DISTRIBUTED BANKING SYSTEM USING BLOCKCHAIN TECHNOLOGY

Ms. Komal G. Pabale[1],
[1] *Student, Department of Computer Engineering,*
Amrutvahini College of Engineering, Maharashtra, India

Dr. Manoj A. Wakchaure[2]
[2] *Professor, Department of Computer Engineering,*
Amrutvahini College of Engineering, Maharashtra, India

ABSTRACT

The Blockchain is a technology that will allow transactions simply, safely, effectively, and also safely. This is a Very promising technology. It's already in a lot of places. It can also solve any problem in the banking sector. This technology became famous after introducing the first cryptocurrency, which is known as bitcoin. Right now, there is a huge problem with banking, and the Blockchain can solve these problems. This paper will demonstrate transacting over a secure, blockchain based network and therefore eliminate the need for intermediary entities. 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. 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. Blockchain, also referred to as a distributed ledger technology, stores different transactions /operations during a chain of blocks in a very distributed manner while not having a trusted third-party. The Blockchain could be a chain of blocks each is being a storehouse that stores information pertaining to a transaction and links to the sooner block within the same trans-action. These connected blocks form a sequential chain providing a pathway of the essential transaction. There are many threats and frauds detected in industry. A centralized database is employed by banking industry which makes the attacker easy to urge access to data and this makes the system insecure. the dis-advantage of this centralized system may be reduced by reforming the system by implementing blockchain technology without using tokens. Blockchain uses decentralized architecture for storing and accessing data over the database. This reduces attacks on database hacked. Transactions done through the blockchain technology are verified by each block within the chain, which can make the transaction safer and help banking industry work faster. Proposed system aims at giving these functionalities in a very distributed banking industry using blockchain, which is able to be at par with this methodologies. It'll also concentrate on the restrictions while implementing blockchain and future scope.

Keyword: *-Distributed Ledger, Blockchain, Database, Banking Sector, Traditional Bank, Cryptography, Transactions.*

I. INTRODUCTION

In recent years, it has been observed that there are many data breaches happening in the banking system. Hackers are stealing vast amounts of money from banks because of the security issue of the banking system. Also, the banking system is improving very slowly. Even in the 21th century, it takes a lot of time, sometimes days, to make transactions. The purpose of this paper is to analyze the Blockchain system and find its use cases in the banking system. It will demonstrate why the implementation of the Blockchain can make the banking industry more secure and make transactions faster. The significance of the paper is to help the decision-makers of the banking sector and government to make them understand blockchain technology and it's potentiality in the banking sector.

Any industry being the middleman between the transactions is susceptible to threats like frauds, crashes, and cyber-attacks. Since most the banking systems are supported a centralize database, they're more susceptible to penetration attacks, which can compromise the confidential details of consumers of the bank. Similarly as for the services provided by the bank, the customer needs to pay the transactional overhead. On the opposite hand, the bank must record and maintain all the transactional details for every customer, which is mostly massive in terms of knowledge. Blockchain technology is that the solution to those problems of the present traditional industry. Blockchain technology originated when a report titled "Bitcoin: A Peer-to-Peer Electronic Cash System" was released in 2008 by Satoshi Nakamoto.. the planet Economic Forum (WEF), in 2016 has suspected that blockchain technology are going to be ready to transform financial services within the banking sector by creating a platform that connects consumers and producers directly.

A Blockchain is a digital, immovable, dispersed ledger that sequentially records transactions in real time. Blockchain technology has the potential to completely reform the universal financial industry by offering the numerous opportunities of how people transact with money and values. Blockchain technology is a new technology which is based on numerical and economic assumptions for managing a database between numerous members without the demand of any central authority. It is an assured distributed database, tamper evident, wherein the efficacy of a transaction can be verified by parties in the transaction. Each group of these transactions is assigned to as a "block". A Block records some or all of the current transactions and goes into a blockchain as a permanent record once it is ended. The benefit of Blockchain is that financial transactions no longer need any central authority and are instantly validated, cleared and settled. Blockchain technology emerge to be an innovation which ensures a major change for capital markets and other financial services.

Blockchain may be a decentralized ledger accustomed securely exchange digital currency, perform deals and transactions. Each member of the network has access to the foremost recent copy of encrypted ledger so as that they're going to validate a fresh transaction. Blockchain ledger may well be a group of all Bitcoin transactions executed within the past. Basically, it's a distributed database which maintains a continuously growing tamper proof organization blocks which holds batches of individual transactions. The finished blocks are added in an exceedingly very linear and chronological order. Each block contains a timestamp and data link which points to a previous block. Banking and financial institutions are using Blockchain based technology to cut back risk and forestall cyber fraud. A block will have one parent but can have multiple child each concerning the identical parent block hence contains same hash within the previous block hash field. Every block contains hash of parent block in its own header and so the sequence of hashes linking individual block with their parent block creates a large chain pointing to the first block called as Genesis block. Bitcoin is peer-to-peer permissionless network which allows every user to connect to the network and send new transaction to verify and make new blocks.

The blockchain technology could be a peer-to-peer distributed structure which can be wont to overcome the difficulty within the traditional industry. It's a group of blocks that hold the encrypted transactional details sharing the identical timestamp. The nodes of the network (miners) are to blame for linking the blocks to 1 another in chronological order, where each block contains the hash of the block created before within the chain. These hash values are the digital signature of every block and are hooked in to two variables, first being the transactional details, and second is that the hash value of the previous block. There are multiple hashing algorithms like SHA256, RSA to attain this. Even a moment change in any of the 2 variables will have a big influence on the digital signature throughout the blockchain, thus overall, it provides an honest security measure in an exceedingly public ledger.

II. LITERATURE SURVEY

Nikita R. Bagrecha, Ishaq M. Polishwala, Pragya A. Mehrotra, Rishabh Sharma et.al [1] To giving these functionalities in a very distributed industry using blockchain, which is able to be at par with the present methodologies. This helps in reducing the transaction fee and time, which is critical in traditional banking systems. Also, as this technology is under development, there is a multiple advancement within the future.

TongWu and Xiubo Liang[2] They illustrates that blockchain is implemented for registration and documentation of varied tangible and intangible goods like belongings rights, pictures, proof of property, vote statistics, smart contracts etc. As all of them required transparent and open information source. The main focus of the paper is about distributed databases where whether or not one or several nodes fail the transaction stored on the opposite nodes aren't affected and therefore the failed nodes can make a copy the data from the opposite nodes pre-sent within the network. They also illustrate that smart contracts basically put a collection of contract terms into agreement among untrusted parties. It also initiates an answer to use blockchain to beat traditional interbank payment issues by creating private blockchain networks thus such transactions are less vulnerable to risk and are longer efficient.

Liangming Wen, Lili Zhang, etal [3**]** They focuses on blockchain and provides a detailed analysis on its core components, technologies and applications. Then, combs the problems faced by data management in quality, security, sharing and so on, and analyzes the application advantages of blockchain technology in data management, and put forwards a data collaborative management model based on blockchain, which has the characteristics of decentralization, collective maintenance, automatic execution, and non-tamperable. The model covers user authentication, data verification, data logging, data sharing and other processes, and is equipped with a data management incentive system, which can achieve convenient, secure and fast data management. Applying blockchain technology to data management can further improve the effectiveness of data management and improve the quality of data, and create a positive data sharing environment.

Riya D. Dozier, Troy A. Montgomery [4] It explores the technology evaluation process concurrently as decision makers re-acted to the potential uses, as against a retrospective view after a technology innovation had been adopted. Evidence suggests that, organizations applied a selected process to work out the worth 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 look at blockchain innovation as a lower priority thanks to the shortage of a transparent path to value. Additionally, financial service organizations consistently leverage industry consortiums to link to external knowledge and help with the decision-making process. Our findings have direct implications to both innovation researchers furthermore as practitioners seeking to guage blockchain technology.

Qifei Zhang, Rajkumar Buyya etal [5] They focuses on Blockchain based trust management in cloud computing systems: a taxonomy, review and future directions. And survey on blockchain based trust approaches in cloud computing systems. Based on a novel cloudedge trust management framework and a double blockchain structure based cloud transaction model, it identifies the open challenges and gives directions for future research in this field.

III. BLOCKCHAIN ARCHITECTURE

Blockchain is a sequence of blocks distributed in a public ledger. Each block has a digital signature, which is in the form of hash code. These hash codes are generated considering the parent block hash code and the set of transactions contained in the current block. The block is divided into two parts: Header and Body.
There are four types of blockchain:

- Public
- Private
- Consortium
- Hybrid

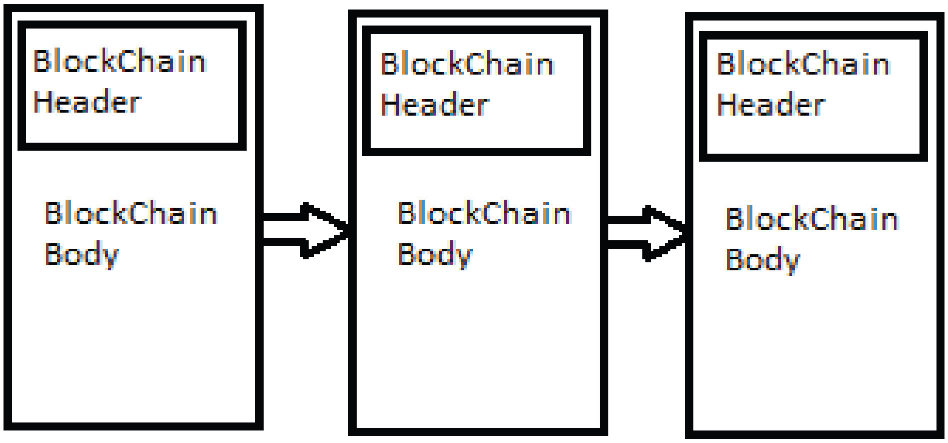


Fig.1. Architecture of Blockchain

A. *Problem Statement:*

The problem is to determine how to reduced the issues face by traditional banking like, data security, Third party involvement and also avoid attacks and generate the security message to user, so by using blockchain technology we reduced the all challenges that are faces by traditional banking system.

B. *Motivation:*

Now a days so many threats and frauds detected in banking system. Like lack of server security, insecure data storage, leakage of data on user side. A centralized database is used by banking system which makes the attacker easy to get access to data and this makes the system insecure. So the Blockchain uses decentralized architecture for storing and accessing data over the database. Blockchain reduces attacks on database hacked. And Transactions done through blockchain technology are verified by each block in the chain, which will make the transaction more secure and help banking system work faster.

C. *Objectives:*

- To study the insight of various challenges and global perspective of blockchain technology in Banking Industry.
- To reduce the need for expensive and time-consuming third-party verifications along a payment process or funds transfer.
- To provides a secure and intrusion free environment for all the transactions occurring between the nodes.
- To study how Blockchain technology that will allow transaction simply, safely, effectively and also safely.
- To study the impact of blockchain on banking industry through cryptocurrency.
- Strengthening data security during transactions and bank payments between different users.

IV. PROPOSED SYSTEM

In this proposed research work to design and develop an approach for efficient and distributed banking system using blockchain technology Blockchain technology has provided the most popular product, i.e. Bitcoin which is a type of cryptocurrency and functions as a public ledger for all transactions happening on the network. It has resolved the problem of double spending, unauthorized spending, and thus increasing security. It also helps to remove the need for an intermediary expert. Since there has been a substantial increase in the number of cyber attacks recently, the Blockchain technology help to attract the varied audience. Blockchain technology has a great future worldwide. An incredible scope of Blockchain technology has been observed in the financial field. The financial organizations were not able to sufficiently handle the heavy workload after demonetization and thus brought out the problems of having a centralized specialist for handling the financial transactions.

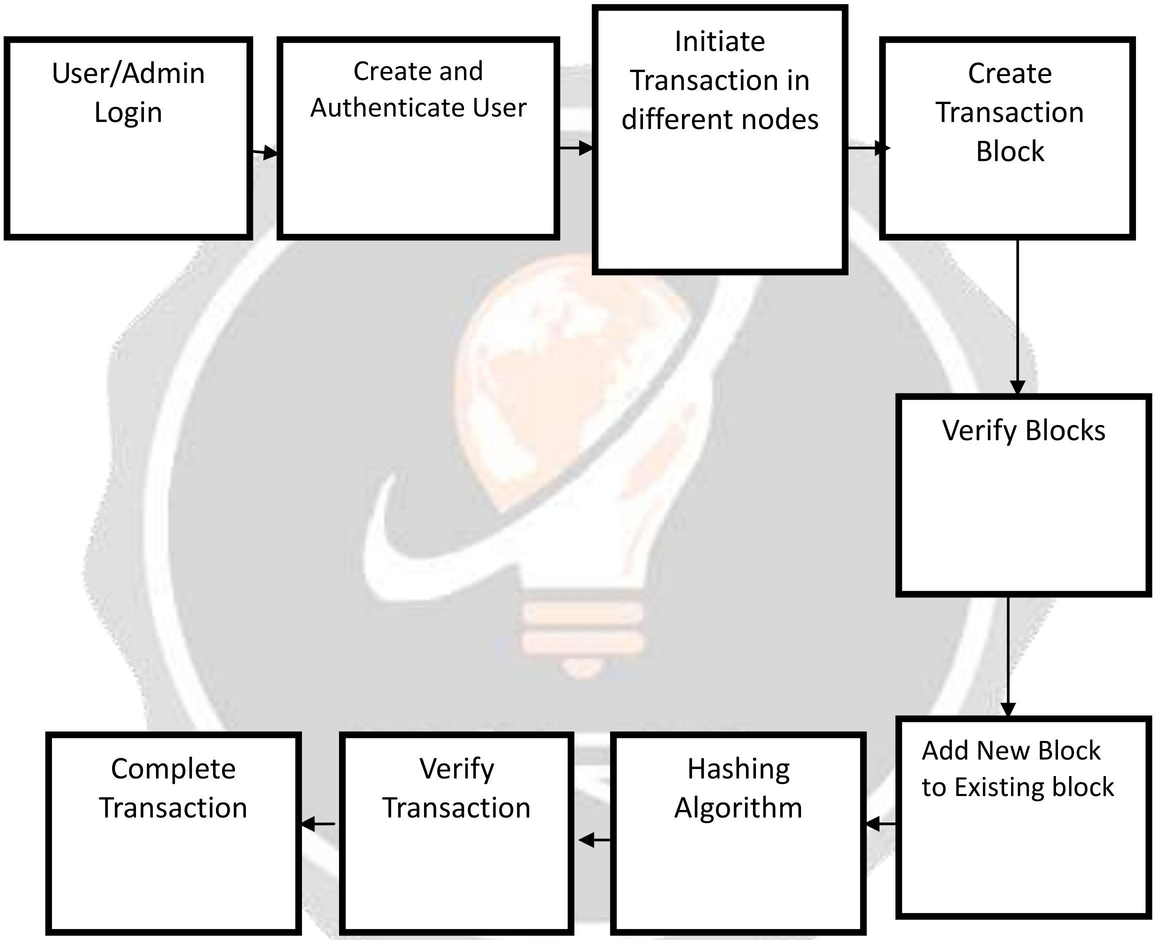


Fig. 2 Architecture diagram

Following is that the working process of the sys-tem that's developed during this study:

- A Blockchain is also a computerized concept for storing da-ta. For every transaction on a blockchain, first it must undergo several key steps.
- For a transaction within the blockchain, and authentication is required, when user request the transaction then a block with the knowledge of the transaction is created
- When the newly created block is shipped to every node or to every participant during a very

blockchain

- This nodes validate the transaction using signature based hashing algorithm.
- If the knowledge of the newly created node is wrong or al-tered, then it'll not match with other blocks of the nodes within the blockchain. Then the validation will fail, and therefore the transaction won't be recorded.
- If the data of the newly created node is match with other blocks of nodes within the blockchain or validation is passed, then the transaction is complete.
- And also the updates are going to be distributed to all or any the nodes in this particular blockchain network. and therefore the block is appended to the prevailing of blockchain. For the Proof of labor, the nodes receive an award, usually in cryptocurrency.

A. System Modules

1. Banking Application:

The banking industry is currently facing multiple pressures, including a decline in profits and an increase in risk, and has entered a new state of change and development. The sudden Internet finance boom has also led to numerous challenges in the traditional banking business. Consequently, commercial banks need to rely on new technological growth to accelerate product and service innovations, thereby adapting to new customer demands and competitive environments.

2. Transactions:

For every transaction on a blockchain, first it must go through several key steps. the working method of the blockchain can be observed. For a transaction in the blockchain, and authentication is required, then a block with the information of the transaction is created. Then the created block is sent to every node or to every participant in a blockchain. Then the nodes validate the transaction. If the information of the newly created node is wrong or altered, then it will not match with other blocks of the nodes in the blockchain. Then the validation will fail, and the transaction will not be recorded. If validation is passed, then the transaction is complete

3. Authentication:

In the blockchain, authentication works through cryptographic keys or data strings that identify users and allows access to their wallet or account on the network system. Every user gets a public key and private key that are visible to other participants.For encryption and decryption, Advanced Encryption Algorithm is used. Encryption is the process of converting the plain text message into cipher text format. For, to prevent unauthorized parties from reading it. Decryption is opposite to the encryption it translate the cipher text message into plaintext message. The original message is called as plaintext. Members' data as well as bank data are reserve in blockchain in the form of an encrypted format. When a user registers their details, All registered data as well as bank data are stored in the form of encrypted pattern. And we can decrypt this data using AES Algorithm.

4. Blockchain:

Blockchains, both public and private, can be implemented across a variety of use cases in the financial world, opening up new sectors of banking services that benefit both banks and customers by allowing faster, cheaper, more secure and more inclusive transactions. After completing the transaction, the transaction blocks are generated. Generally, the block is started with a zero-hash key. Every block is stored in its previous hash key. And this generated block is added to the existing blockchain.

B. System Algorithm

I. AES Algorithm:

The AES Encryption algorithm is a Symmetric block cipher algorithm. AES Algorithm uses a substitution-permutation, or SP network, with multiple rounds to produce cipher text.

The number of rounds depends on the key size being used. A 128-bit key size dictates 10 rounds, a 192-bit key size idictates 12 rounds, and a 256-bit key size has 14 rounds. Each of these rounds requires a round key, but since only one key is inputted into the algorithm, this key needs to be expanded to get keys for each round, including round 0.

1. Step-KeyExpansion – round keys are derived from the cipher key using the AES key schedule. AES requires a sepa-rate 128-bit round key block for every round plus yet one more.

2. Step- Initial round key addition: 1.AddRoundKey – each byte of the state is combined with a byte of the round key using bitwise xor.

3. step - 9, 11 or 13 rounds:

    1. SubBytes – a non-linear substitution step where each byte is replaced with another consistent with a lookup table.

    2. ShiftRows – a transposition step where the last three rows of the state are shifted cyclically a particular num-ber of steps.

    4. MixColumns – a linear mixing operation which oper-ates on the columns of the state, combining the four bytes in each column.

    5. AddRoundKey

4. Step - Final round (making 10, 12 or 14 rounds in total):
1. SubBytes

2. ShiftRows

3. AddRoundKey

II. Hashing Algorithm

A hashing algorithm could be a mathematical algorithm that converts an input file array of a particular type and arbitrary length to an output bit string of a set length.

Hashing algorithms take any input and convert it to the same message by employing a hashing table.

1. Step : 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 a fair multiple of 512.

2. Step : 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.

3. Step : Prepare Processing Functions. . . .

SHA1 requires 80 processing functions defined as: f(t;B,C,D) = (B AND C) OR ((NOT B) AND D) (0 != t != 19) f(t;B,C,D) = B XOR C XOR D (20 != t != 39) f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D) (40 != t !=59) f(t;B,C,D) = B XOR C XOR D (60 != t != 79)

4. Step : Prepare Processing Constants....

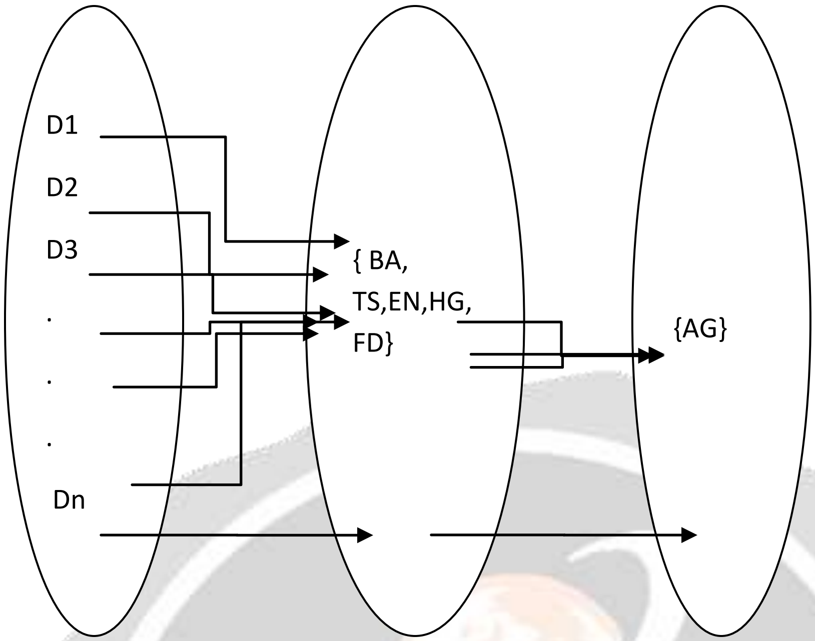
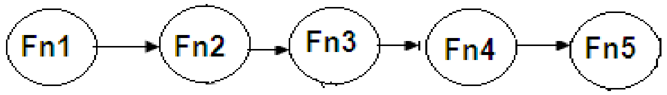
SHA1 requires 80 processing constant words defined as: K(t) = 0x5A827999 (0 != t != 19) K(t) = 0x6ED9EBA1 (20 != t != 39) K(t) = 0x8F1BBCDC (40 != t != 59) K(t) = 0xCA62C1D6 (60 != t != 79)

V. MATHMATICAL MODEL

Sr. No	**Description**	**UML design observations**
1.	1) Banking Application. 2) Transactions 3) Encryption 4) Hashing 5) Fraud Detection. Let the system be described by S, S={BA, TS,EN,HG,FD,AG}	Where S: is a System. BA: Banking Application TS: Transactions EN: Encryption HG: Hashing Generation FD: Fraud Detection AG: Alert Generation
2.	**Activity**	

	D={d1, d2,…………..., dn}
	F={f1, f2, ……………., fn}
	Y={ BA, TS,EN,HG,FD,AG }
		D is the set of Input transactions.
		F is the set of Function.
		Y is a set of techniques use for System.

3.	**Vein Diagram**	

<table>
<tr><td></td><td>
</td><td>S: is a System.
BA: Banking Application
TS: Transactions
EN: Encryption
HG: Hashing Generation
FD: Fraud Detection
AG: Alert Generation</td></tr>
<tr><td><b>4.</b></td><td><b>State diagram</b></td><td></td></tr>
<tr><td></td><td>
</td><td>Fn1: Banking Application
Fn2: Transactions.
Fn3: Encryption
Fn4: Hashing Generation
Fn5: Fraud Detection.</td></tr>
<tr><td><b>5.</b></td><td><b>Functional Dependencies</b></td><td></td></tr>
<tr><td></td><td>
<table>
<tr><th></th><th>Fn1</th><th>Fn2</th><th>Fn3</th><th>Fn4</th><th>Fn5</th></tr>
<tr><td>Fn1</td><td>0</td><td>1</td><td>0</td><td>0</td><td>0</td></tr>
<tr><td>Fn2</td><td>0</td><td>0</td><td>1</td><td>0</td><td>0</td></tr>
<tr><td>Fn3</td><td>0</td><td>0</td><td>0</td><td>1</td><td>0</td></tr>
<tr><td>Fn4</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td></tr>
</table>
</td><td>Fn1: Banking Application
Fn2: Transactions.
Fn3: Encryption
Fn4: Hashing Generation
Fn5: Fraud Detection.</td></tr>
</table>

Fn5	0	0	0	0	0

VI. RESULTS AND DISCUSSION

Recently, there have been significant changes in banking on account of the Blockchain. As the Blockchain permits untrusted gatherings to concur on the condition of a data set, individuals don’t have to depend on agents for an exchange. Blockchain innovation offers monetary types of assistance, for example, installments, without utilizing any outsider like a bank. Blockchain can give quicker instalments and lower expenses than banks, with the decentralization record for installments. On open blockchains, protections like stocks, bonds, and elective resources are set. This makes more productive capital business sectors.

Blockchain technology is that the growing invention which has a sequence of blocks. Banking and financial institutions are using Blockchain based technology to cut back risk and forestall cyber fraud. The transaction data is stored in a very distributed database. Any banking industry being the middleman between the transactions is at risk of threats like frauds, crashes, and cyber-attacks. Blockchain technology helps to get rid of the necessity for an intermediary expert. Most the banking systems are supported to the centralized databases, they're more liable to penetration attacks, which can compromise the confidential details of consumers of the bank. Banking as a service requires maintaining and securing customer information to guard it from hackers, which is increasing day-by- day.

The blockchain technology is a peer-to-peer distributed structure which could be used to overcome the issue in the traditional banking system. Aims at 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.

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

- Cost reduction
- Faster transactions
- Improved security
- Improved information quality

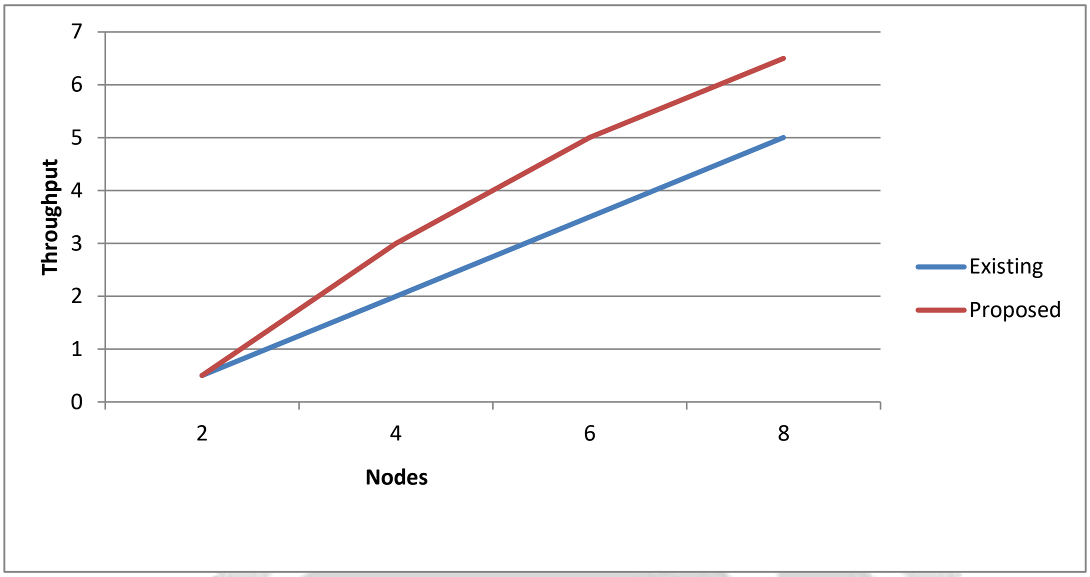


Fig.3 Results and Discussion

Throughput: the measurement of the rate of validation of blocks in the network by nodes. In the present system, people are miners who need more time to validate and build a new bloc because they have to resolve the mathematical difficulty. Nodes consume less time than the present system in the proposed system.

	Existing	Proposed
2	0.5	0.5
4	2	3
6	3.5	5
8	5	6.5

Fig.4 Graph Table

VII. CONCLUSIONS

Thus, to overcome the mentioned disadvantages of the traditional centralized banking system, blockchain technology can be used. Blockchain provides a secure and intrusion free environment for all the transactions occurring between the nodes. This helps in reducing the transaction fee and time, which is significant in traditional banking systems. Also, as this technology is under development, there can be, multiple advancement in the future. So, proposed system aims at giving these functionalities in a very distributed banking industry using blockchain, which is able to be at par with this methodologies. It'll also concentrate on the restrictions while implementing blockchain and future scope.

VIII. ACKNOWLEDGEMENT

The authors would like to give special thanks to the authorities and the Department of Computer Engineering of Savitribai Phule Pune University for giving us the resources and facilities to do this research.

REFERENCES

[1] N.R. Bagrecha1., R. Sharma etal.,"Decentralised Blockchain Technology: Application in Banking Sector", International Conference for Emerging Technology (INCET),2020.

[2] P.P. Niturkar., P.A. Kulat etal., "Block chain technology for protecting the banking 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, Vol-8, PP-2320-9186, 2020

[5] P.D. Dozier., T.A. Montgomery., "Banking on Blockchain: An Evaluation of Innovation Decision Making" IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, 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 Technology", 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: Application in Banking Sector ", International Conference for Emerging Technology. 2020.

[10] S.Thakur., V.Kulkarni., "Blockchain and its Application-A Detailed Survey", IJCA, 2017.