# Blockchain-Based Trusted and Transparent Financial Transaction System in the Public Sector

Abhishek Gandhi[1], Mayur Dahake[2], Dhiraj Gadekar[3], Abhishek Bondage[4]

[1]*Abhishek Gandhi Computer Engineering JSPM'S Imperial College of Engineering And Research, Wagholi, Pune-412207*

[2]*Mayur Dahake Computer Engineering JSPM'S Imperial College of Engineering And Research, Wagholi, Pune-412207*

[3]*Dhiraj Gadekar Computer Engineering JSPM'S Imperial College of Engineering And Research, Wagholi, Pune-412207*

[4]*Abhishek Bondage Computer Engineering JSPM'S Imperial College of Engineering And Research, Wagholi, Pune-412207*

**ABSTRACT -** The Blockchain is a trustworthy system in which a record of transactions made in bitcoin or another cryptocurrency is maintained across several computers that are linked in a peer-to-peer network. To transfer money outside to country its take three to four day to complete the process. The current banking system requires the use of multiple third-party verifications and transfer services in order to complete the transaction. There is no trust and transparency between the user and the bank system. To overcome these problems, in this paper we use Blockchain technology for faster payments than banks. Blockchain technology and distributed ledgers can decrease operational costs and bring us alongside real-time transactions between financial foundations. We use cross chain protocol for reliably exchanging information without third-party in multiple Blockchain systems.

***Keywords:***Blockchain, encryption, Mining, Peer verification, SHA Algorithm

## 1. INTRODUCTION

Nowadays we see that money transferring from one donor to some organization is a part of risk because there can take a lot of time and unacceptable risks in transferring money. They incur a lot of risk and fraud when dealing with money changers and middlemen in areas where traditional banking. This avoids local government corruption, the risk to employees carrying large amounts of cash, and easy sending of funds.

There is a lack of transparency in showing donors how donations are spent and how the act with donor regulations. So, to avoid these types of problem we made this project. [9]By Utilizing a smart system, creates transparency of records and real-time funds traceability of donations, expenses, and contracts with suppliers, eliminating the possibility of fraud and simplifying donor compliance regulations.

Commerce on the Internet has to depends almost exclusively on financial institutions serving as trusted third parties to process electronic payments[2]. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust-based model[2]. A certain percentage of a pretender is accepted as unavoidable. These costs and payment risks can be avoided in person by using natural currency, but no tool exists to make amounts over a communications channel without a granted party.

What is needed is a digital payment system based on cryptographic proof instead of trust, also have proposed a system for electronic transactions for reliably exchanging transactions without a third party in multiple Blockchains system. In this paper, we reviewed a solution to the problem using a peer-to-peer distributed timestamp server to generate computational proof of the sequential order of transactions. Quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of the same node.

## 2. SYSTEM ARCHITECTURE

Based on existing blockchain architecture, we use a new architecture called interactive blockchain architecture, as a solution to communicate different blockchains in the distributed network.

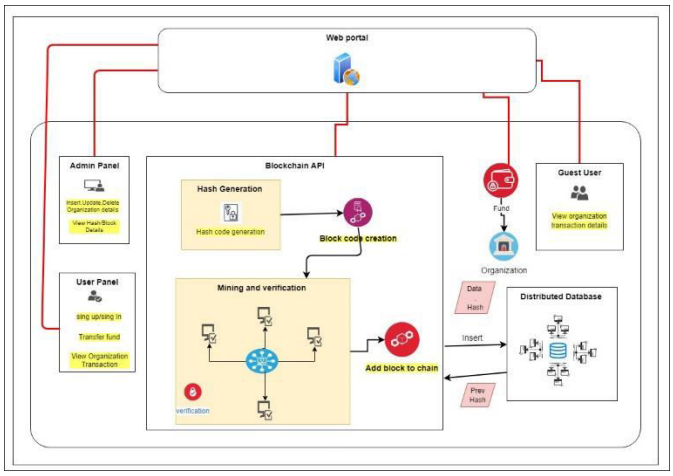


Fig 1:System Architecture

### 2.1 GUI Module:

- **Admin Panel:** In the admin panel, admin can insert, update, and delete the organization. Admin can also view generated hah code by the user.
- **User panel:**
  1. sign up or sign in via web portal.
  2. User can transfer fund to a particular organization.
  3. The user also can view organization transaction details.
- **Guest panel:** In the guest panel, public user can view the transaction received to a particular organization.

### 2.2 Blockchain API:

- **Hash Generation**:SHA-256 it is a cryptographic hash function with a digest length of 256 bits. It is used for creating256-bits unique hash code for transaction block.
- **Creating Block:** It contains a unique hash code as primary key and transaction details like fund sender, fund amount, destination organization.
- **Mining and verification:**

  1. **Mining:** It can mine the hash value to a particular format (e.g. Starting four bits are 0000).

  **2.Verification: The** generated block is distributed over the network and verifies it using the previous hash value.

### 2.3 Database Module:

- **Distributed Database:** A distributed database is located the various location in a distributed environment, in which the data can insert like a hash value, transaction details, etc and previous hash value can retrieve.

## 3. ALGORITHMS USED

**Algorithm 1: Hash Generation**

**Input:**Genesis block, data d

**Output:**Generated hash H according to given data

**Step 1:**Input data as d

**Step 2:**Apply SHA 256 from SHA family

**Step 3:**CurrentHash= SHA256(d)

**Step 4:**ReturnCurrentHash

**Algorithm 2: Protocol for Peer Verification**

**Input:**User Transaction query, Current Node Chain CNode[chain], Other Remaining Nodes blockchain NodesChain[Nodeid] [chain]

**Output:**Recover if any chain is invalid else execute the current query

**Step 1:**User generate any transaction DDL, DML or DCL query

**Step 2:** Get current server blockchain

Chain ←Cnode[Chain]

**Step 3:** For each

$$NodesChain\ [Nodeid, Chain] \sum_{i=1}^{n} (GetChain)$$

End for

**Step 4:**Foreach (read I into NodeChain)

If (!.equals NodeChain[i] with (Cchain))

Flag 1

Else Continue Commit query

**Step 5:**if (Flag == 1)

Count = SimilaryNodesBlockchian()

**Step 6:**Cacluate the majority of server

Recover invalid blockchain from the specific node

**Step 7:** Endif

End for

End for

**Algorithm 2: Mining Algorithm For Valid Hash Creation**

**Input:**Hash Validation Policy P[], Current Hash Values hash_Val

**Output:**Valid hash

**Step 1:**System generate the hash_Val for the $i^{th}$ transaction using Algorithm 1

**Step 2:**if (hash_Val.valid with P[])

Valid hash

Flag =1

**Else**

Flag=0

Mine again randomly

**Step 3:** Return valid hash when flag=1

## 4. RESULTS AND DISCUSSIONS

For the system performance evaluation, calculate the matrices for accuracy. The system is executed on java 3-tier architecture framework with INTEL 2.8 GHz i5 processor and 8 GB RAM with the distributed environment. The below figure 2 shows the time required for the number of transaction. The x-axis shows the number of transaction and Y-axis show the speed of transaction in a millisecond.

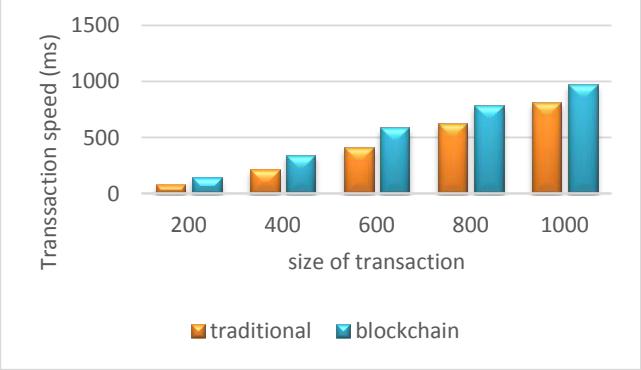


Fig2: Transaction speed (in milliseconds) for the complete transaction with different transaction records

In the second experiment, we compared the traditional (centralize) with proposed system (decentralize)transactionvalidation by consensusalgorithm in the different number of peers to peer nodes.

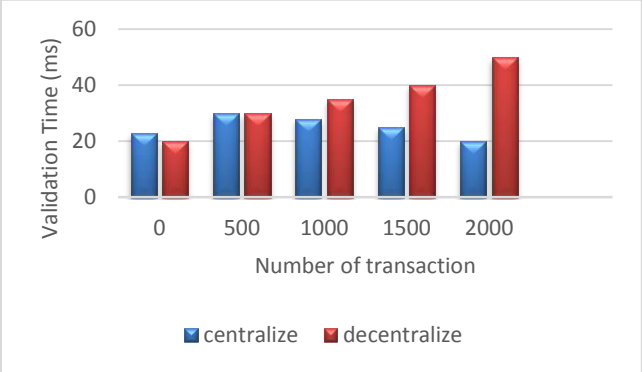


Fig3: Time required for transaction validation.

## 5. CONCLUSION

In this project, based on existing blockchain architecture we proposed a new architecture called interactive blockchain architecture as a solution to communicate different Blockchain in the distributed network for reliably exchanging information across the blockchain system. There is a problem in the traditional system of using the third-party during the transaction and different attack issues in centralized database architecture. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impossible for an intruder to change, if honest nodes control a majority of the same node and also have proposed a system for digital transactions for surely exchanging transactions without a third party in multiple Blockchains system.

## 6. FUTURE WORK

The majority of research is focusing on revealing and improving limitations of Blockchain from privacy and security perspectives, but many of the proposed solutions lack concrete evaluation on their effectiveness. Many other Blockchain scalability related challenges including throughput and latency have been left unstudied.

## 7. REFERENCES


1. Kan Luo, Wei Yu, Hafiz Muhammad Amjad, Kai Hu, Liang Chao Gao,(2018) **"**AMultiples Blockchain Architecture on Inter-Blockchain Communication".
2. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System".
3. Hope-Bailie A, Thomas S. "Interledger: Creating a Standard for Payment", International Conference Companion on World Wide Web. International World Wide Web Conferences Steering Committee, 2016:281-282.
4. Henry Robinson, "Consensus Protocols: Three-phase Commit", Henry in computer science, Distributed systems, 2008
5. Stefan Thomas, Evan Schwartz, "A Protocol for Interledger Payments".
6. Christopher Ehmke, Florian Wessling, Christoph M. Friedrich, "Proof-of-Property – A Lightweight and Scalable Blockchain Protocol" 2018 ACM/IEEE 1st International Workshop on Blockchain.
7. Aitzhan N Z, Svetinovic D. "Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams". IEEE Transactions on Dependable and Secure Computing, 2016
8. J. Warren, "Bit message: A peer-to-peer message authentication Andthe delivery system," white paper (27 November 2012).
9. http://pilot.ngoxchange.com/about
10. BitCoin White Paper | Public Key Cryptography |FinancialTransactionhttps://www.scribd.com/document/364029144/BitCoin-White-Paper
11. Hu K, Zhang T, Yang Z, "Exploring AADL Verification Tool through Model Transformation[J]", Journal of Systems Architecture, 2015,61(3–4):141-156.
12. HissuHyvarinen, Marten Risius, Gustav Friis,"A Blockchain-Based Approach Towards Overcoming Financial Fraud in Public Sector Services".
13. Wang Z, Hu K, Xu K," Structural Analysis of Network Traffic Matrix via Relaxed Principal Component Pursuit[J]", Computer Networks,2011, 56(7):2049-2067.
14. Greenspan G. "MultiChain Private Blockchain" White Paper [J]. 2015.
15. Henry Robinson,"Consensus Protocols: Three-phase Commit Henry incomputer science, Distributed systems", 2008
16. Lamport L, Shostak R, Pease M."The Byzantine Generals Problem [J],"ACM Trans on Programming Languages and Systems", 1982, 4(3):382-401
17. Castro M. Practical Byzantine fault tolerance and proactive recovery [J],"ACM Trans on Computer Systems (TOCS)", 2002, 20(4):398-461.
18. Good Governance by using Blockchain,https://www.ijresm.com/volume-1-issue-12-december-2018/