to reach a consensus on the validity of block data in the decentralized system. The consensus mechanism mainly has PoW, PoS, PBFT and SBFT. The smart contract that is mainly included in the contract layer is the basis of the blockchain programmable feature. The computerized program that can automatically execute the contract terms is stored in the blockchain in the form of code and data sets. Smart contracts, driven by time or events, are executed by blockchain nodes in a distributed manner. All relevant terms are coded, automatically settled, and triggered by signatures or other external data messages. The network layer includes various data transmission protocols and verification mechanisms. The blockchain is a typical P2P network. All nodes are connected through a planar topology and have no central nodes. Any two nodes can be freely traded, and any node can join or leave the network at any time. The P2P protocol in the blockchain is mainly used for information transmission between nodes. The application layer mainly includes Bitcoin, Ethereum and Hyperledger and so on. Bitcoin is mainly for digital currency transactions. Ethereum adds decentralized applications based on digital currency. Hyperledger does not support digital currency transactions, mainly enterprise-level blockchain applications.

## 2.1 Hash and block structure

The hash algorithm is a function that maps a sequence of messages of any length to a shorter fixed-length value, and is characterized by susceptibility, unidirectionality, collision resistance, and high sensitivity. Hash is usually used to ensure data integrity, that is, to verify the data has been illegally tampered with. When the data tested changes, its hash value also changes correspondingly. Therefore, even if the data is in an unsafe environment, the integrity of the data can be detected based on the hash value of the data.

SHA is a type of cryptographic hash function issued by the National Institute of Standards and Technology (NIST) with the general characteristics of a cryptographic hash function. The SHA256 algorithm is a class of the SHA-2 algorithm cluster, which generates a 256-bit message digest. The algorithm's calculation process includes two stages: message preprocessing and main loop. In the message preprocessing stage, binary bit filling and message length filling are performed on the information of any length, and the filled message is divided into several 512-bit message blocks. In the main loop phase, each message block is processed by a compression function. The input of the current compression function is the output of the previous compression function, and the output of the last compression function is the hash value of the original message.

RIPEMD, a summary of the RACE original integrity check message, is a hash function algorithm developed by the COSI research team of the University in Leuven, Belgium. RIPEMD-160 is the most common version of RIPEMD[5]. As the SHA series functions, the first step of the algorithm is message complement, and the complement method is identical to the SHA series algorithm. The core of the processing algorithm is the compression function, which is a loop, where each loop consists of 16 step functions. Using different original logic functions in each loop, the processing of the algorithm is divided into two different cases, with five of the two original logic functions running in reverse order. After all 512-bit packet processing is completed, the resulting 160-bit output is the hash value of the original message.

For blockchain, hash functions can be used to perform block and transaction integrity verification. In the blockchain, the hash value of the information of the previous block is stored in the header of each block, and any user can compare the calculated hash value with the stored hash value. In turn, the integrity of the information of the previous block is detected. Similarly, the hash function can be used to generate public-private key pairs.

The hash pointer is a data structure that contains, in addition to the usual pointers, some data information and password hashes associated with the information. A normal pointer is used to retrieve information, and a hash pointer is used to verify that the information has been tampered. The blockchain is a list of hash pointers, each of which is connected by using a hash value. It is verified according to the hash value whether the data contained in the block is changed, thereby ensuring the integrity of the block information.

## 2. PROBLEM STATEMENT

In the rapidly evolving landscape of global finance, traditional financial systems face persistent challenges that threaten the security, efficiency, and transparency of money transactions. Centralized architectures, characterized by single points of failure and susceptibility to unauthorized access, are increasingly vulnerable in the digital age. These vulnerabilities include the risk of data tampering, identity theft, and inefficiencies associated with reliance on multiple intermediaries, especially in cross-border transactions. Recognizing these challenges, the financial industry is at a critical juncture, necessitating a transformative solution that leverages emerging technologies to fortify transaction security and reshape the dynamics of financial interactions. The primary issue at hand is the fragility of centralized financial systems. The reliance on a centralized authority introduces vulnerabilities that can be exploited by malicious actors. Traditional databases are susceptible to tampering, creating opportunities for fraudulent activities that undermine the integrity of financial transactions. Additionally, the centralized storage of sensitive user information makes these systems attractive targets for cyberattacks, leading to potential breaches and compromise of personal data. Cross-border transactions, a cornerstone of global commerce, face inefficiencies stemming from the involvement of multiple intermediaries. The current infrastructure often results in delays, increased costs, and a lack of transparency. Regulatory compliance further complicates these transactions, as financial systems struggle to reconcile decentralized technologies with evolving legal frameworks. These inefficiencies hinder the seamless flow of funds across borders, negatively impacting businesses and individuals engaged in international transactions. Furthermore, the existing financial ecosystem lacks a comprehensive and user-centric identity management solution. Instances of identity theft and unauthorized access to personal information continue to rise, eroding user trust in digital financial platforms. Conventional identity verification methods, centralized and prone to vulnerabilities, fail to provide robust protection against unauthorized alterations to personal data.

## 3. LITERATURE SURVEY

A literature survey is a systematic review and summary of existing scholarly literature on a particular topic or research question. It involves identifying, analyzing, and synthesizing relevant academic papers, books, articles, and other sources to provide an overview of the current state of knowledge in the field. In the context of enhancing money transaction security through blockchain technology and cryptography, a literature survey would involve searching for and reviewing existing research studies, papers, and publications that discuss various aspects of this topic. This includes examining the theoretical foundations, technological advancements, practical implementations, challenges, and future directions related to using blockchain and cryptography for securing financial transactions. By conducting a literature survey, researchers can gain insights into the key findings, methodologies, gaps in knowledge, and emerging trends in the field. This helps in identifying areas for further investigation, informing the design of new research studies, and contributing to the advancement of knowledge in the domain of money transaction security . [1]Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from: <https://bitcoin.org/bitcoin.pdf> [2]Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world. Penguin. [3]Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375. [4]Swan, M. (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.". [5]Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley. [6]Ali, M., Nelson, J. D., Shea, R., & Freedman, M. J. (2019). Blockmania: from cryptocurrencies to consensus networks– the societal value of decentralized systems. arXiv preprint arXiv:1907.00013. [7]Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—A systematic review. PloS one, 11(10), e0163477. [8]Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292-2303. [9]Cocco, L., & Marchesi, M. (2016). Modeling and simulation of the economics of mining in the bitcoin market. PloS one, 11(10), e0164603. [10]Zohar, A. (2015). Bitcoin: Under the hood. Communications of the ACM, 58(9), 104-113. These references cover a range of topics including the foundational concepts of blockchain, cryptocurrencies, smart contracts, economics of mining, and the societal impacts of decentralized systems. They provide valuable insights into the current state of research and practical applications in the field of blockchain and cryptography for enhancing money transaction security

## 4. TYPES OF BLOCKCHAIN

1. **Public blockchain:** A blockchain that anyone in the world can read, can send transactions to and expect to see them included if they are valid. This means anyone can become part of the network and participate in the consensus process making them permissionless. There is no way to censor transactions on the network nor change

transactions retrospectively. The content of the blockchain can be trusted to be correct. Public blockchains are, however, very inefficient. The more computing power is required to support trust. So, an attacker would need to acquire 51% of the network's computing power to change an entry in the blockchain. (e.g., Bitcoin, Ethereum, ZCash).

2. **Consortium blockchain:** It is a blockchain where a pre-selected set of nodes control the consensus process.
3. **Private blockchain:** A blockchain where access permissions are more lightly controlled, where rights to modify or even read the blockchain state are restricted to a few users, where only known nodes are allowed to participate in the network. Ideally, it is internal for an organization. The writes permissions are kept centralized to one organization. Private blockchain reduces counterparty risk by enabling the exchange of data without the intermediation of third parties.
4. **Permissioned Blockchain:** It is a blockchain where we can allow specific actions to be performed only by specific addresses. The participants in the network can restrict who can participate in the consensus mechanism and who can create a smart contract and give the authority for some participants to provide the validation of blocks of transactions. A control access layer into the blockchain nodes is used. However, raise their questions, Who has the authority to grant permission? A permission blockchain may make its owners feel more secure, giving the database rigorous security and privacy capabilities but can be seen as violating the idea of blockchain because only some participants have more control, which means they can make changes whether or not other network participants agree.

## 5. DIGITAL CONTENT PROTECTION

In order to preserve the privacy for traceable encryption in blockchain, Wu et al. proposed a system in which authenticity and non-repudiation of digital content is guaranteed. The problem tackled by authors is the secret key of the user, which when shared with other entities does not hold the specific information of the user. In case the shared key is corrupted or abused, it makes it difficult to analyze the source of the secret key. Moreover, leakage of confidential information in access control is a bottleneck for existing systems. Therefore, authors have integrated the privacy protection algorithm such as attribute based encryption (ABE) to secure the secret keys. However, the decryption mechanism does not show improved efficiency.

Management of digital data rights is a fundamental requirement to achieve protection of digital data. Existing techniques for data rights lack transparency, decentralization, and trust. In response to above mentioned problems, Zhang and Zhao proposed blockchain-based decentralized solutions. Information regarding the use of digital content, such as transaction and license information is transparent to everyone. Smart contract is designed for the automatic assignment of license. In this mechanism, the owner can set the prices for selling the license to other customers. However, peers of the network have to possess high computational power to perform key acquisition.

### 5.1 The Significance of Security for Blockchain

Before we dive right into understanding the role of cryptography in blockchain, let us reflect briefly on the blockchain itself. It basically refers to a distributed database that offers the features of decentralization, security, traceability, reliability, and immutability. Blockchain takes away the need for traditional approaches for maintaining central nodes and introduces the new approach for mutual maintenance of nodes by multiple users.

As a result, it can entrust information supervision to multiple parties and ensure desired levels of credibility and data integrity. Another important aspect pertaining to blockchain refers to the three distinct types of blockchain platforms. The types of blockchain platforms include public chain, private chain, and alliance chain. All the nodes in a public chain could easily participate or withdraw from the blockchain according to their preferences.

## 6. OBJECTIVE OF THE PROJECT

### Security Enhancement:

Implement robust cryptographic measures and blockchain technology to fortify transaction security, preventing unauthorized access, tampering, and identity theft.

### Transparency and Immutability:

Utilize blockchain's decentralized ledger to ensure transparency and immutability in financial transactions, providing a tamper-resistant record of all activities.

### Efficient Cross-Border Transactions:

Streamline cross-border transactions by leveraging blockchain's decentralized nature, eliminating the need for multiple intermediaries, and reducing delays and associated costs.



---

**Decentralized Identity Management:**

Develop a secure decentralized identity management system using blockchain to protect user identities and sensitive information, minimizing the risk of identity theft.

**Privacy Preservation:**

Implement advanced cryptographic techniques, such as zero-knowledge proofs, to protect user privacy while maintaining verifiable transaction validity.

**Regulatory Compliance:**

Ensure compliance with evolving regulatory frameworks, incorporating features that facilitate adherence to financial regulations without compromising the privacy and security of users.

**Scalability and Future-Proofing:**

Address scalability concerns associated with blockchain technology, ensuring the system's adaptability to future technological advancements and emerging threats.

**User Education and Adoption:**

Develop educational resources and initiatives to enhance user understanding of the new system, fostering widespread adoption and trust in the secure financial ecosystem.

**6.1 Distributed ledger**

A distributed ledger is a directory or database that's stored across various computers (aka nodes). All nodes possess an exact copy of the ledger. When new information is added, the nodes conduct an automatic vote to verify the authenticity of the update.

When the majority of nodes agree (aka gain consensus), the system updates itself accordingly (ie. adopting the new information into all copies of the ledger, or rejecting it). Distributed ledgers run without a central authority, revolutionizing the way we think of democracy.

**Making blockchain mainstream**

Confidence in this technology, especially for digital currencies, is growing across the board. Governments are accelerating their work on Central Bank Digital Currencies. Businesses are building and investing, with the vast majority of global executives surveyed by Deloitte last year saying they believe digital assets will be important to their industries within the next three years.

But the benefits of innovation, especially in the financial sector, cannot be gained at the expense of additional risk to consumers. Central banks and regulators, entrusted with the duty to protect consumers, draft and enforce regulations guided by that lofty responsibility. But, as the Tempo-Cowrie example demonstrates, deployed correctly, blockchain technology can be leveraged to benefit consumers without sacrificing oversight, accountability or regulation.

**7. CRYPTOCURRENCIES****7.1 The Beginning of Blockchain's Technological Rise**

Blockchain's most well-known use (and maybe most controversial) is in cryptocurrencies. Cryptocurrencies are digital currencies (or tokens), like Bitcoin, Ethereum or Litecoin, that can be used to buy goods and services. Just like a digital form of cash, crypto can be used to buy everything from your lunch to your next home. Unlike cash, crypto uses blockchain to act as both a public ledger and an enhanced cryptographic security system, so online transactions are always recorded and secured.

**7.2 HOW DOES CRYPTOCURRENCY WORK?**

Cryptocurrencies are digital currencies that use blockchain technology to record and secure every transaction. A cryptocurrency (for example, Bitcoin) can be used as a digital form of cash to pay for everything from everyday items to larger purchases like cars and homes. It can be bought using one of several digital wallets or trading platforms, then digitally transferred upon purchase of an item, with the blockchain recording the transaction and the new owner. The appeal of cryptocurrencies is that everything is recorded in a public ledger and secured using cryptography, making an irrefutable, timestamped and secure record of every payment.

To date, there are roughly 6,700 cryptocurrencies in the world that have a total market cap around \$1.6 trillion, with Bitcoin holding a majority of the value. These tokens have become incredibly popular over the last few years, with one Bitcoin equaling \$60,000. Here are some of the main reasons why everyone is suddenly taking notice of cryptocurrencies:

- Blockchain's security makes theft much harder since each cryptocurrency has its own irrefutable identifiable number that is attached to one owner.
- Crypto reduces the need for individualized currencies and central banks- With blockchain, crypto can be sent to anywhere and anyone in the world without the need for currency exchanging or without interference from central banks.
- Cryptocurrencies can make some people rich- Speculators have been driving up the price of crypto, especially Bitcoin, helping some early adopters to become billionaires. Whether this is actually a positive has yet to be seen, as some detractors believe that speculators do not have the long-term benefits of crypto in mind.
- More and more large corporations are coming around to the idea of a blockchain-based digital currency for payments. In February 2021, Tesla famously announced that it would invest \$1.5 billion into Bitcoin and accept it as payment for their cars.

Of course, there are many legitimate arguments against blockchain-based digital currencies. First, crypto isn't a very regulated market. Many governments were quick to jump into crypto, but few have a staunch set of codified laws regarding it. Additionally, crypto is incredibly volatile due to those aforementioned speculators. In 2016, Bitcoin was priced around \$450 per token. It then jumped to about \$16,000 a token in 2018, dipped to around \$3,100, then has since increased to more than \$60,000. Lack of stability has caused some people to get very rich, while a majority have still lost thousands.

Whether or not digital currencies are the future remains to be seen. For now, it seems as if blockchain's meteoric rise is more starting to take root in reality than pure hype. Though it's still making headway in this entirely-new, highly-exploratory field, blockchain is also showing promise beyond Bitcoin.



**Figure 1: CRYPTOCURRENCY**

### 7.3 Beyond Bitcoin: Ethereum Blockchain

Originally created as the ultra-transparent ledger system for Bitcoin to operate on, blockchain has long been associated with cryptocurrency, but the technology's transparency and security has seen growing adoption in a number of areas, much of which can be traced back to the development of the Ethereum blockchain.

In late 2013, Russian-Canadian developer Vitalik Buterin published a white paper that proposed a platform combining traditional blockchain functionality with one key difference: the execution of computer code. Thus, the Ethereum Project was born.

Ethereum blockchain lets developers create sophisticated programs that can communicate with one another on the blockchain.

### 7.4 Tokens

Ethereum programmers can create tokens to represent any kind of digital asset, track its ownership and execute its functionality according to a set of programming instructions.

Tokens can be music files, contracts, concert tickets or even a patient's medical records. Most recently, Non-Fungible Tokens (NFTs) have become all the rage. NFTs are unique blockchain-based tokens that store digital media (like a video, music or art). Each NFT has the ability to verify authenticity, past history and sole ownership of the piece of digital media. NFTs have become wildly popular because they offer a new wave of digital creators the ability to buy and sell their creations, while getting proper credit and a fair share of profits.

Newfound uses for blockchain have broadened the potential of the ledger technology to permeate other sectors like media, government and identity security. Thousands of companies are currently researching and developing products

and ecosystems that run entirely on the burgeoning technology.

Blockchain is challenging the current status quo of innovation by letting companies experiment with groundbreaking technology like peer-to-peer energy distribution or decentralized forms for news media. Much like the definition of blockchain, the uses for the ledger system will only evolve as technology evolves.

### How Does Blockchain Work?

The name blockchain is hardly accidental: The digital ledger is often described as a “chain” that’s made up of individual “blocks” of data. As fresh data is periodically added to the network, a new “block” is created and attached to the “chain.” This involves all nodes updating their version of the blockchain ledger to be identical.

How these new blocks are created is key to why blockchain is considered highly secure. A majority of nodes must verify and confirm the legitimacy of the new data before a new block can be added to the ledger. For a cryptocurrency, they might involve ensuring that new transactions in a block were not fraudulent, or that coins had not been spent more than once. This is different from a standalone database or spreadsheet, where one person can make changes without oversight.

“Once there is consensus, the block is added to the chain and the underlying transactions are recorded in the distributed ledger,” says C. Neil Gray, partner in the fintech practice areas at Duane Morris LLP. “Blocks are securely linked together, forming a secure digital chain from the beginning of the ledger to the present.”

Transactions are typically secured using cryptography, meaning the nodes need to solve complex mathematical equations to process a transaction.

“As a reward for their efforts in validating changes to the shared data, nodes are typically rewarded with new amounts of the blockchain’s native currency—e.g., new bitcoin on the bitcoin blockchain,” says Sarah Shtylman, fintech and blockchain counsel with Perkins Coie.

### 9.1.Public Blockchains vs Private Blockchains

There are both public and private blockchains. In a public blockchain, anyone can participate meaning they can read, write or audit the data on the blockchain. Notably, it is very difficult to alter transactions logged in a public blockchain as no single authority controls the nodes.

A private blockchain, meanwhile, is controlled by an organisation or group. Only it can decide who is invited to the system plus it has the authority to go back and alter the blockchain. This private blockchain process is more similar to an in-house data storage system except spread over multiple nodes to increase security.

### How Is Blockchain Used?

Blockchain technology is used for many different purposes, from providing financial services to administering voting systems.

### Cryptocurrency

The most common use of blockchain today is as the backbone of cryptocurrencies, like Bitcoin or Ethereum. When people buy, exchange or spend cryptocurrency, the transactions are recorded on a blockchain. The more people use cryptocurrency, the more widespread blockchain could become.

“Because cryptocurrencies are volatile, they are not yet used much to purchase goods and services. But that is changing as PayPal, Square and other money service businesses make digital asset services broadly available to vendors and retail customers,” notes Patrick Daugherty, senior partner of Foley & Lardner and lead of the firm’s blockchain task force.

## 8. ADVANTAGES OF BLOCKCHAIN

### Higher Accuracy of Transactions

Because a blockchain transaction must be verified by multiple nodes, this can reduce error. If one node has a mistake in the database, the others would see it’s different and catch the error. In contrast, in a traditional database, if someone makes a mistake, it may be more likely to go through. In addition, every asset is individually identified and tracked on the blockchain ledger, so there is no chance of double spending it (like a person overdrawing their bank account, thereby spending money twice).

### No Need for Intermediaries

Using blockchain, two parties in a transaction can confirm and complete something without working through a third party. This saves time as well as the cost of paying for an intermediary like a bank. “It has the ability to bring greater efficiency to all digital commerce, to increase financial empowerment to the unbanked or underbanked populations of the world and to power a new generation of internet applications as a result,” says Shtylman.

### Extra Security

Theoretically, a decentralised network, like blockchain, makes it nearly impossible for someone to make fraudulent transactions. To enter in forged transactions, they would need to hack every node and change every ledger. While this isn't necessarily impossible, many cryptocurrency blockchain systems use proof-of-stake or proof-of-work transaction verification methods that make it difficult, as well as not in participants' best interests, to add fraudulent transactions.

### More Efficient Transfers

Since blockchains operate 24/7, people can make more efficient financial and asset transfers, especially internationally. They don't need to wait days for a bank or a government agency to manually confirm everything.

## 9. DISADVANTAGES OF BLOCKCHAIN

### Limit on Transactions per Second

Given that blockchain depends on a larger network to approve transactions, there's a limit to how quickly it can move. For example, Bitcoin can only process 4.6 transactions per second versus 1,700 per second with Visa. In addition, increasing numbers of transactions can create network speed issues. Until this improves, scalability is a challenge.

### High Energy Costs

Having all the nodes working to verify transactions takes significantly more electricity than a single database or spreadsheet. Not only does this make blockchain-based transactions more expensive, but it also creates a large carbon burden on the environment. Because of this, some industry leaders are beginning to move away from certain blockchain technologies, like Bitcoin: For instance, Elon Musk recently said Tesla would stop accepting Bitcoin partly because he was concerned about the damage to the environment.

### Risk of Asset Loss

Some digital assets are secured using a cryptographic key, like cryptocurrency in a blockchain wallet. You need to carefully guard this key. "If the owner of a digital asset loses the private cryptographic key that gives them access to their asset, currently there is no way to recover it—the asset is gone permanently," says Gray. Because the system is decentralized, you can't call a central authority, like your bank, to ask to regain access.

### Potential for Illegal Activity

Blockchain's decentralization adds more privacy and confidentiality, which unfortunately makes it appealing to criminals. It's harder to track illicit transactions on blockchain than through bank transactions that are tied to a name.

### How to Invest in Blockchain

You can't actually invest in blockchain itself, since it's merely a system for storing and processing transactions. However, you can invest in assets and companies using this technology. "The easiest way is to purchase cryptocurrencies, like Bitcoin, Ethereum and other tokens that run on a blockchain," says Gray. Another option is to invest in blockchain companies using this technology. For example, Santander Bank is experimenting with blockchain-based financial products, and if you were interested in gaining exposure to blockchain technology in your portfolio, you might buy its stock.

For a more diversified approach, you could buy into an exchange-traded fund (ETF) that invests in blockchain assets and companies, like the Amplify Transformational Data Sharing ETF (BLOK), which puts at least 80% of its assets in blockchain companies.

### The Blockchain and the Future of Transactions

Blockchain technology is transformative, and is expected to have a massive economic impact similar to the one the Internet has had in the past few decades. Since blockchain technology is at the heart of Bitcoin and other virtual currencies, it can at the very least be expected to power even more consequential mediums of exchange in the future. However, virtual currencies are merely the first use case of blockchain technology.

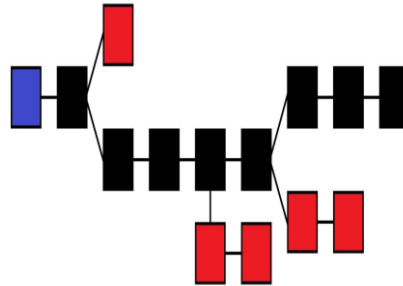
### Blockchain Fundamentals

The blockchain is an open and distributed ledger. It uses an append-only data structure, meaning new transactions and data can be added on to a blockchain, but past data cannot be erased. This results in a verifiable and permanent record of data and transactions between two or more parties. This has the potential to increase transparency and accountability, and positively enhance our social and economic systems.

A blockchain is built by running software and linking several nodes together. A blockchain is not one global entity — there are several blockchains. Imagine a network of connected computers inside a highly secure office, which are connected to each other, but not to the internet. A blockchain is similar to this: it can have numerous connected nodes, but remain totally separate and unique from other blockchains. Institutions and banks can build internal blockchains



with their own features for various organisational purposes. A consensus mechanism and a reward system are required to maintain the integrity and functionality of a blockchain. In the Bitcoin blockchain, consensus is achieved by 'mining', and the reward system is a protocol awarding a miner some amount of Bitcoin upon successfully mining a block. Mining is undertaken by powerful computers solving complex mathematical puzzles. Once a transaction verified, and accepted as true by the entire network, miners start working on the next block. Thus, a blockchain keeps growing (linking each new block to the one before it).



**Figure 2:**Blockchain Fundamentals

The main chain (black) consists of the longest series of blocks from the genesis block (blue) to the current block. Orphan blocks (red) exist outside of the main chain.

### Implications for Transactions

**Blockchain technology will disrupt the way we write and enforce contracts, execute transactions and maintain records.**

Keeping records of transactions is a core function of all businesses. These records are meant to track past performance and help with forecasting and planning for the future. Most organizations' records take a lot of time and effort to create, and often the creation and storage processes are prone to errors. Currently, transactions can be executed immediately, but settlement can take anywhere from several hours to several days. For example, someone selling stock in a corporation on a stock exchange can sell immediately, but settlement can take a few days. Similarly, a deal to purchase a house or car can be negotiated and signed quickly, but the registration process (verifying and registering the change in property ownership) often takes days and may involve lawyers and government employees. In each of these examples, each party maintains its own ledger, and cannot access the ledgers of the other parties involved.

On the blockchain, the process of transaction verification and recording is immediate and permanent. The ledger is distributed across several nodes, meaning the data is replicated and stored instantaneously on each node across the system. When a transaction is recorded in the blockchain, details of the transaction such as price, asset, and ownership, are recorded, verified and settled within seconds across all nodes. A verified change registered on any one ledger is also simultaneously registered on all other copies of the ledger.

### From Virtual Currencies to Enterprise Use

The blockchain underlying Bitcoin is currently the largest and best known blockchain. Ethereum is a separate blockchain: while it supports the Ether currency, it also acts as a distributed computing platform that features smart contract functionality. Therefore, despite having a virtual currency element, it has many more uses than Bitcoin. For example, companies in various industries raising funds through ICOs use Ethereum for their projects. The Hyperledger Project, by the Linux Foundation, aims to bring together a number of independent efforts to develop open protocols and standards in blockchain technology for enterprise use. Hyperledger is a project with several open source blockchains and related tools to support the collaborative development of blockchain — based distributed ledgers.

## 10. REQUIREMENTS

### Software Requirements:

Python IDE(Online/Offline)

We will Mainly use Google Collab for better performance, easy execution and platform Independent.

### Hardware Requirements:

Any Hardware as Mobile, Ipad, Laptop or Desktop will work

### Programming:

Project will be in Python Programming.

### Process/Implementation :

1. We will Write code on Google Collab
2. Will use libraries like import hashlib,json,sys
3. Create a function to generate exchanges between friends.
4. 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
5. Now we will construct blocks

## 11. ARCHITECTURE OF THE PROJECT

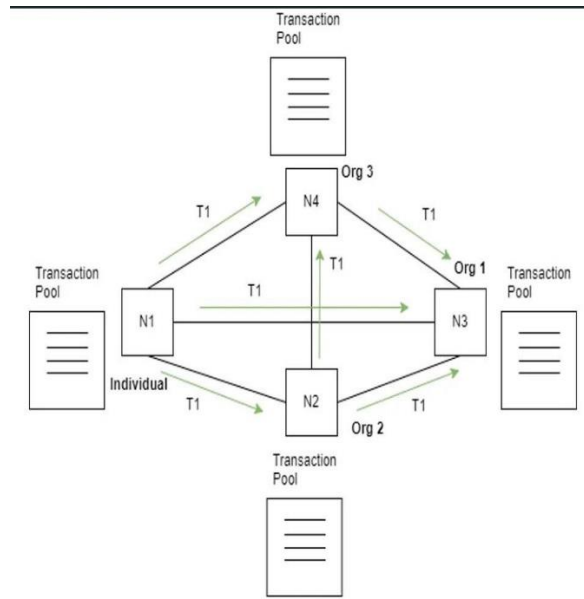


Figure 3:Architecture

## 12. SYSTEM DESIGN

### 12.1 UML DIAGRAMS

#### CLASS DIAGRAM



Figure 5:Class Diagram

### 12.3 USECASE DIAGRAM

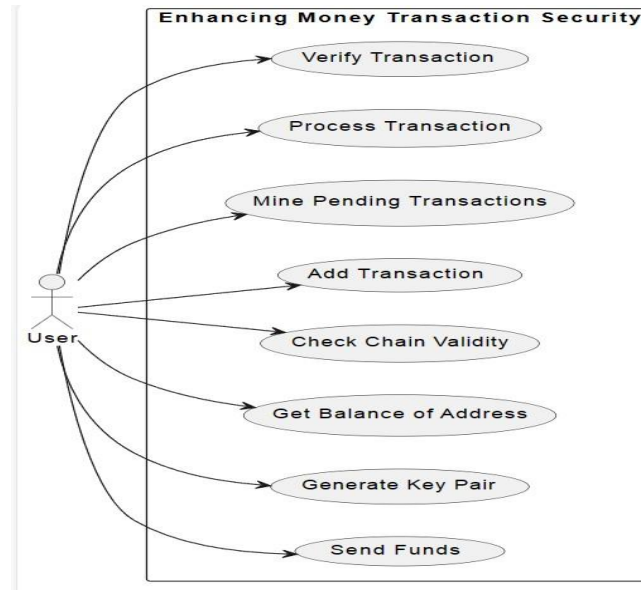


Figure 4:Usecase Diagram

### 12.4 SEQUENCE DIAGRAM

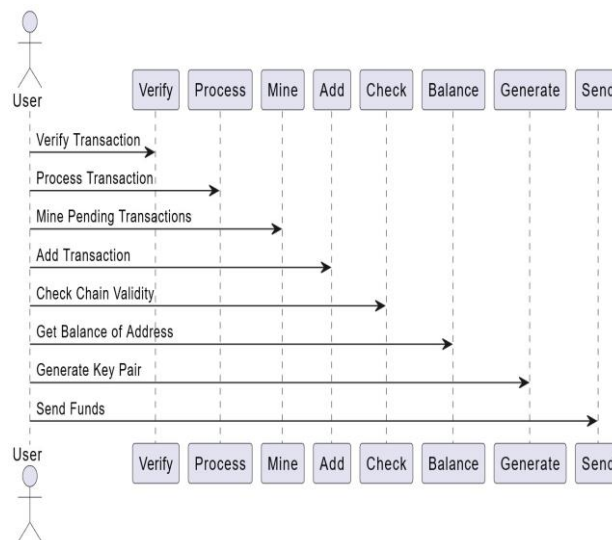


Figure 5:Sequence Diagram For Enhancing money transaction security

### 12.4 ACTIVITY DIAGRAM

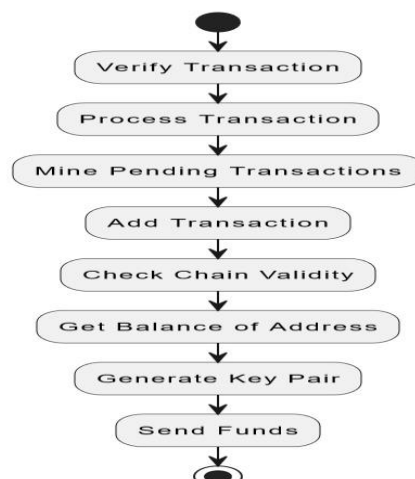


Figure 6:Activity Diagram For Enhancing money transaction security

## SOURCE CODE

### HTML CODE(FRONT END)

```
<html>
<head><title>Test one</title>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
<link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/css/bootstrap.min.css"
integrity="sha384-ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T"
crossorigin="anonymous">
<style type="text/css">
body{
color:white;
font-family: Arial;
}
#box{
width: 800px;
margin: 20px;
background-color: #4CAF50;
border-radius: 25px;
border: none;
padding: 50px;
margin-left: 150px;
}
#name{
margin-left: 50px;
border-radius: 4px;
border: 1px solid;
}
#text{
width: 50%;
height: 30%;
margin: 20px;
padding: 10px;
border-radius: 4px;
border: 1px solid;
}
#submit{
background-color: #87cefa;
border: none;
color: white;
padding: 12px 32px;
margin-left: 140px;
text-align: center;
text-decoration: none;
display: inline-block;
font-size: 16px;
}
```



```
#output{
width: 800px;
height: auto;
background-color: #4CAF50;
border-radius: 25px;
border: none;
padding: 50px;
margin: 20px;
margin-left: 150px;
}
#heading{
margin-top: 20px;
color: #4CAF50;
}
#puttext{
margin-top: -10px;
margin-bottom: 20px;
}
</style>
</head>
<body>
<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.0/umd/popper.min.js"></script>
<script src="https://maxcdn.bootstrapcdn.com/bootstrap/4.5.2/js/bootstrap.min.js"></script>
<div class="text-center">
<h2 id="heading">Decentralized Money Transcation Blockchain System</h2>
<h2 style="color:blue; id="heading">Indian SBI Bank</h2>
</div>
<div class="container">
<div class="row vertical-center-row">
<div id = "box">
<form action="#" method="POST">
<h3>PayeeName <input id="PayeeName" name="PayeeName"/></h3>
<h3>AmountTransfer <input id="AmountTransfer" name="AmountTransfer"/></h3>
<input class="btn btn-primary" id="submit" type="submit"/>
</form>
</div>
</div>
<div class="container center">
<div class="row vertical-center-row">
<div id = "output">
{% for i in name_list %}
<h3 >PayeeName: {{ i[0] }}</h2>
<h4 id="puttext">AmountTransfer: {{ i[1] }}</h3>
{% endfor %}
```

</div>

</div>

</div>

</body>

</html>

#### PYTHON CODE(BACKEND)

```
import datetime
import hashlib
from flask import Flask, request, render_template
class Block:
    blockNo = 0
    data = None
    next = None
    hash = None
    nonce = 0
    previous_hash = 0*0
    timestamp = datetime.datetime.now()
    def __init__(self, data, name):
        self.data = data
        self.blockName = name
    def hash(self):
        h = hashlib.sha256()
        h.update(
            str(self.nonce).encode('utf8')+
            str(self.data).encode('utf8')+
            str(self.previous_hash).encode('utf8')+
            str(self.timestamp).encode('utf8')+
            str(self.blockName).encode('utf8'))
        return h.hexdigest()
    def __str__(self):
        return "Block Hash: " + str(self.hash()) + "\nBlockName: " + str(self.blockName)+ "\nBlock Data: " + str(self.data) +
            "\nHashes: " + str(self.nonce) + "\n-----"
class Blockchain:
    diff = 10
    maxNonce = 2**32
    target = 2**(256-diff)
    block = Block("Genesis text", "Genesis")
    dummy = head = block
    def add(self, block):
        block.previous_hash = self.block.hash()
        self.block.next = block
        self.block = self.block.next
    def mine(self, block):
        for n in range(self.maxNonce):
            if int(block.hash(), 16) <= self.target:
                self.add(block)
                print(block)
```

```

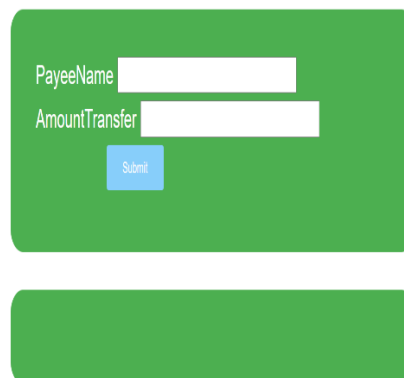
return block.blockName,block.data
else:
block.nonce += 1
app = Flask(_name_)
blockchain = Blockchain()
my_dict = []
@app.route("/")
def my_form():
return render_template('index.html',content = "")
@app.route('/',methods=['POST', 'GET'])
def my_form_post():
PayeeName = request.form['PayeeName']
AmountTransfer = request.form['AmountTransfer']
nm, tx = blockchain.mine(Block(AmountTransfer, PayeeName))
my_dict.append([nm,tx])
return render_template('index.html', name_list = my_dict)
if __name__=="__main__":
app.run(debug=True)

```

### 13. OUTPUT

#### OUTPUT WINDOWS

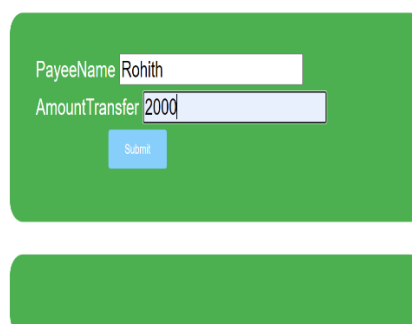
Decentralized Money Transcation Blockchain System  
Indian SBI Bank



**Figure 7:**Output WindOW

#### GIVING INPUT:

Decentralized Money Transcation Blockchain System  
Indian SBI Bank



**Figure 8:**Giving Input

## OUTPUT: REAL STORAGE VIEW

Decentralized Money Transcation Blockchain System

Indian SBI Bank

PayeeName   
AmountTransfer

PayeeName: rohith  
AmountTransfer: 4554  
  
PayeeName: dileep  
AmountTransfer: 7845  
  
PayeeName: Rohith  
AmountTransfer: 10000

Figure 9:Real Storage View

## BACK END WINDOW ON VSC TERMINAL OUTPUT:

```

PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS

Block Data: 2000
Hashes: 160
-----
127.0.0.1 - - [04/May/2024 18:10:50] "POST / HTTP/1.1" 200 -
Block Hash: 19d3370410520f3f6cb09f58b90efbcf21067b7e7d45a43623c2f0af517d9c6a
BlockName: manisha
Block Data: 50000
Hashes: 3692
-----
127.0.0.1 - - [04/May/2024 18:10:58] "POST / HTTP/1.1" 200 -
Block Hash: 55cc996e0a67f96350e78f6cc2ed011ade4da39e5353b750492b63ae42b9781a
BlockName: vaishali
Block Data: 8456
Hashes: 278
-----
127.0.0.1 - - [04/May/2024 18:11:04] "POST / HTTP/1.1" 200 -

```

Figure 10:Back End Window Output

## 14. CONCLUSION

We've created all the architecture for a blockchain, from a set of state transition rules to a method for creating blocks, to mechanisms for checking the validity of transactions, blocks, and the full chain. We can derive the system state from a downloaded copy of the blockchain, validate new blocks that we receive from the network, and create our own blocks. The system state that we've created is effectively a distributed ledger or database- the core of blockchain for secure transfer of money.

This is a new and unique way to develop a system for securing transactions. Third Parties, Attacks or any system will take a lot of time to crack this system. We can say it is tough to break the transaction



---

## **15. 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] Shen, Y., Wang, G. (2017) Improved preimage attacks on RIPEMD-160 and SHA-160. Ksii Transactions on Internet & Information Systems., 12: 727-746.
- [6] Wang, H.Q., Wu, T. (2017) Cryptography in Blockchain. Journal of Nanjing University of Posts and Telecommunications., 37: 61-67.
- [7] Yuan, Y., Wang, F. (2016) Current Status and Prospects of Blockchain Technology Development. Acta Automatica Sinica., 42: 481-494.
- [8] Miyaji, A. (1994) Elliptic Curves Suitable for Cryptosystems. Ieice Transactions on Fundamentals of Electronics Communications & Computer Sciences., 77: 98-105.
- [9] He, P., Yu, G., Zhang, Y.F. (2017) Prospective review of blockchain technology and application. Computer Science., 44: 1-7.
- [10] Zhai, S.P., Li, Z.Z. (2018) The data block chain of the key technologies Consistency. Computer Technology and Development., 8: 1-6.
- [11] An, Q.W. (2017) Research and application of key technologies for decentralized transactions based on blockchain. Donghua University.