International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 02 | Feb 2020 www.irjet.net p-ISSN: 2395-0072

Study of Blockchain and its Concepts

Rohini Pise[1], Monika Hajgude[2], Vaishnavi Swami[3], Swamini Godse[4], Kaveri Thombare[5]

[1,2,3,4,5]*Professor, Dept. of IT Engineering, Pimpri Chincwad College of Engineering, Maharashtra, India*

Abstract - *A major advantage of blockchain technology is its distributed nature. It is seen in traditional system at the time of audit some kind of tampering may happen to the transactions stored in the system. The proposed system will be helpful for storing all kind of transactions that are happening in the organization. By storing the transaction we will be able to ensure that no tampering on the data can be done by the related person. Requester, processor, administrator, supplier. The system will be deployed on private blockchain and will be consisting of Smart contract for validating different conditions. There will be transparency in between all of the nodes as they can read all the transactions i.e. everyone will have transaction copy and hence will help for maintaining transparency.*

Key Words: blockchain, log-chain, log storage, Hyperledger, consensus algorithm.

1. INTRODUCTION

Blockchain is a technology which is distributed to store data, and it has the following properties: immutability, append only, ordered, time-stamped, open and transparent, secure, and eventually consistent. According to blockchain properties, this technology can be applied in several situations, when needing to guarantee the proof of existence, nonexistence, time order, identity, authorship, and ownership. [6]

This technology can be used to develop a system where all the records of transactions taking place in an organisation be transparent in order to avoid fraud. This technology can be implemented with the help of different concepts of blockchain viz. smart contracts, consensus, platforms like Ethereum, Hyperledger fabric. [7] Different techniques of supply chain management and storage of information will help to boost the system in terms of efficiency.

2. LOG SYSTEM

The logging system records the logs generated by the software so that the administrator can handle the problems that occur. However, the traditional log system is not secure enough and the stored logs are easily falsified. As a decentralized distributed storage technology, the blockchain can ensure that the blockchain network works normally in the presence of a few malicious nodes or failed nodes. So we use the blockchain to store the logs, which improves the security of the log system.[1]

The proposed log system mainly includes three parts: log collection, log storage, and log query. The log collection is composed of multiple log collection units. Each collection unit can passively receive log information sent by the server node, and can also actively collect log information generated by the server.[8] The collecting unit filters the collected log data according to the customized rules, perform format conversion on the logs obtained by the screening, converts different types of logs on different software into a unified log format, and finally sends them to an arbitrary blockchain node.[7] The blockchain node that receives the log encapsulates the log into a standard transaction and sends it to all the accounting nodes. The accounting node collects these transactions and stores them in the generated blocks through the consensus process transaction, thereby completing the storage of the logs. [4]Since the blockchain is a decentralized distributed data storage system, each node holds the complete data in the blockchain, so any node in the blockchain can provide log query services.

2.1 Logchain as Service

LCaaS is a hierarchical blockchain framework, graphically shown in Figure 1. The figure depicts a two-level hierarchy, but the number of levels can be increased if a use-case requires it. Current blockchain consensus protocols require every Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit the use of hard returns to only one return at the node of the network to process every block of the blockchain, hence a major scalability limitation. We overcome this limitation by segmenting a portion of a blockchain and locking-it-down in a block of a higher-level blockchain, i.e., we create a two level hierarchy of blockchains. Validating the integrity of a high-level block, confirms the integrity of all the blocks of the lower-level blockchain and leads to reduction of the number of operations needed to validate the chain

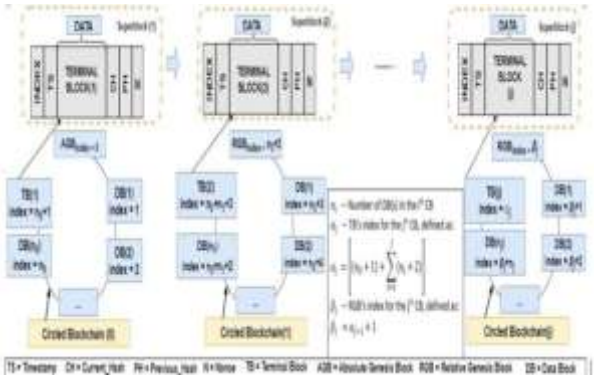

Fig-1 Super Blockchain[3]

2.2 Medusa

It is a Blockchain Powered Log Storage System. In this section, we illustrate the design of a web log storage system based on HyperLedger. HyperLedger yields higher throughput and lower latency compared with other blockchain systems. Alongside its efficiency advantages, HyperLedger is a permissioned blockchain, which is an ideal fit for enterprise software design scenario .Medusa yields good performance in low latency and non-real time batch processing scenarios. Medusa takes advantage of the smart contract functionality of HyperLedger.It is easy to deploy and use for end users.[2]

3. PLATFORMS USED FOR BLOCKCHAIN

There are many different platforms available for implementing blockchain like Hyperledger, Etherum, Corda.

This section gives a brief study of Hyperledger Fabric.When compared and studied available platforms for blockchain and smart contract Hyperledger Fabric is considered more suitable and efficient platform for implementing permissioned blockchain. It is an open source project hosted by Linux Foundation. It is basically divided in modules and is extensible in nature. It is the first blockchain system that runs distributed applications written in general purpose programming language. It's systemic working does not depend on any kind of cryptocurrency.

Hyperledger divides the transaction flow in three steps:

Executing transaction, that is checking its correctness, second ordering through consensus protocol and third transaction validation per application specific trust validation.

It combines two approaches of execution:

Active: Where set of peers execute a single transaction, this promotes parallel transaction execution.

Passive: In this type, active approach is only implemented if all peers agree to the consensus algorithm in total order among them.

There are two parts in distributed application of fabrics:

Smart contract: It is actually the immutable program code that implements the application logic and runs during the execution phase.

Endorsement policy that is evaluated in the validation phase. Endorsement policies cannot be chosen or modified by untrusted application developers.

The fig 2 shows the execute order and validate architecture of the fabric.

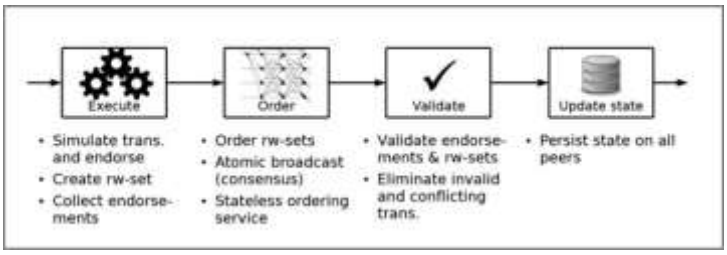

Fig-2 Architecture of Fabric[9]

Fabric network nodes has one of these 3 roles:

Clients: They submit transaction proposals for execution Peers: Execute transaction proposals and validate transactions

Ordering service: They establishes the total order of all transactions The phases and transaction flow in network is as follows:

Execution phase: In the execution phase, signing of proposal takes place by client. The simulation of proposal takes place by executing the operation on the specified Smart Contract, which has been installed on the blockchain.

Ordering Phase: Order is established for all submitted transactions per channel. Here consensus on transactions are established.

Validation phase: It includes parallel evaluation of endorsement policy, read and write check is done for all transactions, block is updated to locally stored ledger and the status of block is updated.

4. INTRODUCTION TO CONSENSUS ALGORITHM

Consensus algorithms are a decision-making process for a group, where each individual of the group constructs and supports the decision that works best for others. It's a form of resolution where individual needs to support the majority decision, whether they liked it or not.The key work in Blockchain is the consensus algorithm, which decides on how understanding is made between all the nodes to add a new block in the network. These Blockchain algorithms can be basically classified into two groups. One of them is proof-based consensus, in which the nodes joining the network need to proove that they are more qualified, more powerful than others, to do add the new block. The second group is voting-based consensus, in which nodes in the network interchange their results of validating a new block or a transaction, before making the final decision. These different consensus algorithms give us an idea, how nodes in the verifying network agree with each other about the ledger that they hold.

We can consider Proof-of-work protocol as an example of proof based consensus method. Proof-of-work is to reach an agreement, which requires a node to try and solve a hard, computational problem in order to verify a group of

transactions and append them as a new block to the blockchain. As an example of voting based consensus we can have, Proof of-stake protocol. In this protocol, user votes are weighted by their 'stake' i.e their share and users might be charged for faulty behavior. [12]

4.1 Proof based Consensus Modal

The basic concept of proof-based consensus algorithm is that among many nodes joining the network, the node that performs enough proof will get the right to add a new block to the chain, and also receive the reward. As mentioned, in the Blockchain network, if every node tries to broadcast their blocks containing the verified transactions, confusion could possibly arise. For example, consider a transaction 'that is verified by many nodes, who will then put it into their blocks, and broadcast to other nodes. If the communicating work would not cost at all then, this transaction could be duplicated in different blocks, which makes the ledger meaningless. Till now, many variants of proof-based consensus algorithms have been proposed, which are based on Proof-of-Work, Proof-of-Stake, their hybrid form, and other variants which are made independently from these two major ones.[12]

There are, many variants of proof-based consensus algorithms that have been proposed, which are based on Proof-of-Work, Proof-of- Stake, their hybrid form, and other variants that are produced from these two major ones.

4.2 Voting based Consensus Method

In order to execute the voting based consensus algorithm, the nodes inside the verifying network should be known and adjustable, so that they can exchange the message easier. The main difference compared to proof-based consensus algorithms, is that in this any node is often free to connect and leave from the verifying network. In this method all nodes need to verify the block or transaction to append it mutually by voting. They will communicate with others, before deciding to append their proposed blocks to their chain or not. In any of the voting based consensus, nodes need to see that there are at least *T(T is a threshold value)* nodes having the same proposed block with them which need to do the appending work. This is much similar to the method for tolerating faults used in the distributed system. Consider proof-of-stake which is a type of voting based consensus, here the nodes are validators. The validators lock up some of their coins as a stake in the network. Afterwards, the validators bet on the blocks that they feel will be added next to the chain. When the block gets added, the validators get a block reward in proportion to their stake. [12]

It can be observed that proof based consensus will prove to be helpful for private blockchain whereas voting based consensus can be useful for public blockchain.

Blockchain consensus algorithms are methods to bring equality and fairness in the online world. The agreement method used in this is called a consensus theorem.

5. APPLICATIONS OF LOG STORAGE USING BLOCKCHAIN

5.1 In the library

For storing the transactions of books i.e. requesting for the books and sending it to the administrator and finally getting books from the supplier. [7]

5.2 In organizations:

For storing all the transactions which are happening between the organizations and the clients or the supplier and organization or inter organizations is more important and it should be kept secure hence we can store all the transactions on blockchain. [6]

5.3 In medical:

For storing all the data of the patients and their med -ical related all the logs can be stored on the log chain which will be helpful for future use.

5.4Log data as adigital evidence:

We can use log data as a digital evidence at the time of audit. [4]

5.5In Cloud Storage*:*

LCaaS can act as a hierarchical ledger and a repository for all logs generated by Cloud solutions and can be accessed by all Cloud participants (namely, providers and users) to establish trust among them. Using verification services, a Cloud user can verify the logs provided by the Cloud provider against the records in the hierarchical ledger and finds out if the logs were tampered with or not.[3]

6. CONCLUSION

This study has found that the log storage can be implemented sufficiently by using the blockchain. There are different methods to implement the log storage system like using simple log system[1], by making use of log chain [3],by using hyperledger [2] So we can implement log storage system using the blockchain for log will be helpful for making the system transparent ,tamper proof and is more effective than traditional system.

7. REFERENCES

[1] Jiansen Huang, Jiyang Zhang, Hui Li,. "Blockchain Based Log System", "IEEE International Conference on Big Data (Big Data)"2018.

[2] Desheng Yang , Nian Duan, Yang Guo and Lu Zhang, "Medusa: Blockchain Powered Log Storage System",IEEE paper – 2018

[3] IEEE paper – William Pourmajidi, Andriy Miranskyy ," Logchain: Blockchain-assisted Log Storage", "NSERC Discovery" 2018

[4] Rafael Accorsi, "Log Data as Digital Evidence: What Secure Logging Protocols Have to Offer?", IEEE paper "33rd Annual IEEE International Computer Software and Applications Conference",2009

[5] Dávid János Fehér1, Barnabás Sándor2, "Log File Authentication and Storage on Blockchain Network", IEEE paper

[6] URL - https://blockgeeks.com/guides/what-is-blockchain-technology/

[7] URL- https://www.investopedia.com/terms/b/blockchain.asp

[8] Dr. Manish Kumar , Ashish Kumar Singh,dr. T V Suresh Kumar " Secure Log Storage Using Blockchain and Cloud Infrastructure" IEEE paper " 9th ICCCNT 2018 July 10-12, 2018, IISC, Bengaluru Bengaluru, India"2018

[9] Elli Androulaki, Christian Cachin,Christopher Ferris "Hyperledger Fabric:

A Distributed Operating System for Permissioned Blockchains" IEEE paper

[10] SiddharthSabadra, Chinmay Saraf "Blockchain Platforms: A Compendium" IEEE International Conference on Innovative Research and Development (ICIRD)11-12 May 2018,Bangkok Thailand.

[11] URL- https://blockgeeks.com/guides/what-is-blockchain-technology/

[12] Giang-Truong Nguyen, Kyungbaek Kim."A Survey about Consensus Algorithms Used in Blockchain", 2018.