

# *Blockchain Technology for Protecting Banking System*

**Komal Mahajan**  
MSC (Computer Science)  
Indira College, Malegaon

**Radhika Shinde**  
MSC (Computer Science)  
Indira College, Malegaon

**Prof. Gokul B. Hiray**  
Indira College, Malegaon

---

**Abstract-:** *Adding digital technology has revolutionized the life of people. There are numerous pitfalls and frauds detected in banking system. A centralized database is used by banking system which makes the bushwhacker easy to get access to data and this makes the system insecure. The debit of this centralized system can be reduced by reforming the system by enforcing blockchain technology without using commemoratives. Blockchain uses decentralized armature for storing and penetrating data over the database. This reduces attacks on database addressed. Deals done through blockchain technology are vindicated by each block in the chain, which will make the sale more secure and help banking system work briskly*

**Keywords—** Blockchain, Prevention, Security, Digital technology

---

## I. INTRODUCTION

Blockchain is a decentralized ledger used to securely exchange digital currency, perform deals and transactions. Each member of the network has access to the latest copy of encrypted ledger so that they can validate a new transaction. Blockchain ledger is a collection of all Bitcoin transactions executed in the past. Basically, it's a distributed database which maintains a continuously growing tamper proof data structure blocks which holds batches of individual transactions. The completed blocks are added in a linear and chronological order. Each block contains a timestamp and information link which points to a previous block. Banking and financial institutions are using Blockchain based technology to reduce risk and prevent cyber fraud. A block will have one parent but can have multiple child each referring to the same parent block hence contains same hash in the previous block hash field. Every block contains hash of parent block in its own header and the sequence of hashes linking individual block with their parent block creates a big chain pointing to the first block called as Genesis block. Bitcoin is peer-to-peer permission-less network which allows every user to connect to the network and send new transaction to verify and create new blocks.

The blockchain technology is a peer-to-peer distributed structure which could be used to overcome the issue in the traditional banking system. It is a collection of blocks that hold the encrypted transactional details sharing the same timestamp. The nodes of the network (miners) are responsible for linking the blocks to one another in chronological order, where each block contains the hash of the block created before in the chain. These hash values are the digital signature of each block and are dependent on two variables, first being the transactional details, and second is the hash value of the previous block. There are multiple hashing algorithms like SHA256, RSA to achieve this. Even a minute change in any of the two variables will have a significant influence on the digital signature throughout the blockchain; thus overall, it provides a good security measure in a public ledger.

## II. LITERATURE SURVEY

These are the literature survey which is based on different research paper that related to our own project

Nikita Rajeshkumar Bagrecha, Ishaq Mustafa Polishwala [1] To giving these functionalities in a distributed banking system using blockchain, which will be at par with the current methodologies. It will also focus on the limitations while implementing blockchain and future scope.

Natalia A. Popova, Natalia G. Butakova[2] To analyzes the protection mechanisms of distributed databases, proposes a solution to the problem of maintaining the uniqueness of information in them based on Blockchain technology without tokens and gives recommendations on the introduction of Blockchain technology into modern banking system The purpose of the work is the analysis and development of recommendations for the protection of information in geographically-distributed structures, typical of modern banks, based on the Blockchain technology

D.Sharma[3] To figure out the platform, the initial point of this research is an analysis of how the technology operates and functions after that the benefit for business and economic transaction are analysed and afterwards the research deals with an impact of new technology on banking, above all on financial functions. The hypothesis is that blockchain has achieved a great impact on banking sector, also it has the potential to thoroughly modify only the financial and banking sector but also the way we buy and sell our interaction with the authorities as a way of authenticating the holding from the authorship. Using the available data and hypothesis of knowledge from the fields of technology, economics, finance, and politics, 4 scenarios were set up for the future of basic technology. The scenario combined with trend analysis in order to prove the starting hypothesis with high reliability, authenticated and accuracy. Banking progressively detect the power of this technology to exploit the benefits of the Fourth Technological Revolution. The research conclusion shows that the technology being checked already has a deep impact on the banking sector, that it is in the starting phase of modifying many industries, with the possibility that they will change them automatically in the next five to ten years.

Priya D. Dozier, Troy A. Montgomery[4] It explores the technology evaluation process concurrently as decision makers reacted to the potential uses, as opposed to a retrospective view after a technology innovation had been adopted. Evidence suggests that, organizations applied a specific process to determine the value of blockchain that consisted of understand, organize, and test, which collectively helped create the proof-of-value model. Surprisingly, they find that financial service organizations tend to view blockchain innovation as a lower priority due to the lack of a clear path to value. Additionally, financial service organizations consistently leverage industry consultants to link to external knowledge and help with the decision-making process. Our findings have direct implications to both innovation researchers as well as practitioners seeking to evaluate blockchain technology.

Ye Guo, Chen Liang[5] Present the issues of implementing blockchain in financial sectors. It illustrates how some of the current major banking organizations are exploring regarding the same. As it has been already stated that Blockchain is a truly decentralized system but under many scenarios a security of certain extent is required especially while dealing with money. Thus, they have compared Public Blockchains, Consortium Blockchains and Private Blockchains. They propose numerous financial institutions which can create a consortium blockchain which is the promising model in the banking industry. They have also proposed how industrial standards could be implemented using this technology.

Liu Songyue, He Shangyang[6] They focuses on building an irreversible distributed financial system based on large data in the context of large data in order to apply the scenario of "Block Chain Technology + Accounting Services" to the accounting industry, and prospects the application of Block Chain Storage Technology and Intelligent Internet of Things technology based on large data, providing inspiration for future research.

Satoshi Nakamoto[7] proposes a system for electronic transaction among consumers without relying on trust. Here the cryptocurrency is formed by a framework of digital signatures which provides ownership and prevents the problem of double spending. Also, a peer-to-peer network using Proof of Work (POW) is proposed to enable this system. Hence it is a robust and secure distributed system. This paper proposes a basic idea of using Hash values and Timestamp server so as to maintain the integrity of the

cryptocurrency and the transactions by broadcasting a new creation of block or a new transaction among all the nodes present in the network.

Tong Wu and Xiubo Liang[8] They illustrates that blockchain can be implemented for registration and documentation of various tangible and intangible goods like intellectual property rights, pictures, proof of property, vote statistics, smart contracts etc. As they all require a transparent and open information source. The major focus of the paper is about distributed databases where even if one or several nodes fail the transaction stored on the other nodes are not affected and the failed nodes can back up the information from the other nodes present in the network. They also illustrate that smart contracts basically put a set of contract terms into agreement among untrusted parties. It also initiates a solution to use blockchain to overcome traditional interbank payment issues by creating private blockchain networks thus such transactions are less prone to risk and are more time efficient.

Supriya Thakur Aras, Vrushali Kulkarni [9]explains the concept of non-tokenized schema, blockchain taxonomy and hybrid solutions to become permissioned blockchain from permission less blockchain. Proof of Work (POW) protocol enables all the nodes in the network to solve a cryptographic puzzle by brute force and the winning node is rewarded with some revenue which is then broadcasted in the network. Proof of Stake (POS) protocol is basically block verification by miners using ethereum and altcoins which does not rely on excessive computations.

Ibrar Ahmed, Shilpi , Mohammad Amjad[10] Provides the evolution of blockchain technology from Merkle tree to provide a secure history of data exchange. It explains the concept of asymmetric cryptography among nodes of a distributed network. This paper portrays a basic blockchain architecture that is the sequence of blocks and the inter-relation between them using the hash of the parent block. It also provides an architecture of the block where the block is divided into a block header and the transactional details.

### III. PROPOSED SYSTEM

In the proposed system, the typical bank design, which comprises on a centralized database, would be excluded in the suggested system. The data will be dispersed extensively over the block chain, making banking institutions decentralized. This won't only make data more secure, but it'll also polarize authority. There are two advantages to the sale system outlined over. To begin with, it'll speed up deals by barring the central procedures that are now used in regular deals, and it'll also make it nearly delicate for an individual to hack the system since it'll demand a massive quantum of calculating power that no bone possesses. To apply the below- mentioned system, we can have two different types of bumps, verification bumps belonging to the bank and the stoner knot for guests. And there will be multiple stoner bumps and verification bumps in a distributed system. Verification bumps will be responsible for the authorized tasks similar as vindicating a client's account, vindicating a sale and creating a block for a number of deals for a given timestamp. And after creating the block it has to broadcast it in the network. stoner knot is used by the guests so they can initiate a new sale, view their account history and so on. Each stoner knot is meant to store the public and private key needed for the stoner's sale. Also, it'll store the most streamlined blockchain. This won't only make the data ore secure but also will remove the power centralization. The deals over the block chain will be in form of translated commemoratives which will be vindicated by each bumps on the block chain. To make any sale valid, the bumps of the block chain will have to give the evidence of the processing it has done in order to corroborate the sale. That evidence will be taken in terms of the quantum of processing done. The below mentioned sale system has two benefits. this system would be suitable to apply a distributed system as well as the banking bumps could besemi-automatized so as to reduce work.

- Authentication
- Application for banking to handle the transactions.
- Decentralized application.

➤ Hashing Signature verification.

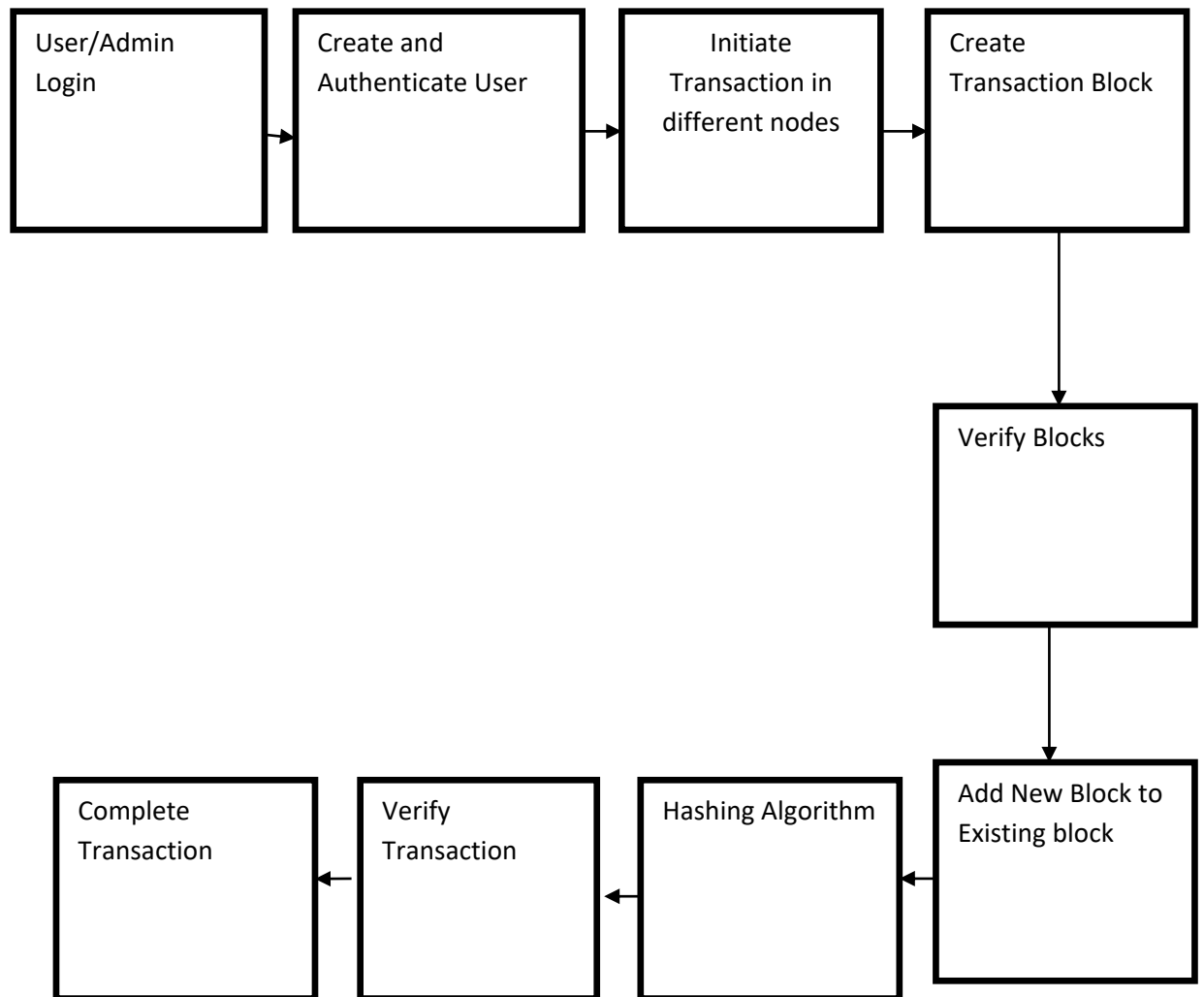


Fig -1: Proposed System

➤ **Algorithm**

Hashing Algorithm

A hashing algorithm is a mathematical algorithm that converts an input data array of a certain type and arbitrary length to an output bit string of a fixed length. Hashing algorithms take any input and convert it to a uniform message by using a hashing table.

Step 1: Append Padding Bits.

Message is “padded” with a 1 and as many 0’s as necessary to bring the message length to 64 bits fewer than an even multiple of 512.

Step 2: Append Length....

64 bits are appended to the end of the padded message. These bits hold the binary format of 64 bits indicating the length of the original message.

Step 3: Prepare Processing Functions.

## ➤ Fraud Detection

### Auditing Algorithm

1. Start
2. Read data owner id(udoid)
3. If (doid udoid)
4. Stop
5. Read file name from AWS
6. Retrieve No. of blokes from TPA xml
7. Select the blocks number the user want to verify.
8. Get the auxiliary information for block chal from TPA xml
9. Based on Auxiliary information generate new root for MHT
10. If (new root root) file modified
11. Else File not modified
12. Stop.

## CONCLUSION

Blockchain technology can be utilised to get around the drawbacks of the old centralised banking system that have been stated. All transactions between nodes on the blockchain take place in a safe and secure environment. Due to the time and transaction charge reduction, which is important in conventional banking systems. Additionally, this technology is still being developed, so future advancements may be numerous. Blockchain technology can be utilised to get around the drawbacks of the old centralised banking system that have been stated. All transactions between nodes on the blockchain take place in a safe and secure environment. Due to the time and transaction charge reduction, which is important in conventional banking systems. Additionally, this technology is still being developed, so future advancements may be numerous.

## REFERENCES

1. N.R. Bagrecha1., R. Sharma etal., "Decentralised Blockchain Technology: Appli- cation in Banking Sector", International Conference for Emerging Technology (INCET),2020.
2. P.P. Niturkar., P.A. Kulat etal., "Block chain technology for protecting the bank- ing transaction without using tokens", Proceedings of the Second International Conference on Inventive Research in Computing Applications (ICIRCA) PP- 978-7281,2020
3. Liu Songyue., He Shangyang., "Aplication of block chaining technology in finance and accounting field", International Conference on Intelligent Transportation, Big Data Smart City (ICITBS) PP- 978-1-7281, 2019.
4. Divya Sharma,"Application of block chain in an indian Banking Sector", [www.globalscientificjournal.com](http://www.globalscientificjournal.com), Vol-8, PP-2320-9186, 2020.
5. P.D. Dozier., T.A. Montgomery., "Banking on Blockchain: An Evaluation of In- novation Decision Making" IEEE TRANSACTIONS ON ENGINEERING MAN- AGEMENT, PP-0018-9391, 2019.
6. V. Naik, R. Singh etal., "Expeditious banking using Blockchain Technology", IEEE International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE) ,2020.
7. F. Essaf., S. Sakho., "Improving Banking Transactions Using Blockchain Tech- nology", IEEE 5th International Conference on Computer and Communications, 2019.
8. Ye Guo and Chen Liang ." Blockchain application and outlook in the banking industry", Springer Open, 2016.
9. N.R. Bagrecha1., R. Sharma., "Decentralised Blockchain Technology: Appli- cation in Banking Sector ", International Conference for Emerging Technol- ogy.2020