Consensus Mechanism on Secure Challenges in Blockchain Networks

G. Subathra[1], Dr. A. Antonidoss[2]

[1]*Research scholar, Hindustan Institute of Technology and Science*
[2]*Associate Professor Hindustan Institute of Technology and Science*

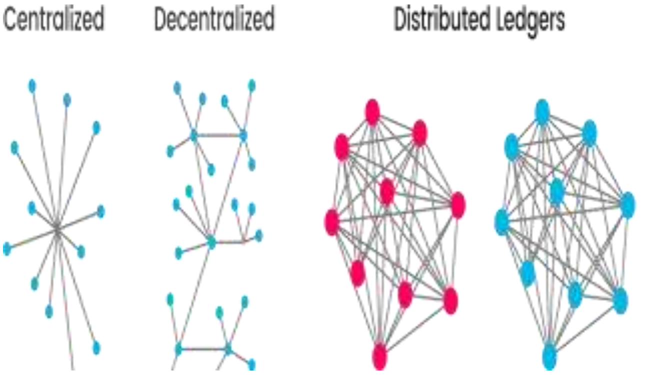
Abstract - Blockchain has recently emerged as a fascinating technology among others providing compelling features about data integrity, security, throughput. Also, a distributed database which maintains a continuously growing tamper proof data structure blocks which holds batches of individual transactions. This paper explains the concept of blockchain and how it is being implemented among various areas like cloud, big data, IOT and so on. This inherits mainly for improving security, data integrity, privacy on transactions, performance, stability, storage and so on. Although the feature of blockchain technologies may bring us more reliable and convenient services, the security issues and challenges behind this innovative technique that we need to concern.

Key Words: *blockchain, cloud computing, big data, IOT and security and privacy.*

1. INTRODUCTION

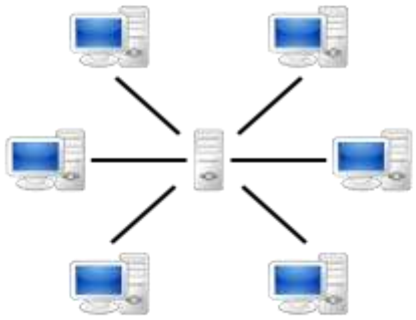
Block chain is a growing list of records called blocks which are linked and secured using cryptography. Each block typically contains a cryptography hash, a timestamp and a transaction data. A hash is a unique digital signature generated cryptography which links the two subsequent blocks to form a chain. Basically, it is a decentralized ledger used to securely exchange digital currency, perform deals and transactions.

It acts as a distributed public ledger. Each block typically contains a hash pointer which links it to a previous block, a timestamp, and transaction data. By design, blockchains are inherently resistant to modification of the data. They are typically managed by a peer-to-peer network collectively adhering to a protocol for validating new blocks.



Blockchain derives a peer to peer network

A peer-to-peer (P2P) network in which interconnected nodes ("peers") share resources amongst each other without the use of a centralized administrative system



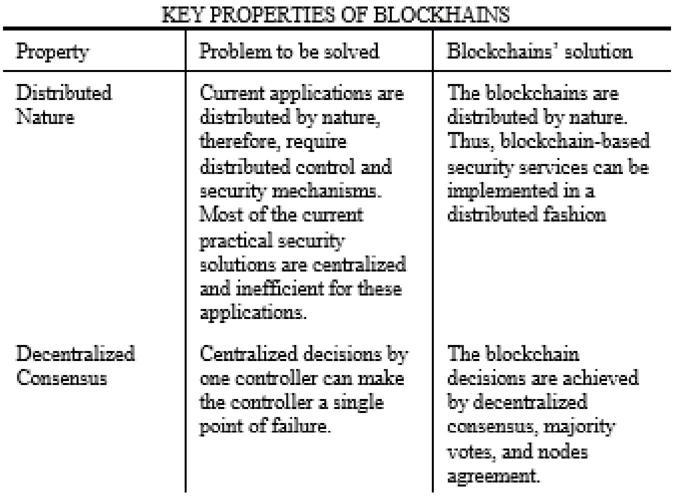
1.1 Blockchain Applications

Bitcoin is the first application of blockchain, is a digital and global money system currency. Each address has two important pieces of cryptographic information, or keys: a public one and a private one. The public key, which is what the "bitcoin address" is created from, is similar to an email address; anyone can look it up and send bitcoins to it. The private address, or private key, is similar to an email password; only with it can the owner send bitcoins from it. Because of this, it is very important that this private key is kept secret. To send bitcoins from an address, you prove to the network that you own the private key that corresponds to the address, without revealing the private key. This is done with a branch of mathematics known as public key cryptography. The blockchain gives internet users the ability to create value and authenticates digital information.

Smart contracts -Distributed ledgers enable the coding of simple contracts that will execute when specified conditions are met. Ethereum is an open source blockchain project that was built specifically to realize this possibility. Still, in early stages, Ethereum has the potential to leverage the usefulness of blockchains on a truly world-changing scale. At the technology's current level of development, smart contracts can be programmed to perform simple functions**.**

2. Properties of Blockchain

Table -1: Sample Table format



KEY PROPERTIES OF BLOCKHAINS

Property	Problem to be solved	Blockchains' solution
Distributed Nature	Current applications are distributed by nature, therefore, require distributed control and security mechanisms. Most of the current practical security solutions are centralized and inefficient for these applications.	The blockchains are distributed by nature. Thus, blockchain-based security services can be implemented in a distributed fashion
Decentralized Consensus	Centralized decisions by one controller can make the controller a single point of failure.	The blockchain decisions are achieved by decentralized consensus, majority votes, and nodes agreement.

The security issues and challenges behind the blockchain technologies that brings us more reliable and convenient services. This discuss about the different applications in blockchain and the services they offer to overcome the challenges. The applications that involves in this technology are digital currency: bitcoin, smart contracts: Ethereum, Hyperledger so on. the security issues and challenges that deals with are fork problems, majority attack occur in mining process, scalability on blockchain, cost problem. Finally, it concludes that blockchain is a hot trend which improves and overcomes current issue by implementing with its technologies and prevents impact to current systems.

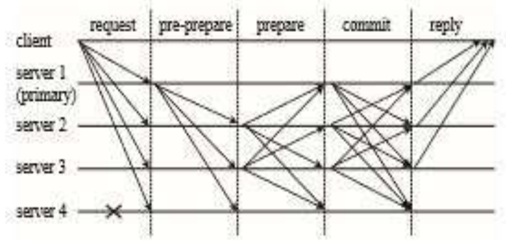


Chart -1: Operations on consensus Algorithm

The primary node sends the pre-prepare messages to everyone in the network, all nodes except for the one who drops out reply the message to primary node. The message will be like signatures, sequence number etc. The node accepts the pre-prepare message, it follows up sending the prepare messages to everyone on the network, which shows the nodes are in prepared state.

Then the receiving nodes with prepare messages sends a commit request to everyone which expects f+1 reply message where f indicates byzantine faults. if client receives the same f+1 reply then it considered being a valid and finally it indicates the correct response for the request.

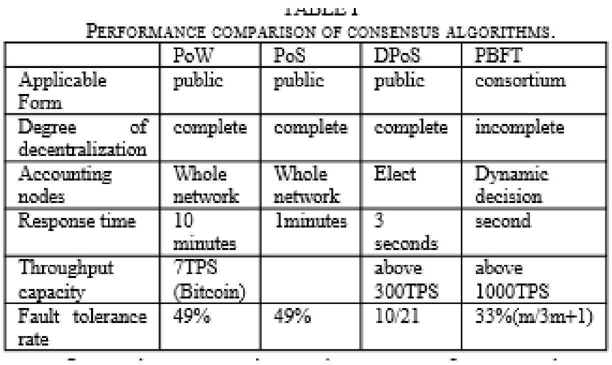


TABLE I

PERFORMANCE COMPARISON OF CONSENSUS ALGORITHMS.

	PoW	PoS	DPoS	PBFT
Applicable Form	public	public	public	consortium
Degree of decentralization	complete	complete	complete	incomplete
Accounting nodes	Whole network	Whole network	Elect	Dynamic decision
Response time	10 minutes	1minutes	3 seconds	second
Throughput capacity	7TPS (Bitcoin)		above 300TPS	above 1000TPS
Fault tolerance rate	49%	49%	10/21	33%(m/3m+1)

Fig -1: Performance Evaluation

the reliability of the blockchain can be guaranteed by the above algorithms to a certain extent, the throughput, delay and block generation etc cannot be solved well simultaneously. In these schemes, the data security depends on computing power. So, it is difficult for consortium blockchain to be applied widely. BFT is a classical consistency algorithm for distributed systems.

3. CONCLUSION

As the core of blockchain, the consensus mechanism has been studied widely, and different consensus mechanisms are required to support the blockchain systems in different application backgrounds [21]. In consortium blockchain, the computing overhead is reduced, and the centralization trend is avoided by the consensus of PBFT effectively. However, it performs poorly in the system with a large number of nodes due to the frequent view change and huge network communication. To solve these problems, a new efficient consensus mechanism, CDBFT, based on credit evaluation, has been proposed. The simulation results show that the communication overhead and the participating probability of exception nodes are reduced greatly, and the efficiency of system is improved by credit, vote, reward and punishment mechanisms of CDPBF in the consensus process.

REFERENCES

[1] **ChainFS: Blockchain-Secured Cloud Storage** Qiwu Zou1, Yuzhe Tang1, Ju Chen1, Kai Li1, Charles A. Kamhoua2, Kevin Kwiat3, Laurent Njilla3 1 Department of EECS, Syracuse University, New York .

[2] M. Castro, B. Liskov, and M. Pease, “Practical Byzantine fault tolerance and proactive recovery,” ACM Trans. Comput. Syst,, vol. 20, pp. 398461, 2002.

[3] M. J. Fischer, N. A. Lynch, and M. S. Paterson, “Impossibility of distributed consensus with one faulty process,” J. of the ACM, vol. 32, pp. 374-382, 1985. K. Elissa, “Title of paper if known,” unpublished.

[4] D. Larime, “Delegated Proof-of-Stake (DPOS),” Bitshare whitepaper, 2014.

[5] Bitcoin. https://bitcoin.org/en/.

[6] J. C. Cheng, N. Y. Lee, C. Chi and Y. H. Chen, "Blockchain and smart contract for digital certificate," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, Japan, 2018, pp. 1046-105

[7] S. Almajali, H. B. Salameh, M. Ayyash and H. Elgala, "A framework for efficient and secured mobility of IoT devices in mobile edge computing," 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), Barcelona, 2018, pp. 58-62.

[8] Zhou, L. Wang, Y. Sun and P. Lv, "BeeKeeper: A Blockchainbased IoT System with Secure Storage and Homomorphic Computation," in IEEE Access.

[9] M. Singh, A. Singh and S. Kim, "Blockchain: A game changer for securing IoT data," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 51-55.

BIOGRAPHIES

Ms. G. Subathra, is a research scholar of Hindustan Institute of Technology and Science, Chennai. She is pursuing Ph.D in the area of Blockchain

Dr. A. Antonidoss currently working as Associate Professor in Hindustan Institute of Technology and Science, Chennai. His areas of interest are Cloud Computing and Data Mining.