IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

Financial Transaction Management for NGO using Block Chain

Nandini S[1], Chandana S[2], Charanya P M[3], Dhanya Suryamath[4], Bhavani D[5]
Assistant Professor, Department of CSE[1]
Engineering Students, Department of CSE[2,3,4,5]
SJC Institute of Technology Chickballapur, Karnataka, India

Abstract: *Non-governmental organizations or NGOs, are primarily nonprofit groups, and a large portion of them are supported by members of NGO and public donations. The credibility of an NGO is substantially enhanced and donor confidence is greatly increased by maintaining transparency regarding how donations are used. Donor organizations provide funding to non-governmental organizations(NGOs) in developing various initiatives such as economic development, women's empowerment, promoting education, responding to calamities and natural disasters. Due to some NGOs' involvement in the misuse of funds, some donor agencies cease to have faith in NGOs method of operation. This system is decentralized, not owned or operated by a single person or organization but rather shared among users. We have developed a blockchain-based Donation System capable of decentralizing the resources used by a given organization. The user may create any new organization and others will be allowed to donate money in the organization. As a result, the public become the true owners of the resources, and the charity fund system as a whole becomes more transparent. Blockchain technology and distributed ledgers can reduce operational costs and bring us closer to real-time transactions between financial institutions. System uses cross chain protocol for reliably exchanging information without third party in a multiple Blockchain system.*

Keywords: Ethereum, Distributed ledger,Smart contracts, Solidity, Security, Cryptography

I. INTRODUCTION

NGO is a nonprofit, citizen-based group that functions independently of government but may be involved in international philanthropic,developmental, or social missions.

A block chain is an electronic ledger of recordsthat is shared among all the participants. This technology addresses every transaction'sauthenticity by confirming the parties involved,the time and date of transaction as well as the contents of particular transaction.

The term "block" refers to transaction data, which is subsequently arranged in a "chain" that connects to other blocks of data forming ablockchain. This synchronized approach makesit simple to identify any changes to the chain, aiding the system's defense against unauthorized and unlawful transactions.

The Blockchain is a trustworthy digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value. To transfer money outside the country its take three to four days to complete the process. The current banking system requires the use of multiple third- party verification and transferring services in order to complete transaction. There is notrust and transparency between user andbank system. To overcome these problems system use blockchain technology for fasterpayments at lower fees than banks. Blockchain technology and distributed ledgers can reduce operational costs andbring us closer to real-time transactions between financial institutions. System uses cross chain protocol for reliably exchanging information without third party in a multipleBlockchain system.

II. LITERATURE SURVEY

Blockchain is a new technology for datasharing between untrusted peers. However, it does not work well with massive transactions. Besides, there are high barriersbetween heterogeneous blockchain systems.In this paper, we proposed an innovative component-based framework for exchanging information across arbitrary blockchain system called interactivemultiple blockchain architecture. In our architecture, a dynamic network of multi-chain is created for inter-

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

blockchain communication. We propose the inter- blockchain connection model for routing management and messages transferring.Additionally, our proposed protocols provide transactions with atomicity and consistency in crossing-chain scene. In the end, our experiment results based on a network of private multiple blockchain systems show that the throughput is increased by a number of chains parallelrunning [1].

A purely peer-to-peer version of electronic cash would allow online payments to 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 lost if a trusted third party is still required to prevent double- spending. We propose a solution to the double-spending problem using a peer-to-peer network. Thenetwork timestamps transactions 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 chain not onlyserves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attackthe network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone[2].

The expansion of blockchain technologies from financial applications to other fields intensifies the problem of an increasing size of data stored in the blockchain. Unfortunately, new participants of the blockchain network are required to download the whole blockchain to gain an overview about the state of the system and to validate incoming transactions. Approaches like IOTA, SegWit or the Lightning Network try to solve the scalability issues of blockchain applications. Unfortunately, they focus on strategies slowing down the blockchain's growth instead of reducing the problems arising from a growing chain or introduce new concepts to oust the linear blockchain altogether. The approach proposedin this paper is based on the idea of Ethereum to keepthe state of the system explicitly in the current block but further pursues this by including the relevant partof the current system state in new transactions as well.This enables other participants to validate incoming transactions without having to download the whole blockchain initially. Following this idea use cases can be supported that require scalable blockchain technology but not necessarily an indefinite and complete transaction history[3].

Smart grids equipped with bi-directional communication flow are expected to provide more sophisticated consumption monitoring andenergy trading. However, the issues related to thesecurity and privacy of consumption and tradingdata present serious challenges. In this paper we address the problem of providing transaction security in decentralized smart grid energy trading without reliance on trusted third parties. We have implemented a proof-of-concept fordecentralized energy trading system using blockchain technology, multi-signatures, and anonymous encrypted messaging streams, enabling peers to anonymously negotiate energyprices and securely perform trading transactions.We conducted case studies to perform security analysis and performance evaluation within the context of the elicited security and privacy requirements[4].

We propose a system that allows users to securely send and receive messages, and subscribe to broadcast messages, using a trustlessdecentralized peer-to-peer protocol. Users need not exchange any data beyond a relatively short (around 36 character) address to ensure security and they need not have any concept of public or private keys to use the system. It is also designedto mask non-content data, like the sender and receiver of messages, from those not involved inthe communication[5].

III. DESIGN

Fig 1 use to create a multiple Distributed ledger and banking system transnational data and stored all transnational data into multiple data nodes. The eachnode 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.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

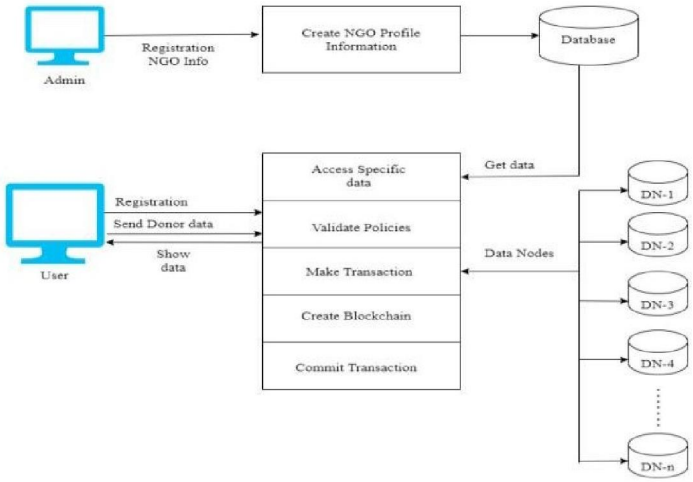

Fig 1: System Architecture

IV. METHODOLOGY

4.1 Hash Generation

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)

Step4 : Retrun CurrentHash.

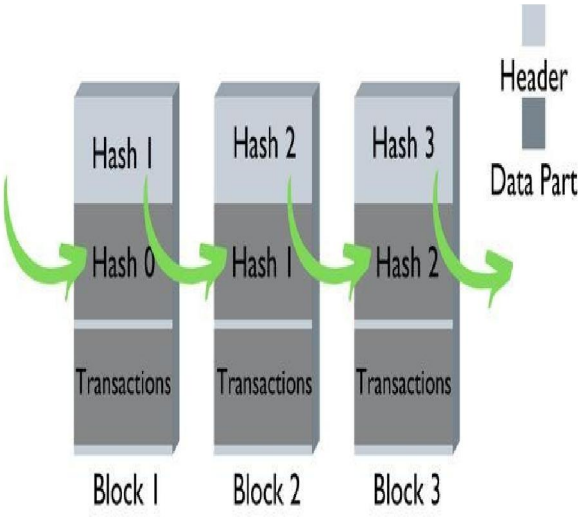

Fig 2: SHA256 Work flow

A secure hashing algorithm or commonlyreferred to as SHA-256, is an unkeyed cryptographic hashing function that takes an input of variable length and produces a 256- bit long hash output. SHA-256 is one of the first and most prominently used hashing algorithms in blockchains like Bitcoin, Bitcoin Cash, and Bitcoin SV.

SHA-256 is used in various stages ina blockchain, most prominently:

Mining: In the process of mining, SHA-256is used to create a hash of a block's header, which includes the previous block's hash, thetransaction data, and a nonce. Miners attemptto find a nonce value that, when combined with the rest of the header data, produces a hash output that meets a specific difficulty requirement.

Block validation: SHA-256 is used to verifythe integrity of a block's header. Nodes checkthat the hash of the header is less than the current difficulty target, which requires acertain number of leading zeros in the hash output. This ensures that the block has been legitimately mined and that its transactions are valid.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

Consensus mechanism: Miners calculate the hash of new blocks to be created using SHA256 by varying the value of nonce in a bitcoin block until they reach the hash belowthe threshold. Then that block can beaccepted into the ledger.
Chains of blocks: Each block in the ledger contains a hash generated by SHA-256 referring to the preceding block in the chain. **Digital signatures**: Transactions use digital signatures to maintain integrity, the information used in the transaction is hashedusing SHA-256, and then it is encrypted withthe sender's private key to generate asignature. The miner then
verifies this signature to validate the transaction.
Avalanche effect: If there is a small change in the input, the output changes dramatically. This makes sure that the hash value cannot be guessed based on the input values. This makes the hash more secure.

4.2 Protocol for Peer Verification

In this module, system verifies each and everynode which is connected in the Blockchain
using corresponding node Id.

Algorithm

Input : User Transaction Query, Current Node Chain - CNode[chain]
Remaining Nodes in blockchainNodesChain[Nodeid][chain]
Output: Recover if any chain is invalid, elseexecute the current query
Step 1: The user generates a transaction query (DDL,DML, or DCL).
Step 2: Get the current server blockchain (CChain) ofthe current node (CNode).
Step 3: For each node in the chain
// Get the blockchain of the current node (CNode) and compare it with the blockchain of the other nodes(NodesChain).
// If any node's blockchain is different from the current node's blockchain, flag it as invalid
(Flag = 1) and move on to the next node in the chain.
// If all nodes have the same blockchain as the currentnode, then continue with the query execution(Commit Query).
Step 4: If Flag == 1 (i.e., at least one node's blockchain is invalid), count the number of nodes that have a similar blockchain (Count = SimilarNodesBlockchain()).
Step 5: Calculate the majority of the servers, i.e., if the majority of nodes have the same blockchain, thenthe current node's blockchain is considered invalid, and the invalid blockchains need to be recovered.
Step 6: If the current node's blockchain is invalid, recover it by getting the valid blockchain from a specific node.
Step 7: End if.End for
End for

V. CONCLUSION

NGO is a nonprofit, citizen-based group that functions independently of government but may be involved in international philanthropic, developmental, or social missions.
In this system, we employ the cross-chain protocol to securely exchange informationacross several Blockchain systems without the involvement of a third party. Three-phase commit is employed in our suggested approach to verify the communication result. The third party may be eliminated through guarantee transfer of cross-chain transactions. Additionally, our solutionoffers atomicity and consistency for cross- chain transactions. In order to increase the security of various Blockchain systems, our future work will include encryption and access control to the inter-Blockchain connection paradigm. We also need to use formal ways to check our inter-Blockchain connection model.
For NGOs wishing to enhance their financial management procedures, putting into place a blockchain-based financial transaction management system can be a good investment. It may increase efficiency, accountability, and transparency, improving the NGO's results.

ACKNOWLEDGEMENTS:

We would like to thank SJC Institute of Technology, our college, Prof. ARAVIND TEJAS CHANDRA, our project coordinator, and Prof. Nandini S, our mentor, for providing us with the opportunity to work on this project and for

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

providing us with the direction and support we needed to make it asuccess. Additionally, we would like to express our gratitude to our colleagues for their support, fervor, and contributions to our endeavor. They are essential to our project's success.

REFERENCES

[1]. "A Multiples Blockchain Architecture on Inter- Blockchain Communication ",1. Kan Luo, Wei Yu, Hafiz Muhammad Amjad, Kai Hu, LingChao Gao, (2018) , 10.1109/QRS-C.2018.00037.

[2]. "Bit coin: A Peer-to-Peer Electronic Cash System",Satoshi Nakamoto "Interledger: Creating a Standard for Payment",3. Hope-Bailie A, Thomas S;International Conference Companion on WorldWideWeb. InternationalWorldWideWeb Conferences Steering Committee, 2016:281-282.

[3]. "A Protocol for Interledger Payments",Stefan Thomas, Evan Schwartz "Consensus Protocols: Three-phase Commit",Henry Robinson;Henry in computer science, Distributed systems, 2008.

[4]. "Proof-of-Property – A Lightweight and Scalable Blockchain Protocol",Christopher Ehmke, FlorianWessling, Christoph M. Friedrich;2018 ACM/IEEE 1st InternationalWorkshop on Blockchain.

[5]. "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, 10.1109/TDSC.2016.2616861.

[6]. "Bit message: A peer-to-peer message authentication And delivery system,"8. J. Warren, white paper (27 November 2012).

[7]. "A Deep Dive into Blockchain-based Smart Contract-specific Security Vulnerabilitie" Rohini Pise Sonali Patil 10.1109ICBDS53701.2022.99359492022

[8]. "Smart Contract Designs on Blockchain Applications" Alkhansaa Abuhashim,Chiu C. Tan 10.1109/ISCC50000.2020.9219622,2020.

[9]. "Visualization of Blockchain Consensus Degradation" Author:Luca Ambrosini,Matija Piškorec Claudio J. Tessone 10.1109/ICBC54727.2022.9805498,2022.

[10]. "A Study on Blockchain Application in Donation Platform" Author:Wooyoung Lee,Dukjin Kim, Byeong Ryun Jeon

[11]. 10.1109/SNPDWinter52325.2021.00075,2021.

[12]. "Platform for Tracking Donations of Charitable Foundations Based on Blockchain Technology" Auth:Hadi Saleh, Sergey Avdoshin,Azamat Dzhonov 10.1109/APSSE47353.2019.00031,2019.

[13]. "A Blockchain-based Material Donation Platform" Auth:Tong Li,Donghui Hu,Meng Li,Yifan Li Shuli Zheng 10.1109/ICBCTIS55569.2022.00061,2022.

[14]. "Non-Fungible Token Donation Platform Delivers Continuous Goodwill without Daunting Donor Commitment" Auth:En-Chia Chang,Nan-Ching Tai 10.1109/GCCE56475.2022.10014392,2022.

[15]. "Public Fund Care Tracking System based on Blockchain" Auth:Srishti Kumari,Tushar Dixit,Prem Prakash Vaishali Sharma 10.1109/ASIANCON55314.2022.9908651,2022.

[16]. "Decentralized Fundraising Application Using Blockchain" Auth:Rishi Dange,Aditya Sawant,Aditya Chavan Prerna Bhardwaj,Ashwini Bundele 10.1109/ICBDS53701.2022.9935998,2022.

[17]. "Aid, Charity and Donation Tracking System Using Blockchain" Auth:Aashutosh Singh,Rohan Rajak,Harsh Mistry Prachi Raut 10.1109/ICOEI48184.2020.9143001,2022.

[18]. "Smart NGO Tracking System Using Blockchain Technology" Auth:Yashwanth Kumar G N,Supreetha M 10.1109/MysuruCon55714.2022.9972465,2022.

[19]. "Developing a Reliable Service System of Charity Donation During the Covid-19 Outbreak" Auth :Hanyang Wu,Xianchen Zhu 10.1109/ACCESS.2020.3017654,2020