International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

Blockchain Implementation for NGO Transaction

Trupti More[1], Srushti Bhole[2], Pranav Patil[3], Prof. Madhavi S. Pandre [4]

UG Students, Department of Computer Engineering, PVPIT, Pune, India[1,2,3]

Asst. Professor, Department of Computer Engineering, PVPIT, Pune, India[4]

ABSTRACT: The Blockchain is a trustworthy digital ledger of economic transactions that can be programmedto record not just financial transactions but virtually everything of value. To transfer moneyoutside to country its take three to four day to complete the process. The current banking systemit requires the use of multiple third-party verification and transferring services in order tocomplete transaction. There is no trust and transparency between user and bank system. Toovercome these problemssystem use blockchain technology for faster payments at lower fees thanbanks. Blockchain technology and distributed ledgers can reduce operational costs and bring uscloser to real-time transactions between financial institutions. System uses cross chain protocol forreliably exchanging information without third party in a multiple Blockchain system.

KEYWORDS: Blockchain, Cross-chain, Three-Phase commit protocol, Hashing, Mining, Consensus algorithm

I.INTRODUCTION

Blockchain, the digital ledger technology that can securely maintain continuously growing listsof data records and transactions, has the power to potentially transform health care, accordingto industry experts. By simplifying and expediting the way the voting industry processesdata in such areas as revenue cycle management, health data interoperability and supply chainvalidation, blockchain has the power to dramatically reduce back-office data input and maintenancecosts and improve data accuracy and security. This scope of proposed work in belowdata-driven areas

1. Longitudinal voting records Can blockchain enable patient records to securely link and be accessible across non-affiliated provider organizations to improve care coordination?
2. Automated health claims adjudication By using a smart contract structure, can blockchain help seamlessly adjudicate payers and patients provider payments for a more cost-efficient process?
3. Interoperability can blockchain overcome current patient data interoperability issues and gather the information needed to more effectively support population health initiatives for large health systems?
4. Online patient access Will blockchain technology enable patients to more easily, effectively and securely gain access to their own medical records?
5. Supply chain management Can blockchain enhance voting contract management and reduce costs by allowing such features as real-time contract tracking and execution.

Technology has positive impacts on many aspects of our social life. Designing a 24 hour globallyconnected architecture enables ease of access to a variety of resources and services.To designand implement own SHA family block for whole block chain.The blockchain technologyis presented as a game changer for many of the existing and emerging technologies.

II.LITERATURE REVIEW

In this paper proposed an innovative component based framework for exchanginginformation across arbitrary blockchain system called interactive multipleblockchain architecture. Architecture, a dynamic network of multichain is created forinter blockchain communication. System propose the inter-block chain connection modelfor routing management and messages transferring. Additionally, our proposed protocolsprovide transactions with atomicity and consistency in crossing-chain scene. In the end,our experiment results based on a network of private multiple blockchain systems showthat the throughput is increased by a number of chains parallel running [1].

System present a protocol for payments across payment systems. It enablessecure transfers between ledgers and allows anyone with accounts on two ledgers to createa connection between them. It uses ledger provided escrow conditional

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

locking of fundsto allow secure payments through untrusted connectors. Our protocol lowers the barriersto facilitating Interledger payments. Connectors compete to provide the best rates andspeed. The protocol can scale to handle unlimited payment volume, simply by addingmore connectors and ledgers. The sender of a payment is guaranteed a cryptographicallysigned receipt from the recipient, if the payment succeeds, or else the return of theirescrowed funds [2].

Software connector helps make explicitly important architectural considerationson the resulting performance and quality attributes (for example, security, privacy,scalability and sustainability) of the system. In this paper system provide rationales to supportthe architectural decision on whether to employ a decentralized blockchain as opposed toother software solutions, like traditional shared data storage. System explore specific implicationsof using the blockchain as a software connector including design trade-offsregarding quality attributes [3].

A purely peer-to-peer version of electronic cash would allow online paymentsto be sent directly from one party to another without going through a financialinstitution. Digital signatures provide part of the solution, but the main benefits are lostif a trusted third party is still required to prevent double-spending. System propose a solution to the double-spending problem using a peer-to-peer network. The network timestampstransactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chainnot only serves as proof of the sequence of events witnessed, but proof that it came fromthe largest pool of CPU power [4].

In this paper system address the problem of providing transaction security indecentralized smart grid energy trading without reliance on trusted third parties. System haveimplemented a proof-of-concept for decentralized energy trading system using Blockchaintechnology, multi-signatures, and anonymous encrypted messaging streams, enablingpeers to anonymously negotiate energy prices and securely perform trading transactions. System conducted case studies to perform security analysis and performance evaluation withinthe context of the elicited security and privacy requirements [5].

System will introduce the Interledger Protocol (ILP), a new neutral paymentsprotocol being incubated in the Interledger Payments Community Group, also at theW3C. System will demonstrate how, in the future, the combination of the W3C's Web PaymentsAPIs and the power of ILP payments will not only be frictionless but fully integratedinto how system use the Web and ubiquitous payments in an Internet of value [6].

III.PROPOSED SYSTEM DESIGN

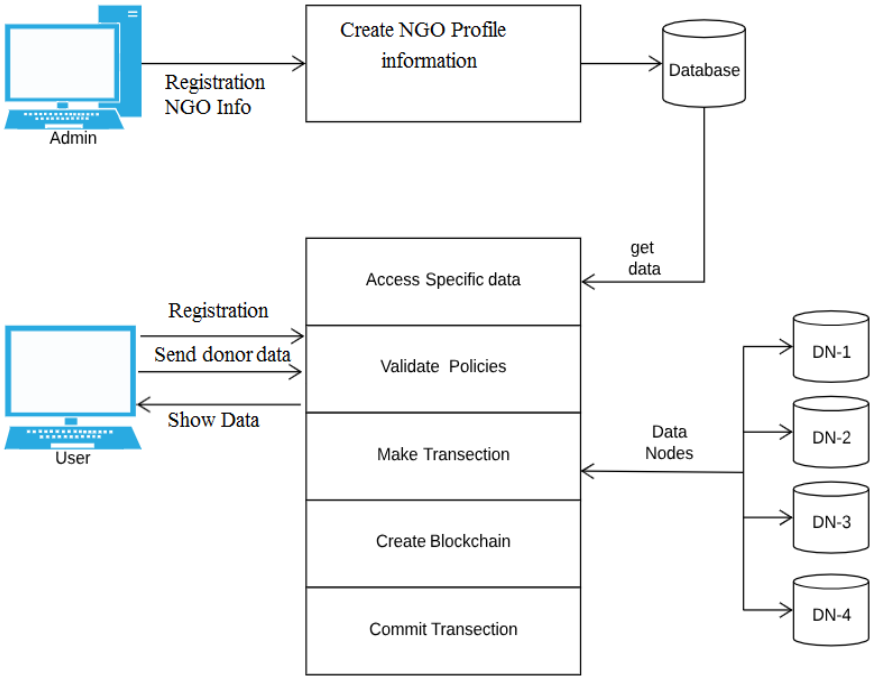

Figure 1: Proposed system architecture

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

Implementation Procedure

First we create a multiple Distributed ledger and banking system transnational data and stored all transnational data into multiple data nodes. The aach node will holds the specific block for each transaction. The same block has replace for all nodes, and generates a valid block chain.System will retrieve data from all data nodes and commit the transaction, it should be any kind of DDL, DML as well as DCL transnational query.If any block chain invalid during the validation of data servers, then system will automatically recover whole block-chain using majority of servers. Finally we will address and eliminate the run-time server attacks and recover it using own blockchain.

Algorithm Design

Algorithm 1 : Hash Generation

Input : Genesis block, Previous hash, 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 : RetrunCurrentHash

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 current query
Step 1 : User generate the any transaction DDL, DML or DCL query
Step 2 : Get current server blockchain
Cchain ←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 blockchin from specific node
Step 7: End if
End for
End for

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 ith 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

IV.RESULTS AND DISCUSSIONS

For the system performance evaluation, the system calculates the matrices for accuracy. The system is executed on java 3-tier architecture framework with INTEL 2.8 GHz i3 processor and 4 GB RAM with a distributed environment. The

below figure (b) shows the time required for a consensus algorithm to validate the blockchain in 4 nodes. The x-axis shows the size of blockchain and Y shows the time required in milliseconds for validation.

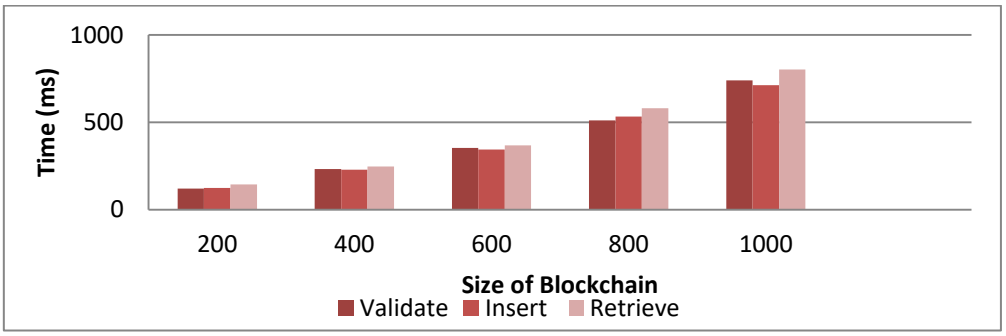

Fig. (b): Time required (in milliseconds) for complete transaction with different records blockchain using 4 data nodes in P2P Network

In another test case we evaluate the proposed system with smart contract validation by consensus algorithm in different number of peer to peer node.

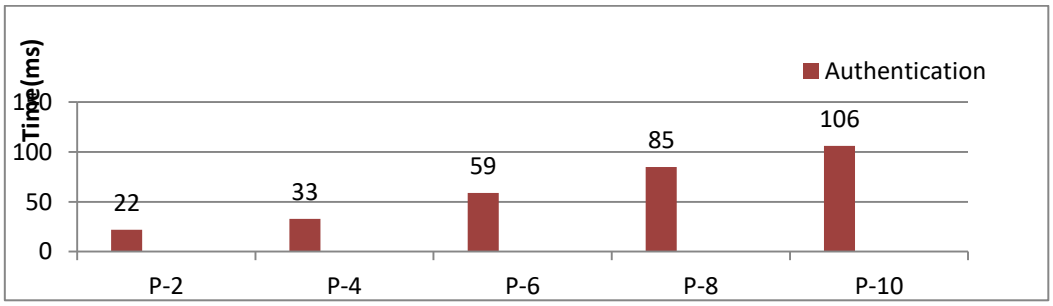

Fig. (c): Time required for smart contract validation with different no. of P2P network in blockchain.

The number of variation taken by algorithm from propose SHA value are evaluated in the third test case. Basically this has been done to evaluate the propose hash string is valid or not according to given mining policy. In many times when system generates SHA code for given transactional data its never fulfill the mining policy. To fulfill the propose mining policy according to given scenario mining to generate the multiple variation on given string. The below figure (d) shows the time required to generate the valid SHA string for specific transaction.

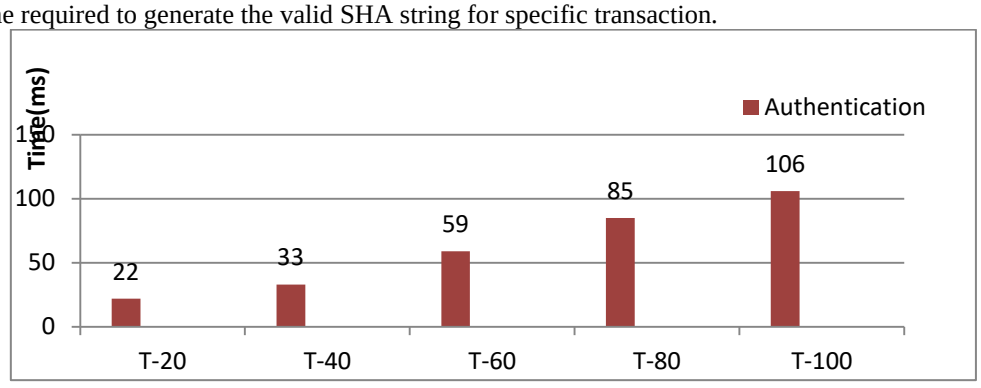

Fig. (d): Time required for mining for number of transactions in milliseconds

V.CONCLUSION

In this system we use cross chain protocol for reliably exchanging information without thirdpartyin a multiple Blockchain systems. In our proposed system, three-phase commit is used
for confirming the communication result. Guarantee transfer of crossing-chain transactions canremove the third party. Our system also provides atomicity and consistency for crossing-chaintransactions. Our future work focuses on adding

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

encryption and access control into inter-Blockchain connectionmodel, improving the security of the multiple Blockchain systems. We also need to verifyour inter-Blockchain connection model with formal methods.

REFERENCES

[1] "A Multiples Blockchain Architecture on Inter-Blockchain Communication ",1. Kan Luo, Wei Yu, Hafiz Muhammad Amjad, Kai Hu, LingChao Gao, (2018) .
[2]"Bit coin: A Peer-to-Peer Electronic Cash System",Satoshi Nakamoto
[3]"Interledger: Creating a Standard for Payment",3. Hope-Bailie A, Thomas S;International Conference Companion onWorldWideWeb. InternationalWorldWideWeb Conferences Steering Committee, 2016:281-282.
[4]"A Protocol for Interledger Payments",Stefan Thomas, Evan Schwartz
[5] "Consensus Protocols: Three-phase Commit",Henry Robinson;Henry in computer science, Distributed systems, 2008.
[6] "Proof-of-Property – A Lightweight and Scalable Blockchain Protocol",Christopher Ehmke, FlorianWessling, Christoph M. Friedrich;2018 ACM/IEEE 1st InternationalWorkshop on Blockchain.
[7]"Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams" ,Aitzhan N Z, Svetinovic D;IEEE Transactions on Dependable and Secure Computing, 2016.
[8] "Bit message: A peer-to-peer message authentication And delivery system,"8. J. Warren, white paper (27 November 2012).