# BLOCKCHAIN- A SECURE MODE FOR TRANSACTION

[1]Nikunj Guna, [2]Divyang Thummar, [3]Viral Jadav, [4]Aniket Kore
[1, 2, 3] B.E Student, [4]Assistant Professor
[1, 2, 3, 4] Dept of Computer Engineering
[1,2,3,4] Universal College of Engineering, Mumbai, India

***Abstract :*** Blockchain is growing as a potentially Out of line force capable of changing the financial services industry by making the fund transfer immediate, cheaper and more secure. Current existing system is not secure enough to give 100% fraud protection because of more manual work and lack of security of data. Blockchain is nothing but a chain made of blocks (nodes).These process node does the all major work. These blocks are connected to each other using cryptography. This system will be more expeditious, more efficient, and has user affectional interfaces in the banking and has zero probability of losing data while processing of the user data. In integration to enabling trade, block chain is larceny-and tamper-resistant model, it eliminates errors and the duplication, blockchain is ideal for reserving the data in blocks and using a tamper-proof hash format, so the data can be securely stored by bank and make the current existing system much more secure and faster.Which is already done in case of cryptocurrency.

***Index Terms*** **- Blockchain, Cryptography, P2P (peer-to-peer) network, Hashing, Cryptocurrency.**

## I. INTRODUCTION

Blockchain is digital, distributed and public ledger.Blockchain technology was first used in now a days popular cryptocurrency called BITCOIN (virtual currency), but it is expected that its characteristics of accurate and guarded data transfer in distributed P2P network could make other applications possible.In blockchain nodes are connected cryptographically and in chronological order.The blockchain offers ability to distribute ledgers in decentralized way and that's a key concept. Unlike centralized system where the ledgers of records are stored in single specific entity like a bank or govermental institution, the blockchain shares the ledgers in between its participants [1]. That's what make blockchain decentralized.This means that ledgers are written and stored in network and its members are responsible to update and monitor it.Every block of record is constantly synchronized by the diffferent members of the open network, creating multiple copies of the data through a shared record-keeping system ensuring no single person or an organisation holds ownership of data. When an incipient transaction or an edit to a subsisting transaction comes in to a blockchain, generally a most of the nodes within a blockchain implementation have to apply steps (algorithm) to calculate and validate and verify the past of the individual blockchain's block that is introduced. When all the node come to an agreement or consensus that history and signature of the transaction is valid then that new particular block is then added to chain of the transaction [2]. If a majority of nodes does not agree to the integration in ledger ingression then block is not added to chain.This kind of working allows this blockchain methodology to run without any need of central authority. In blockchain each block contain number of transactions. It provides a decentralized, immutable data store that can be used across a network of users, engenders assets and acts as a shared ebony book that records all transactions.So, a blockchain establishes an auditable and indisputable open record of information that is cheaper, faster and more secure than any other centralized system.

## II. RELATED WORK

The following research articles are selected for review:

Akhil Tandulwadikar, has researched on Blockchain in banking and has given anatomy of blockchain transaction.He has given use of smart contract in finance. A smart contract is a computer rules of conduct meant to digitally help, (check for truth/prove true), or enforce the (back-and-forward conversation to agree on something) or conductance of a contract (agreement) [3]. For example, a borrower misses an imprest payment, the keenly intellective contract would rescind access to the digital keys as collateral. Similarly, in the case of a bond transaction, this contract will monitor the transfer of ownership from buyer to seller and release funds to the seller when transfer is finalized [4].

Xiwei Xu and Vincent Gramoli has concluded that cryptocurrencies are low-cost and basically and mostly independent of any (controlled by one central place) authority to move (from one place to another) virtual money or issue new units of money. New units of money are issued by the users of the cryptocurrency through mining. The virtual money can be moved (from one place to another) among peer-to-(person who is in a similar age group or academic field) users without going through a trusted authority to buy products (that are bought and sold) and services in real world.Bitcoin is the first and most widely used cryptocurrency [5].

Quoc Khanh Nguyen has introduced the advantages and of blockchain like Blockchain promotes keenly intellective contracts, which increases the efficiency of transactions and fees payment in the stock market.But also has drawbacks such as it limits the

competitiveness between banks to improve their own system as blockchain network will be shared among all banks participated in the system [6].And incompleteness in terms of legal and regulation on Bitcoin and cryptocurrencies prevents Blockchain technology from being widely applied. This makes this technology to make a breakthrough in the payment industry [7].

Tong Wu & Xiubo Liang has proposed the typical architecture of blockchain application consists of the application layer, the interface layer, the shared protocol layer, and the shared data layer. The hierarchical characteristics of the blockchain application and the traditional application are very different.There is also mention of Xswap which is fully self-developed and order-driven credit matching trading system which is launched by the China Foreign Exchange Trade System (CFETS). The system can automatically refresh the hidden orders and bypass orders, it even provide each participating institution with real-time, optimum and tradeable market quotations [8].

Chris Huls have worked on uses of blockchain in banking and gave major application of this technology in finance which are:

- Reduction of fraud in bank: Banks currently uses centralized database.Due to this, system is more vulnerable hackers and cyber-attacks as all the information is located in one place.
- KYC: The KYC(know your customer)will be stored in blockchain so whenever other bank need to verify new customer that bank can directly see that KYC

## III. PROPOSED WORK

### 3.1 User module

- User create new saving account/current account.
- User can see his past transaction and account details.
- User can request bank transfer.
- User can request bank for various service like cheque book, credit card.
- User can add beneficiary for NEFT.

### 3.2 Admin module

- Admin can add bank branch.
- Admin can approve user account request and service request.

### 3.3 Blockchain module

- Block chain is separate independent process written in Java Micro services.
- The job of each block is to first decode the transaction then validate the check sum using hash function
- It will then verify the rules define at respective nodes if checksum is matched
- Then it will recalculate the checksum and passes the transaction to next step
- If invalid checksum or rules it will terminate the transaction with suitable error code.

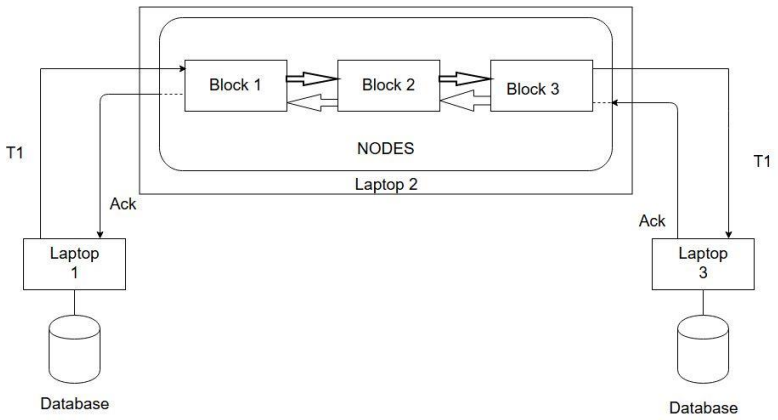


Figure 1.Blockdiagram
Here, T1=transaction

**3.4 Security module**:

There are three security models implemented in the proposed protype.

- Login module security using particular session validation ex JsessionId
- There will OTP generation in case of Beneficiary add and NEFT transaction
- There will be checksum encoding for every transaction to make sure transaction is safe over network.

**3.5 Cryptographic hash function**:

A hash function maps random size inputs or messages to fixed size hash values or tags. In order to give a good reason for the realness of a message through its tag, a hash function tries to secure/make sure of pseudo one-way ness, that is, the practical infeasibility of creating the input message given the tag, and pseudo crash resistance, it means that no two block can produce same hash value. Due to these two properties of (related to secret computer codes) hash functions, it is most secure function and also made sure that if somehow two value is produced or hash value got tampered, block's hash value will not match with the original tag, and so, the tampering will be obvious [10]. In fact, for minor differences in the input message, the tag created by a (related to secret computer codes) hash function is supposed to show major (random) difference. This allows us to use hash functions for creating tamper obvious structures.

## IV. DISCUSSION

By real life implementation of proposed system there are several major significance of it.

- Blockchain promotes keenly intellective contracts, which increases the efficiency of trade and fees payment in the stock exchange.
- Fees for foreign exchange transactions, remittances, credit card transactions and other products can be reduced substantially. Specifically, it is estimated that $16 billion will be saved annually, equally one third of transaction fees. Capital requirements for banks can be reduced by $120 billion [11]. Costs for remittances will fall approximately 1% compared to the global average of the "traditional channels" of 7.7%. (Demos, 2016) Recently, Blockchain intermediaries have been providing excellent Bitcoin transaction service in those countries like Kenya and the Philippines.
- The fact that information is automatically recorded and monitored during the transaction process makes the destination and purpose of the money transferred more transparent, which supports the fight against financial crime such as money laundering [12].
- The digitization and verification of records not only reduce necessary procedures and save paper but also ease the follow-up process of trade agreements. It also ensures that financial transactions are better protected while banks and regulatory bodies would be able to keep track of customers more easily.
- There are also cut-throat competitions from mobile payment systems, for instance, the dominance of giants like Apple Pay, PayPal, and Google Wallet [7].
- Reduction of settlement time in very few seconds by removing intermediaries.
- Replacement of trusted third parties with access by all participants in the value chain to cloud-based assets that verify each party's identity [13].
- Significant security enhancement in areas such as payments and credit card fraud through a decentralized public transaction record that stores details of every transaction and under¬goes continuous verification by miners.

## V. CONCLUSION

Blockchain is a fundamental information technology for secure value transfer over networks.Many new application areas are possible both finance and outside. In brief, the advent of new digital technology has been weakening the intermediary role of banks. Blockchain has indicates that it is the technology of trust, allowing different people and organization to cooperate and create shared values. The application of blockchain opens up a new era with tremendous opportunities, where the nature of business and competition will need to be changed within the framework of cooperation to coexist [7]. A variety of blockchain systems have emerged, though it is still too early in the innovation and development cycle to determine which of these systems, if any, will become sustainable, scalable and successful in the future. We can, assume continued experimentation by technology companies, financial services firms, and other key players in the space going forward as they work to make an effective, secure, and viable real-world blockchain ecosystem a reality. Using the proposed system we can overcome issues in current system.The system provides proper security, regulation and reduces the manual work and make transaction expeditious.

## VI. REFERENCES


**[1]** https://www.quora.com/What-is-block-chain-technology-could-you-explain-it-in-an-easy-way?redirected_qid=6512211H

**[2]** https://blockgeeks.com/guides/blockchain-scalability/

**[3]** https://en.wikipedia.org/wiki/Smart_contract

**[4]** Akhil Tandulwadikar," Blockchain in banking: A measured Approach", April 2016.

**[5]** Xiwei Xu,Cesare Pautasso,Liming Zhu,Alexander Ponomarev,Vincent Gramoli," The Blockchain as a Software Connector", 05 April 2016.

**[6]** https://rbi.org.in/scripts/AnnualReportPublications.aspx?Id=333

**[7]** Quoc Khanh Nguyen," Blockchain–AFinancial Technology for Future Sustainable Development", 25 November 2016.

**[8]** Tong Wu & Xiubo Liang," Exploration and Practice of Inter-bank Application Based on Blockchain"25 Auguest 2017.

**[9]** Chris Huls," Four Blockchain Use Cases for Banks (white paper)", Fintech PVT LTD.

**[10]** https://indiatechlaw.com/wpcontent/uploads/2017/White-Paper-on-Blockchain-TechnologyIDRBT.compressed.pdf

**[11]** https://www.lusakatimes.com/2012/01/24/government-ups-minimum-capital-requirements-banks-k12-billion-k104-billion/

**[12]** https://www.globalbankingandfinance.com/eu-strengthens-its-arsenal-in-fight-against-financial-crime-with-5th-anti-money-laundering- directive/

**[13]** https://www.linkedin.com/pulse/blockchain-technology-platforms-frameworks-shiv-kumar-bhasin