Building a blockchain approach with hyperledger transaction flow and distributed consensus algorithms

S. Dhanalakshmi, B. G. Obula Reddy, K. Yogitha Lakshmi

Abstract: ***Blockchain is an important, emerging technology and specifying lot of possibilities, its very much trending topic in recent years. Bitcon is well known implementation of block chain technology, Bitcoin in cryptocurrency has turned the recognition of the universe towards a unique technology. Its benefit as decentralization, persistency and consistency of sharing the informations, blockchain is a distributed ledger that can record transactions efficiently verifiable and permanent way between two parties. Blockchain technologies focus on various applications perspectives and discuss the new technological challenges in confidentiality, integrity, authentication, internet of things and smart contract etc. it can be used to record the peer to peer network with public or private key pair of transactions, authors signed the transactions to be verified with key pair, save the transactions in blockchain network, once the transaction verified it cannot be altered subsequently. This paper present and focus on various techniques of hyperledger fabric systems architecture, transaction flow, membership and identity management, then understanding of hyperledger fabric with consensus algorithms. Hyperledger is one of the fastest growing open-source blockchain, it can dozens of company working together, building a blockchain fabric that can support the framework to test the interaction between application and secure blockchain networks, that require every peer to execute every transaction maintain a ledger and run consensus, does not support private blockchain and confidentiality. The first block chain systems is hyperledger fabric run on distributed applications with multiple programming language.***

Index Choice: Blockchain, Peer-to-Peer Network, Private-Public Key Pair, Hyperledger Fabric, Consensus Agorithms, Blockchain, Smart Contract

I. INTRODUCTION

Blockchain is a Singly Linked List of block, with each block containing a number of transactions. It's a decentralized and information sharing platform, not trust with multiple domains, users can be shared the block and record all the transactions, each transaction can be easily queried. block chain have been created in the process of development is bit coin, is growing list of records with linked list manners, each list in the blocks using with cryptographic functions. The cryptographic hash function contains the hash of the previous block, timestamp and transaction id, multiple authoritative domains of decentralized computation and information sharing platform to collaborate, cooperate and coordinate in decision making process, both users can share the information and also simultaneously edit the information in google documents, one problem to be raised in centralized systems for single point of failure, to load the data in google doc do not have sufficient bandwidth, not able to edit the documents. Fig.1. represents that blockchain system architecture of centralized vs decentralized vs distributed systems techniques. Each node specifying

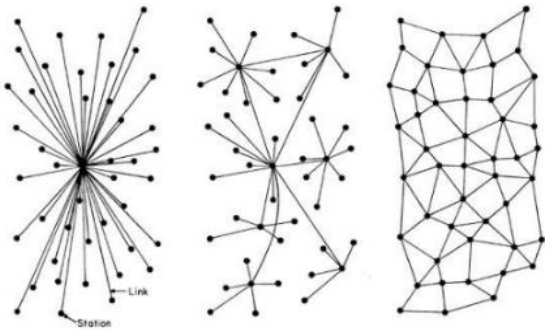

Fig.1. Centralized vs Decentralized vs Distributed Systems Architecture

A systems is centralized single point of node is not safe, The cryptographic hash function any string as input and fixed size output, secure hash algorithm that generate 256 bits in blockchain. Hash function performs the collision-free, hiding and puzzle-friendly. In cryptographic hash pointer stored hash of the information, retrieve the information and check the information, but the checked information has not been modified. In centralized systems single point is not safe vs decentralized systems can have multiple points of coordination vs distributed systems can have each one execute the job. The authentications of private-public key-pair used in transport layer security with network, the network legitimize transaction after that add transaction to blockchain. A Sequence of blocks in blockchain hold the complete record of transactions like public ledger, the integrity data written in the blockchain indicate correct and cannot be altered subsequently. Limiting to access the information in confidentiality, only authorized user can access the information that information also protected.

Its maintained distributed network of peer nodes is an immutable transaction ledger. These peer nodes perform and maintain a copy of ledger, ledger by applying transaction that have validated by consensus protocol. Private-public key pair offer a new technology is hyperledger fabric.

Revised Manuscript Received on December 28, 2018.

S.Dhanalakshmi, Professor, Department of CSE, Malla Reddy Engineering College (A),Telangana, India
B.G.Obula Reddy, Associate Professor, Department of CSE, Malla Reddy Engineering College (A),Telangana, India
K.Yogitha Lakshmi, Assistant Professor, Department of CSE, Malla Reddy Engineering College (A),Telangana, India

Its an open source distributed ledger technology platform in permissioned blockchain. Its maintains multiple organizations run on one peer or one organizations run on multiple peer, its support general purpose programming languages. The peer nodes support the notations of chaincode, users can implement a cryptocurrency through chaincode, chaincode is a smartcontract in blockchain environments.

II. DISTRIBUTED CONSENSUS MECHANISMS IN BLOCKCHAIN

Bitcoin network in permissioned blockchain, in a decentralized or distributed network, the consensus is a procedure to reach in a agreement of multi-agent in distributed or decentralized platforms, it's important for message passing environment in a distributed systems. Apply consensus in bitcoin network, traditional or conventional distributed systems to ensure reliability and fault tolerance. Distributed consensus like that decentralized environment have multiple individual parties and can take their own decision, it happened that some nodes, some parties, some individual are working maliciously or working as faulty individual. So ensure that operation, in the presence of faulty individuals to perform and develop the distributed consensus environment, the main objective is to ensure reliability. State machine replication and clock synchronization is an example of distributed consensus in bitcoin network. In state machine replication is an distributed protocol over a network, every individual nodes runs on current version of the protocol and stood the state of the protocol in different state machine, so the entire execution part of the protocol can be represented as a state machine, these state machines need to be replicated into multiple nodes, every individual node can reach to a command point or command output of that protocol. BFT (Byzantine-fault-tolerant) protocol is state machine replication protocol, it's interested in blockchain technology, then its distributes an application over many processes, faults, attacks and subset of the processes. Distributed consensus no failure in this systems, it's easy and trivial to reach in consensus, so the genetic algorithm broadcast the personal choice to all, then apply choice function, if your choice is the maximum of all the receive value, then you achieve consensus. The Fig.2. Shows that the choice functions of distributed consensus systems, the main objectives to reach maximum values for all nodes.

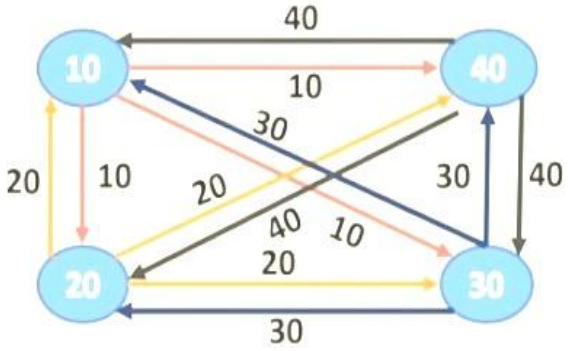

Fig.2. Choice Function in Consensus

For example here 4 individual nodes, make a choice of the individual nodes are 10, 20, 30 or 40 and informed they are individual choices to all other nodes in the network, and whenever every node receives all the choices from all the neighbours they can apply on max function then find out the maximum value, easily see that every node will reach the value of 40. If they apply the maximum function of all received values. So this architecture is easy and straight forward for this scenarios, this scenario indicate that no faultless in the system, every individual node can receive the message correctly, should not be any failure in the system. This system is called synchronous message passing systems.

In distributed consensus systems consider three different type of failures, crash fault - just like a node, so the node suddenly crashes or the nodes become unavailable in the middle of communication, you are not expected to receive any message from that particular node, network or partitioned faults - network link fails in partitioned in the network, the individual nodes are interconnected with each other, if any particular node fails in the network, the node can be specified two partition, so the entire network get partition and you are not expected to receive any message from any node of this network link failure, and byzantine fault – a node starts behaving maliciously. This mechanisms is a idealistic point-of-view, it's a decision making process for group of people involved and discussed with on decide on that value, every correct individual must agree on the same value in agreement process.

- The blockchain technology uses five most common consensus mechanisms; POW (Proof of Work –bitcoin and other blockchains), POS (Proof of Stake - peercoin), DPOS (Delegated Proof of Stake), PBFT (Practical Byzantine Fault Tolerance – used for hyperledger fabric) and DAG (Directed Acyclic Graph). Find the hash value, then the value allowed and add new block of transaction to the blockchain is POW. POS is lower energy consumption, different way to achieve and validate the transactions. DPOS is variation on POS, it's the coin holder and ownership in the network. PBFT relies that number of nodes confirm and DAG is a graph theory, it's the common sub expression in the given expression, it cannot form a cycles in graph. This DAGs transactions run on different chains simultaneously, process over 10000 transactions per second. The stable of blockchain industry is proof of work and proof of stake; these are the most prominent consensus algorithms in blockchain technology. Consensus models are primary components of distributed systems and understanding of blockchain fundamentals.

A. Byzantine Generals Problem

One of the most difficult challenges addressed by the block chain technology is Byzantine Fault Tolerance, its distributed computing systems. It may happen that the node sends different message to different peers, this general class of faults in a distributed system under closed environment, its call as a byzantine general problem or byzantine fault tolerant problem. This problem is class of failure in characteristics of systems; Fig.3. Represents that byzantine problem under multiple scenarios, this kind of problem denote that lamport timestamp.

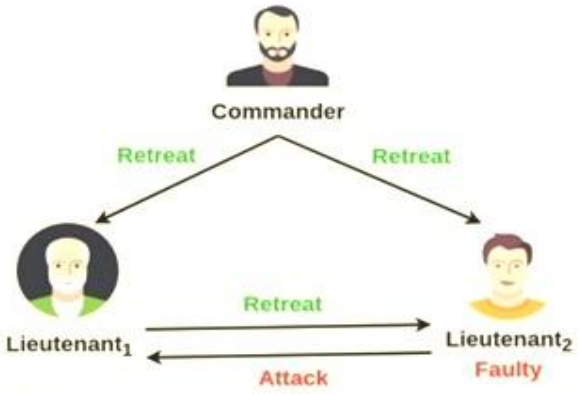

Fig.3. Multiple Scenarios of Byzantine Problem Architecture

The failure is based on imperfect information on the particular components or particular event. In byzantine architecture can have one commander and two different lieutenants, the commander send the message to the lieutenants, the lieutenant can share the messages then try to find out the commander is faulty or lieutenant is faulty. The perspective of three generals, in this case try to design a problem & also design a solution for that problem. In this architecture assume that two lieutenant, lieutenant1 is correct lieutenant and lieutenant2 is faulty lieutenant. Now if the Lieutenant is faulty,then the lieutenant may send different messages, so the commander is correct commander then send messages to both the lieutenants. Here lieutenant2 is faulty lieutenant does not obey the message to commander, the faulty lieutenant2 sends an attack message to lieutenant1. lieutenants1 is the correct lieutenant send the correct message ie., what message received from the commander side that message sent to the lieutenant2. So lieutenant1 is received two different messages from commander and lieutenant2,by integrity condition both lieutenants conclude the commanders message, this contradicts the agreement condition, but this agreement condition cannot met for the single fault occurs in the nodes. so this byzantine generals model indicate that receiver always know that the identity of sender, fully connected, synchronous systems and reliably communicate with all lieutenants.

B. Practical Byzantine Fault Tolerance Model

Practical byzantine fault tolerance consensus algorithms for ensuring the safety property then consider a complete asynchronous system or pure asynchronous systems. This algorithm is termed as practical, because it ensure safety over on asynchronous network, so this system supports byzantine failure and low overhead. The diagram Fig.4. Represents that multiple of lieutenants of distributed environment in blockchain network. Its asynchronous distributed systems, a client send a request to invoke service operation to commander/primary, commander/primary multicasts the requests to backups of all lieutenants/secondary, after receiving message from commander, the clients waits for replies different backup with the same results. all lieutenants/secondary send reply/response to client, maximum number of faulty replicas that can be tolerated.

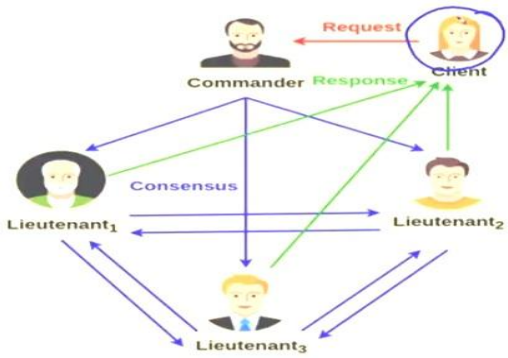

Fig.4. Multiple lieutenant of PBFT Model

It also supports privacy over the systems. it assured that the messages are tamper proof, it applies a hashing technique similar to blockchain and it also applies authentication technique through digital signature mechanism. so that none of the messages are transfer from individual nodes in the system. PBFT model well adopted in consensys for permissioned blockchain environments like hyperledger and tendermint core. Its open environment and every node meet to sense that multicast message to every other node, so the system has a high message complexity.

III. HYDERLEDGER CONCEPTS IN BLOCKCHAIN

A. System Architecture

Its a blockchain framework implementation of hyperledger projects, its open source platform for deploying and operating permissioned blockchain, running on distributed applications and support consensus protocols, first blockchain system is fabric, that run and written in generic purpose programming languages. The certificate authority provide the certificate services to the user in blockchain technology, external certificate authority services and fabric certificate services are optional and its connected between the membership services, these services relate to user transactions and secured connections between the transport layer security, The diagram Fig.5.represents that hyperledger fabric architecture building block. Membership service provider enroll the client application.

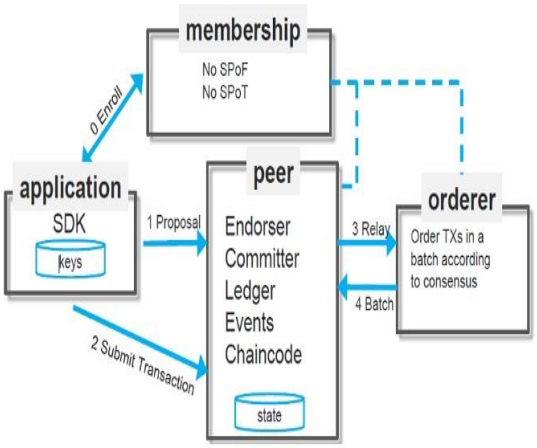

Fig.5.Building Blocks for Hyperledger Fabric Architecture

The client application connected to peer network, peer network performs the notations of endorser, committer, ledger, chaincode and events. Blockchain can have many componenets, peer is one components of blockchain,ie, in peer multiple organizations on run on one peer or one organizations run on multiple peer. Peer nodes can have two main functions of endorser (endorse proposal for transaction) and committer (block of transactions to ledger). Ledger is maintaining peer, its constructed by ordering services, its verify the history of all transactions of successful information (valid and invalid transactions information) stored on it. The ordering service is a centralized service, this service provide the delivery quarantees, shared communication channel to clients and peers, so the client connect to communication channel and broadcast message to all peers. Chaincode is the smart contract written in java, is invoked by transaction.

B. Smart Contracts in Blockchain

A self executing contract in terms of the agreement between the buyer and seller is directly written into the lines of code. It's consistent of updating the information. User can access and see the information, that information sent and stored in concept is called smart contract, which contains transactions with some conditions and rule smart contract is implemented. It's clearly defined the functions and specifies the way of work, performance of credible transactions without third parties. Smart contracts are core of blockchain technologies, its self verifying and self executing agreements and address the Contract Lifecycle Management (CLM).

C. Comparing Ethereum and Bitcoin Blockchain

Ethereum is open source,distributed computing for public blockchain based technology. It's a transaction based state transistion systems. Ethereum is similar to bitcoin but focus on smart contract in any decentralized applications, bitcoin is the peer to peer cash system in electronic format.The following Fig.6.. described that comparison of bitcoinstack and ethereum stack. The initiating transactions of bitcoin blockchain is wallet applications.

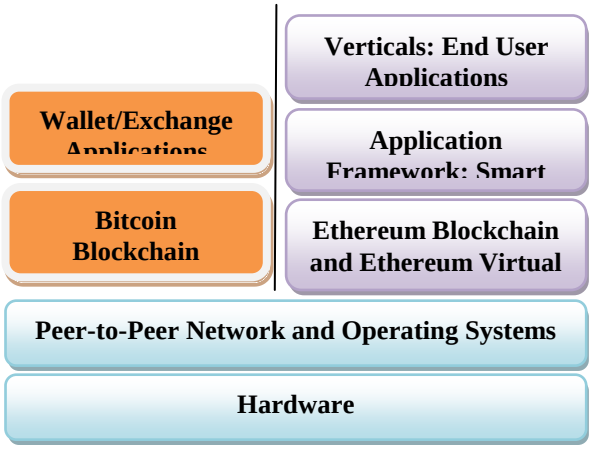

Fig.6. Overview of Bitcoin Stack with Ehereum Stack

IV. CONCLUSION

Blockchain is the context of digital currency, most prominent and emerging technology for decentralized and transactional sharing of data in large networks. Now blockchain technology currently implemented in bank sectors, industry, financial services and supply chain industry.different people use different application protocols how the transaction can be secured from other, then how to encrypt the key pair with authentication process in blockchain environments. Distributed system environements of hyperledger fabric make it highly scalable system supporting with permissioned blockchain with flexible systems. In this paper design and analyze the different consensus algorithms and hyperledger fabric technique and smart contracts problems. How the transaction to be secured from one another, then the message can be delivered in secured manner or not. The feature of blockchain technology can be extend with wide variety of areas such as security, membership access controls, research aspects, byzcoin, data analytics and artificial intelligence

REFERENCES

1. High-Performance Consensus Mechanisms for Blockchains Signe Rüsch TU Braunschweig, Germany ruesch@ibr.cs.tu-bs.de, EuroDW'18, April 23, 2018, Porto, Portugal 2018, PP 1-3, http://conferences.inf.ed.ac.uk/EuroDW2018/papers/eurodw18-Rusch.pdf
2. Ambili, KN., and Sindhu, M., and Sethumadhavan, M., On Federated and Proof Of Validation Based Consensus Algorithm In Blockchain. IOP Conference Series: Materials Science and Engineering, 2017
3. Atzei, N., Bartoletti, M., and Cimoli, T., A survey of attacks on ethereum smart contracts (sok). In International Conference on Principles of Security and Trust (2017), Springer, pp. 164-186.
4. Baliga, A., Understanding blockchain consensus models. Tech. rep., Persistent Systems Ltd, 2017.
5. Cachin, C., Architecture of the hyperledger blockchain fabric. In Workshop on Distributed Cryptocurrencies and Consensus Ledgers, (2016).
6. Imran Bashir, Mastering Blockchain, Distributed ledgers, decentralization and smart contracts explained, (2017)
7. KPMG, Consensus immutable agreement for internet of values, https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmgblockchain-consensus-mechanism.pdf
8. Mattila, J., The blockchain phenomenon. (Berkeley Roundtable of the International Economy, 2016, edn.), (2016).
9. Nakamoto, S., Bitcoin: A peer-to-peer electronic cash system, 2008.
10. Sankar, L. S., Sindhu, M., and Sethumadhavan, M., Survey of consensus protocols on blockchain applications. In Advanced Computing and Communication Systems(ICACCS), 2017 4th International Conference on (2017), IEEE, pp. 1-5. [10] Wood, G., Ethereum: A secure decentralized generalized transaction ledger. Ethereum Project Yellow Paper (2014).
11. Application of blockchain technology to banking and financial sector in India, 2017.
12. Survey on blockchain technologies and related services, Japans Ministry of Economy, Trade, and Industry (METI), 2016.
13. Blockchains & distributed ledger technologies, https://blockchainhub.net/blockchains-and-distributed-ledgertechnologies-in-general/.
14. https://arxiv.org/pdf/1801.10228 hyperledger fabric: a distributed operating system for permissioned blockchains", research paper in eurosys 2018.
15. https://blog.acolyer.org/2018/06/04/hyperledger-fabric-a-distributed-operating-system-for-permissioned-blockchains/
16. https://hyperledger-fabric.readthedocs.io/en/release-1.2/blockchain.html
17. https://blockgeeks.com/guides/blockchain-consensus/