Bank Records Storage System Through Blockchain

Rohitchandran R
Computer Science And Engineering
Saveetha Engineering College
Chennai, India
rohit242smirtha@gmail.com

Santhoshkumar B
Computer Science And Engineering
Saveetha Engineering College
Chennai, India
sanrekbal@gmail.com

Manoj Kumar V
Computer Science And Engineering
Saveetha Engineering College
Chennai, India
manojvk2002@gmail.com

Ravindhar N.V (asst.professor)
Computer Science And Engineering
Saveetha Engineering College
Chennai, India
ravindhar@saveetha.ac.in

***Abstract* - This research puts forth a system that utilizes the integration of blockchain, a database for storage, and cryptography to preserve the confidentiality and security of bank records. The blockchain ensures the protection and dependability of data storage through its use, while smart contracts regulate the way the data is stored and shared. The original bank records are kept in a secured, encrypted format on a separate database, with only their hash values recorded on the blockchain. To further secure the data, the off-chain records are frequently connected with the hash information on the blockchain. The utilization of cryptography aids in the encryption of documents and the digital signing of messages. The system has a WebApp interface that enables parties involved in the transaction to communicate in a decentralized manner.**

Keywords - Cryptography, Blockchain.

I. INTRODUCTION

Blockchain technology enables parties who do not fully trust each other to reach consensus regarding the status of a database, without the need for an intermediary. By offering a ledger that is not managed by any one entity, blockchains have the potential to deliver specific financial services, such as payments or securities, without relying on a bank.

Additionally, the use of blockchain technology makes possible the implementation of tools like smart contracts, which are automated agreements built on the blockchain. These contracts have the potential to streamline various manual processes, from compliance and claims administration to the distribution of assets outlined in a will.

In cases where decentralization is not a major concern, DLT provides an option for businesses seeking improved coordination. DLT, which is similar to blockchain, can help companies improve their governance and set higher standards for data sharing and collaboration.

Blockchain and DLT present a significant chance to transform the banking sector worth over $7 trillion by eliminating intermediaries and the core services offered by banks.

1) Payment Processing: The establishment of a decentralized ledger for payment transactions, like with Bitcoin, using blockchain technology has the possibility of enabling faster payment processing at reduced costs, compared to using traditional banking methods.

2) Clearing and Settlements: The adoption of distributed ledgers via blockchain technology has the possibility of lowering operational costs and approaching the realization of real-time transactions between financial organizations

3) Financing: With Initial Coin Offerings (ICOs), a new approach to financing is being tested which decouples the process of obtaining capital from conventional funding services and firms.

4) Investments: By turning traditional securities such as bonds, stocks, and alternative assets into tokens and placing them on public blockchain networks, blockchain technology has the potential to create more efficient and interconnected capital markets.

II. LITERATURE REVIEW

The authors of [1] discussed the design and development of a secure and private system for managing patients' electronic healthcare records in third-party cloud platforms.

In [2], the writers described a mixed model for a digital money released by a central bank that makes use of blockchain technology. They additionally, the authors propose a CBDC supervision mode and optimize the DPOS-BFT algorithm to speed up consensus. The system's efficiency has been demonstrated through simulation experiments.

The authors of [3] have looked into ways to enhance the functionality of the Hyperledger Fabric technology.

Their findings demonstrate that the batch processing method can significantly improve the performance of Hyperledger Fabric.

A blockchain application in education is presented by the writers of [4] as a Data Security Storing Proof System. This study aims to lessen mistakes and data fabrication in the education sector, which has struggled with incorrect data preservation. A process analysis method is used in the research to create reliable systems for confirming data preservation.

The authors of [5] described a method for using cloud storage and the blockchain environment to securely store electronic medical records (EMR) on the interplanetary file system (IPFS). The suggested system, which makes use of the safe elements of an autonomous Interplanetary File System, is an unified storing system for healthcare organisations globally (IPFS). Additionally, the system makes use of the blockchain environment to store private information and the role-based access control (RBAC) systemto manage entry to the storage.

The authors of [6] proposed "A Fog Computing Architecture Integrating Blockchain and Internet of Things for Securing Bank Accounts". A blockchain is a decentralized ledger in which all participants can see each other's transactions. A blockchain is a distributed ledger that records asset trades between members of a community. The connection between two blocks is made using the SHA-256 algorithm. Block chain breaks data into little parts and distributes them around a network of computers instead of storing data in a single spot or uploading it to a cloud service. Use the block chain technique to validate and trace transactions for online commerce. Block chains were created to handle certain transactions with specific validation needs.

III. METHODOLOGY

Implementing bank records through blockchain requires a thorough methodology to ensure secure and efficient implementation. Here are the steps for implementing bank records through blockchain:

Determine the bank's requirements and processes: The bank should evaluate its existing processes and determine the aspects that could be improved through blockchain implementation.

Select the appropriate blockchain platform: Once the requirements and processes have been identified, the bank can select the appropriate blockchain platform that aligns with its needs.

Design the smart contracts: The bank should design smart contracts that reflect its processes and requirements. Smart contracts are agreements that automatically carry out their conditions after being put into lines of code. They automate processes and ensure security by verifying the legitimacy of transactions before execution.

Develop the blockchain infrastructure: Once the smart contracts have been designed, the bank can begin developing the blockchain infrastructure. This involves setting up nodes, creating a consensus mechanism, and establishing a governance structure. The bank should also ensure that its infrastructure is secure and scalable to accommodate future growth.

Test the blockchain infrastructure: The bank should test the blockchain infrastructure to ensure that it meets the requirements and specifications. Testing should involve running various scenarios and verifying that the smart contracts and the blockchain infrastructure work as intended.

Integrate the blockchain infrastructure with the bank's existing systems: Once testing is complete, the bank can integrate the blockchain infrastructure with its existing systems. This may require modifying or updating the existing systems to ensure compatibility with the new blockchain infrastructure.

Provide training and support: The bank should provide training to its employees on how to use the new blockchain infrastructure. It should also provide support to ensure that any issues are resolved promptly, and the blockchain infrastructure continues to meet the bank's needs.

By adopting blockchain technology, which records or securely stores data in the form of blocks, a user has the capacity to send money to another user. To increase security, the ganache server stores the user's private key. In order to view the balance, Metamask has access to user accounts.

In conclusion, implementing bank records through blockchain requires careful planning and execution. The bank should identify its needs, select the appropriate platform, design smart contracts, develop the infrastructure, test it, integrate it with existing systems, and provide training and support to ensure a successful implementation.

A. HASH FUNCTION AND MINING

The process of Bitcoin mining involves finding a nonce value that, when concatenated with a message (in this case, "hello bitcoin"), results in a hash string with a specific number of driving ones. This is achieved by using the SHA256 hash function[14], which converts a line of erratic length into a fixed-length line of 64 hexadecimal characters. To mine a nonce, the process must be repeated multiple times to reach the desired difficulty level. In this example, the difficulty level is set to 2 leading ones. A wallet in the context of Bitcoin is comprised of a private and public key pair. The public key is utilized to get exchanges, while the confidential key is utilized to spend reserves. In reality, wallets are more complex, consisting of multiple key pairs and addresses to enhance privacy and security. The process of Bitcoin mining involves finding a nonce value that, when concatenated with a message (in this case, "hello bitcoin"), results in a hash string with a specific number of driving ones. This is achieved by using the SHA256 hash function, which converts a line of erratic length into a fixed-length line of 64 hexadecimal characters. To mine a nonce, the process must be repeated multiple times to reach the desired difficulty level.

B. PUTTING TRANSACTIONS IN BLOCK

When wallets are created and transactions are conducted, the transactions are grouped into blocks. Miners then engage in the process of mining these blocks, which requires verification of the transactions what's more, tracking down a nonce that outcomes in a hash that beginnings with a particular number of zeros[15]. Mining is compensated through the main exchange in the block, ordinarily known as the Beginning block, which awards 25 coins to the address chosen by the miner. Furthermore, the miner can direct transaction fees to their desired address by including them in the block during the mining process.

C. PROOF OF WORK

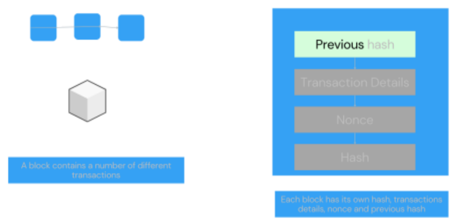

Fig. 1. Proof of Work

Previous hash: The hash address of a block indicates its location in the blockchain, and each block contains a reference to the previous block, which is identified by its hash (shown in Fig. 1).

Transaction details: The block is designed to store all the necessary transaction details that need to take place [9]. It serves as a repository for this information.

Nonce: To distinguish a block's hash address, a Nonce - a unique numerical value is assigned in cryptography [12]. This Nonce can only be used once and is adjusted by miners to create a valid hashing value. By obtaining the perfect Nonce, the hash value is recalculated to increase its difficulty in being compromised.

Hash address of the block: When information is processed through a hashing calculation, it generates a 256-digit, 64-character length value, known as a unique "hash address" or the hash address of the block [11]. To fulfill the predetermined condition, people worldwide use computational algorithms to determine the correct value of the hash. Once the predetermined condition is met, the transaction is completed. In other words, blockchain miners globally attempt to solve a mathematical puzzle, and the first one to solve it is rewarded.

Ethereum platform: While the user is authenticated into the block using a combination of their public and private keys.

Some of the top benefits of Blockchain in banking are given below:-

- Cost reduction
- Faster transactions
- Improved security

IV. SYSTEM ARCHITECTURE

The process of blockchain involves establishing wallets for users and enabling transactions between them, which are then grouped into blocks. Miners then perform the task of mining these blocks by verifying the transactions and finding a nonce that results in a hash that begins with a certain number of zeros [5]. The miner is rewarded for this process through the Genesis block, typically the first transaction in the block, which grants 25 coins to the miner's selected address. The miner also has the option to redirect transaction fees to their preferred address by including them in the block during the mining process. Because blockchain is a decentralized system, a bank has the capacity to store user records through blocks. No one can access the information without the user's private key. Without paying additional costs, a transaction can be completed anywhere in the world [10]. A blockchain transaction process shown below in Fig. 2.

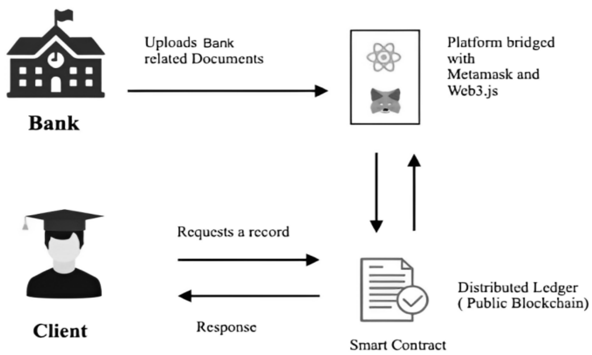

Fig. 2. System Architecture

V. MODULE DESCRIPTION

The three components of this proposed systemare:

- Blockchain Data Storage.

- Data Storage through Transactions.
- Hash Storage on the Blockchain.

Storing data on the blockchain: The user's public key is retrieved from the ganache server and used to generate wallets. A user's account can be imported into metamask using their private key. Metamask has access to all user accounts[13]. The act of storing data on the blockchain is challenging due to various difficulties that arise.

Data-driven Transactions on the blockchain: The blockchain operates on transactions (shown in Fig. 3) that are executed based on the data stored in the blockchain [16].

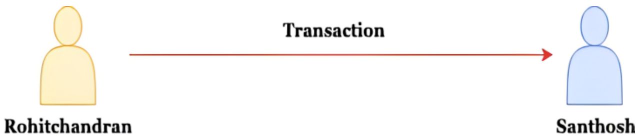

Fig. 3. Transaction on Blockchain

Hashes for Encryption and Security: Hashes are utilized for safeguarding the content by encrypting messages through the blockchain which is shown below in fig. 4.

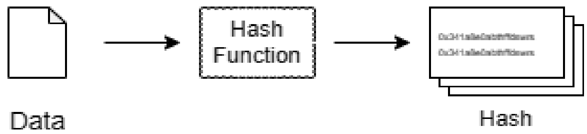

Fig. 4. Generating Hash by using SHA-256 Algorithm

VI. CONCLUSION

By implementing this proposed system, the existing bank service can be made more secure transaction, can track the failed transactions, and can retrieve the money by implementing record storage system through blockchain.

REFERENCES

[1] K. Zala, H. K. Thakkar, R. Jadeja, P. Singh, K. Kotecha and M. Shukla, "PRMS: Design and Development of Patients' E-Healthcare Records Management System for Privacy Preservation in Third Party Cloud Platforms," in IEEE Access, vol. 10, pp. 85777-85791, 2022, doi: 10.1109/ACCESS.2022.3198094.

[2] J. Zhang et al., "A Hybrid Model for Central Bank Digital Currency Based on Blockchain," in IEEE Access, vol. 9, pp. 53589-53601, 2021, doi: 10.1109/ACCESS.2021.3071033.

[3] J. -W. Lee and S. Park, "A Study On Performance Improvement Of Hyperledger Fabric Through Batched Chaincode Message," 2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS), Daegu, Korea (South), 2020, pp. 259-262, doi: 10.23919/APNOMS50412.2020.9236779.

[4] U. Rahardja, Q. Aini, N. Lutfiani, F. P. Oganda and A. Ramadan, "Blockchain Application in Education Data Security Storage Verification System," 2022 1st International Conference on Technology Innovation and Its Applications (ICTIIA), Tangerang, Indonesia, 2022, pp. 1-4, doi: 10.1109/ICTIIA54654.2022.9936028.

[5] S. Routray and R. Ganiga, "Secure Storage of Electronic Medical Records(EMR) on Interplanetary File System(IPFS) Using Cloud Storage and Blockchain Ecosystem," 2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT), Erode, India, 2021, pp. 1-9, doi: 10.1109/ICECCT52121.2021.9616690.

[6] A. S, N. R and N. S, "A Fog Computing Architecture Integrating Blockchain and Internet of Things for Securing Bank Accounts," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2022, pp. 1326-1330, doi: 10.1109/ICAAIC53929.2022.9792983.

[7] S. Sakho, Z. Jianbiao, F. Essaf and K. Badiss, "Improving Banking Transactions Using Blockchain Technology," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 2019, pp. 1258-1263, doi: 10.1109/ICCC47050.2019.9064344.

[8] Y. -T. Lee, J. -J. Lin, J. Y. -J. Hsu and J. -L. Wu, "A Time Bank System Design on the Basis of Hyperledger Fabric Framework," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2020, pp. 1-3, doi: 10.1109/ICBC48266.2020.9169476.

[9] J. Liu, X. He, R. Sun, X. Du and M. Guizani, "Privacy-Preserving Data Sharing Scheme with FL via MPC in Financial Permissioned Blockchain," ICC 2021 - IEEE International Conference on Communications, Montreal, QC, Canada, 2021, pp. 1-6, doi: 10.1109/ICC42927.2021.9500868.

[10] N. H. Arrifin and U. Subramanian, "Blockchain in Banking," 2022 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, Indonesia, 2022, pp. 58-63, doi: 10.1109/ICITSI56531.2022.9970827.

[11] S. P. Gochhayat, E. Bandara, S. Shetty and P. Foytik, "Yugala: Blockchain Based Encrypted Cloud Storage for IoT Data," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 483-489, doi: 10.1109/Blockchain.2019.00073.

[12] J. P. de Brito Gonçalves, G. Spelta, R. da Silva Villaça and R. L. Gomes, "IoT Data Storage on a Blockchain Using Smart Contracts and IPFS," 2022 IEEE International Conference on Blockchain (Blockchain), Espoo, Finland, 2022, pp. 508-511, doi: 10.1109/Blockchain55522.2022.00078.

[13] A. Davenport and S. Shetty, "Air Gapped Wallet Schemes and Private Key Leakage in Permissioned Blockchain Platforms," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 541-545, doi: 10.1109/Blockchain.2019.00004

[14] J. S. Gazsi, S. Zafreen, G. G. Dagher and M. Long, "VAULT: A Scalable Blockchain-Based Protocol for Secure Data Access and Collaboration," 2021 IEEE International Conference on Blockchain (Blockchain), Melbourne, Australia, 2021, pp. 376-381, doi: 10.1109/Blockchain53845.2021.00059.

[15] Z. Su, H. Wang, H. Wang and X. Shi, "A Financial data security sharing solution based on blockchain technology and proxy re-encryption technology," 2020 IEEE 3rd International Conference of Safe Production and Informatization (IICSPI), Chongqing City, China, 2020, pp. 462-465, doi: 10.1109/IICSPI51290.2020.9332363.

[16] M. Xie, Z. Liao and L. Huang, "Data Security Based on Blockchain Digital Currency," 2020 3rd International Conference on Smart BlockChain (SmartBlock), Zhengzhou, China, 2020, pp. 5-10, doi: 10.1109/SmartBlock52591.2020.00009.