JCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

Funds Transfer Using Blockchain

D. Venkata Sai[1*], A. Yeshwanth Sai[2], E. Koti Reddy[3], K. Suresh Babu[4]

[1,2,3,4] Dept. of Computer Science and engineering, Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India

Corresponding Author: dasarivenkatsai@gmail.com, Tel.: +91-6301886387

DOI: https://doi.org/10.26438/ijcse/v7i3.7679 | Available online at: www.ijcseonline.org

Accepted: 07/Mar/2019, Published: 31/Mar/2019

Abstract: Even though they are many non-profit organizations, they are still viewed as for-profit organizations, as they are run with a corporate structure. Similarly, many charity organizations are being misappropriated without as there is no way for donors to know how their money is being spent. Due to this, the needy are not receiving the full welfare. With a Charity DApp on blockchain, charity organizations can collect funds. ID can be used to register donors as well as organizations. Spending of funds is made transparent through the power of blockchain.

Keywords: *blockchain, Smartcontracts, consensus, Dapp.*

I. INTRODUCTION

Block chain is distributed, decentralized public ledger used to store the transactions that are made on peer to peer network. A data storage unit with a time stamp is a block is linked with the previous block in the block chain in chronological order. Each block consists of block header and block body. The block header consists of block sequence number, time stamp, block size and a hash value of the previous block. Block body consist of transaction counter, transactions. The storage and transmission of data in the block chain no longer dependent on central nodes, but the data is transmitted freely between communication nodes according to consensus mechanisms. Using asymmetric encryption technology, the transaction data stored in block can be tamper proof[1].

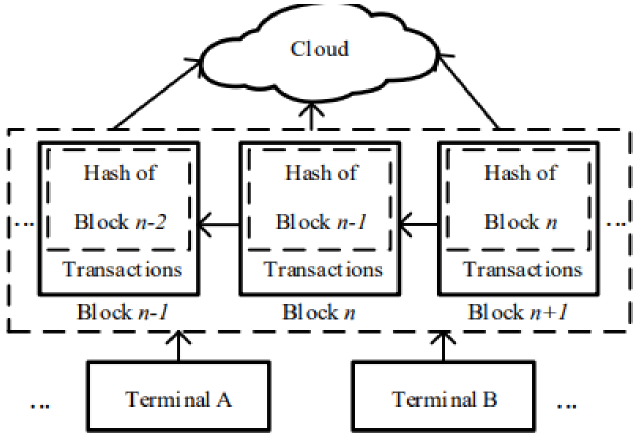


Fig 1: system structure

II. CATEGORIES IN BLOCKCHAIN

For the first categorisation we have:

- In permissionless blockchains, anyone can participate in the verification process, i.e. no authorisation is required to participate in the verification process and a user can contribute his/her computational power, usually in return for a monetary reward.
- Permissioned blockchains, where verification nodes are preselected by a central authority or consortium.

For the second categorisation we have:

- In Public blockchains anyone can read and submit transactions to the blockchain.
- In Private blockchains, permission is restricted to users within an organisation or group of organisations.

2.1 Permissionless blockchain or public blockchain:

In permissionless blockchain every user is allowed to create his own address and begin to interact with the network, by submitting transactions and adding entries to the ledger. Any node in the network can employ the mining protocols to verify the transactions by mining operations, in exchange for mining fees and block rewards. Permissionless blockchain uses proof of work where mining is done by solving complex mathematical equations which in return validate the transactions that to be added to the ledger. Digital currencies like Ethereum, the blockchain network also support smart contracts, which are automated transactions that self-execute when some criteria are met [1].

2.2 Permissioned Blockchain:

Permissioned blockchains are like a closed ecosystem, where users are not freely able to join the network, see the recorded history, or issue transactions of their own. Permissioned blockchains are preferred by centralized organizations, which leverage the power of the network for their own, internal business operations. Permissioned blockchains have a set of trusted parties to carry out verification, and additional verifiers can be added with the agreement of the current members or a central authority. Permissioned blockchains are intended to compatibility with existing applications. They can be fully private or consortium blockchains. Because the actors on the network are named, the intention is that they are also legally accountable for their activity. An advantage of a permissioned blockchain is scalability. In a permissioless block chain, each node verifies all the transactions and the data is stored on every computer in the network. It is sure that once the number of transactions increases substantially, the users that are able to perform this processing and verification will decrease, resulting in more centralisation. In a permissioned blockchain, only a smaller number of selected participants as miners, and in large institutions, they will be able to scale their computing power to meet the increase in the number of transactions. As there will be preselected participants it will be easy to alter the results and can reject the transaction easily [2].

III. SMART CONTRACTS

A smart contract is a type of agreement that uses blockchain to automatically and securely execute obligations when certain conditions are met. Like other blockchain-based technologies, the smart contract is designed to function unlike a centralised authority. A smart contract is both self-executing and self-enforcing. Smart contracts operate on straight forward 'if this, then that' Boolean logic. In this approach, an asset or currency is transferred into a program and program runs this code to validate automatically to determine whether the asset should go to one person or back to the other person or be refunded. Ethereum is a platform for deployment of internet services, for which the smart contracts are building blocks [2][3].

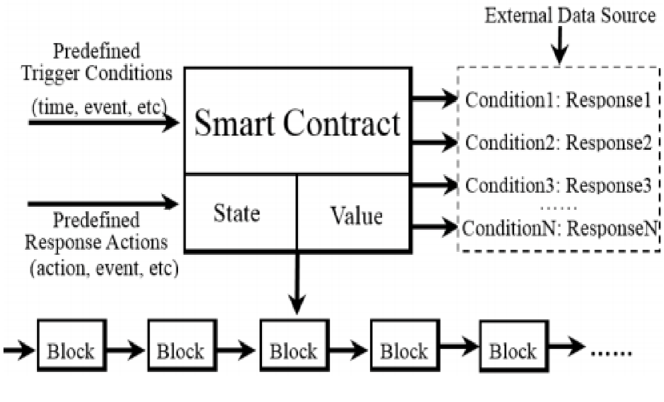


Fig.2 Blockchain-enabled smart contracts[4].

IV. CONSENSUS MECHANISMS

Different consensus mechanisms are developed for blockchain like "proof-of-work" or "proof-of-stake". Depending on the consensus mechanism, there can be different notions of when a transaction is taken to be committed or confirmed and thus immutable.

4.1 Proof of work: Proof of work an expensive problem has to be solved by a miner which needs large computational power. A cryptocurrency is given to the first miner who solves each blocks problem. Network miners compete to be the first to find a solution for the mathematical problem [5].

4.2 Proof of stake: In proof of stake the creator of a new block is chosen in a deterministic way, depending on its wealth defined as stake. The pos system there is no block reward, the miners take the transaction fees [5].

4.3 Delegated Proof of Stake*:* In the blockchain with DPoS, each node can select the witnesses based on its stake. In the whole network, the top *N* witnesses that have participated in the campaign and got the most votes have the accounting right. The number *N* of witnesses is defined such that at least 50% of voting stakeholders believe there is sufficient decentralization**.** The elected witnesses create new blocks one by one as assigned and get some rewards. The witnesses need to ensure adequate online time. If a witness is unable to create its assigned block, the activity of that block will be moved to the next block and the stakeholders will vote for a new witness to replace it.

4.4 Practical Byzantine Fault Tolerance:
In PBFT(Practical Byzantine Fault Tolerance) system **[6]** the algorithm complexity was reduced to a polynomial level, which greatly improved efficiency. There are five stages in PBFT

1) Request*:* The client sends a request to the master server node, the master node gives the request timestamp.

2) Pre-prepare: The master server node records the request message and gives it an order number. Then the master node broadcasts a pre-prepared message to the other following server nodes. The other server nodes initially determine whether to accept the request or not.

3) Prepare*:* If a server node chooses to accept the request, it broadcasts a prepare message to all the other server nodes and receives the prepare messages from the other nodes. After having collected 2*f*+1 messages, if a majority of nodes choose to accept the request, then it will enter the commit state.

4) Commit*: Each* node in a commit state sends a commit message to all the other nodes in the server. At the same time, if a server node receives 2*f*+1 commit messages, it could believe that most nodes reach a consensus to accept the request. Then the node executes the instructions in the request message.

5) Reply*:* the server nodes reply to the client. If the client does not receive a reply because of the network delay, the request is resent to the server nodes. If the request has been executed, the server nodes only need to send the reply message repeatedly[2].

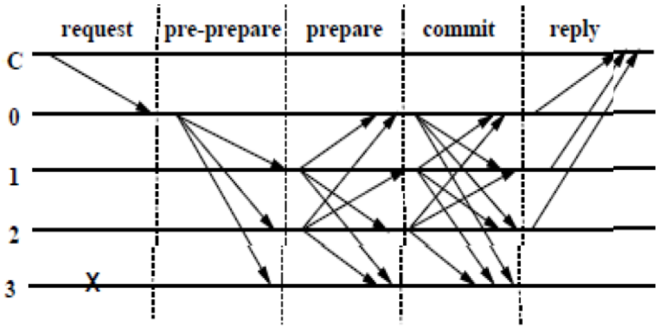


Fig. 3 Steps of PBFT[6]

V. BLOCKCHAIN ARCHITECTURE

5.1 Block

The sequence of blocks together forms a blockchain, which holds a complete list of transaction records like a conventional public ledger. A block contains one parent block, with the block hash contained in the block header. The first block in the blockchain is called genesis block.

- **Block:** Single block contains the block header and block body
  Block header contains the following.
- **Block version**: The block version in a block indicates which set of block validation rules to follow.
- **Merkle tree root hash**: the hash value of all the transactions in the block is called Merkle tree root hash.
- **Timestamp:** current time in seconds in the universal time since January 1, 1970.
- **nbit**: target threshold of a valid block hash is represented in n bits.
- **Nonce**: Nonce is a 4-byte field, which usually starts with 0 and increases for every hash calculation.
- **Parent block hash:** 256-bit hashes value those points to the previous block.
- **Block Body**: The block body contains transaction counter and transactions. Depending on the number of transactions and size of the transaction the size of the block is determined. Blockchain uses asymmetric key cryptography mechanisms to validate the authentication of transactions. A digital signature based on asymmetric cryptography is used in an untrustworthy environment [8].

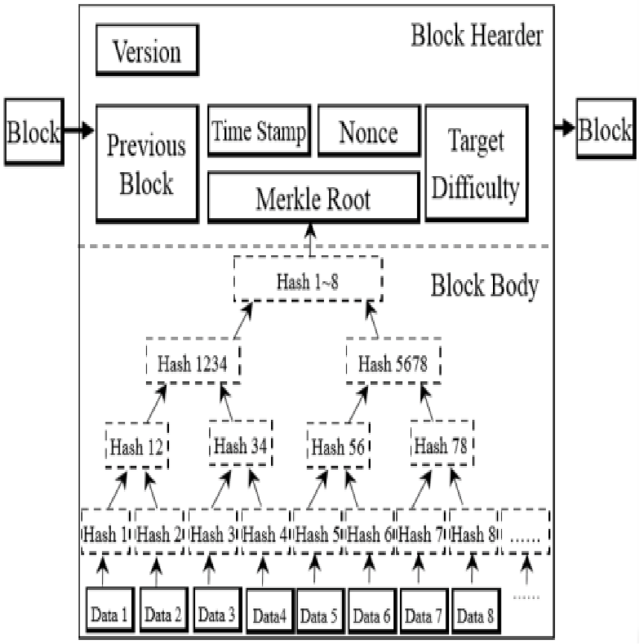


Fig Block chain Architecture[4]

5.2 Digital Signature

Each user has a pair of private key and public key.

The private key should be kept in confident which used to sign the transactions. The digital signed transactions are broadcasted throughout the whole network. The typical digital signature is used with two phases: signing phase and verification phase

5.3 Key Characteristics of Blockchain

Decentralization: Contrast to the centralized mode, the third party is no longer needed in blockchain. Consensus algorithms in blockchain are used to achieve data consistency in a distributed network.

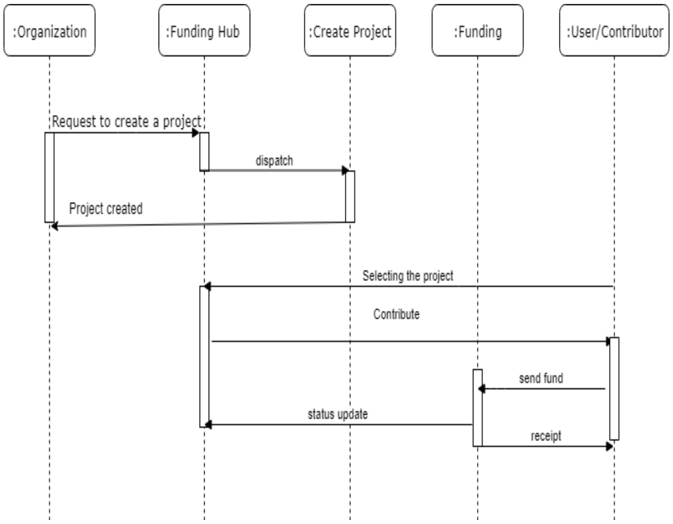
Persistency: Validity of a transaction is checked quickly and invalid transactions would not be admitted by honest miners. It is vain in money either to delete or rollback transactions once they are included in the blockchain. Blocks which contains invalid transactions could be discovered immediately.

Anonymity*:* Each user can interact with the blockchain with an address that is generated, which does not reveal the real identity of the user. The transactions in the blockchain have account addresses but not individual data by this privacy can be achieved[8][9].

Auditability*:* Bitcoin blockchain stores data about user balances based on the Unspent Transaction Output (UTXO) model **[10]**: Any transaction has to refer to some previous unspent transactions. Once the current transaction is recorded into the blockchain, the state of those referred unspent transactions changes from unspent to spent. So transactions could be easily verified and tracked[8].

VI. PROPOSED BLOCKCHAIN FUNDING SYSTEM

- The fundinghub contract used to show the projects created up to present and it's status of the projects such as the amount of fund raised, active or closed.
- Project contract contains the structure and the functions to create and give the funding stage of the project to calculate whether the funds collected to meet the requirement of the project or not with certain functions.
- Funding contract makes the fund transfer from the donor to the project.
- The organization creates the projects by making a call to fundinghub, it creates a project by a call to the project contract. After successful creation of the project, it updates to in projecthub.
- A user can view the projects from fundinghub. On selecting the project, can contribute to it by fund transferring. The status of the project fund updates.
- The Dapp follows security and privacy requirements i.e.,
  - It provides transparency and security with builds the trust and encourages to donate with precision.
  - Other people cannot obtain personally identifiable information from data in the blockchain.



VII. CONCLUSION

To solve the problem of funding fraud, this study proposed the blockchain fund transfer, which can store information about the organizational projects and the funds in blockchain network The funds spending for a project will be transparent. The Blockchain technology can ensure data integrity, the information of the funds will be stored to verify authenticity.

REFERENCES

[1]. LiuFei Chen , YuShan Li , Hong Wen , WenXin Lei , WenJing Hou ,Jie Chen Block Chain Based Secure Scheme For Mobile Communication

[2] Gareth W. Petersz ,Efstathios Panayiy Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money.

[3]. Buterin, Vitalik. 2014b. A next-generation smart contract and decentralized application platform. White Paper.

[4]. Yong Yuan, Fei-Yue Wang Blockchain and Cryptocurrencies: Model, Techniques, and Applications.

[5] Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, Chen Qijun,A Review on Consensus Algorithm of Blockchain.

[6]. M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in Symposium on Operating Systems Design and Implementation, 1999, pp. 173--186.

[7]. Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, Paul Rimba: A Taxonomy of Blockchain-Based Systems for Architecture Design Design process of Blockchain based system

[8]. Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and Huaimin Wang3 :An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends.

[9]. Harry Halpin *Inria* , Marta Piekarska *Blockstream Montral* Introduction to Security and Privacy on the Blockchain

[10] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

Authors Profile

Mr.D Venkata Sai pursing bachelor of technology in computer science and engineering from vasireddy venkatadri institute of technology, Guntur, JNTU Kakinada.

Mr.A.Yeshwanth Sai pursing bachelor of technology in computer science and engineering from vasireddy venkatadri institute of technology, Guntur, JNTU Kakinada.

.

Mr. E Koti Reddy pursing bachelor of technology in computer science and engineering from vasireddy venkatadri institute of technology, Guntur, JNTU Kakinada.

.

Mr. K Suresh Babu pursed Bachelor of Engineering from KITS, Ramtek, Nagpur University, in 1993 ,Master of Science from BITS, Pinali in year 2002, Master of Technology from JNTU College of Engineering in year 2010. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer science and engineering venkatadri institute of technology, Guntur since 2010.