A Survey on Blockchain Technology

Dr.Vijaya Ravichandran M.E.,Phd[1], Sathish R M.E.,(Phd)[2], Nilavann S[3], Gopi K[4]
[1, 2, 3, 4] Dept of Information Technology
[1, 2, 3, 4] KGiSL institute of Technology Coimbatore

Abstract- *Blockchain technology is gaining momentum rapidly in recent years due to its ability to make multiple parties who do not trust each other to agree upon a state with a verifiable and tamper-proof manner managed by peer-to-peer Network. As technology evolves rapidly we need to understand the core concepts in order to use Technology reliably. In this paper, we reviewing the concepts that makeup blockchain technology such as cryptography, consensus, smart contracts, and Blockchain Platforms. We then see the comparison between the different consensus algorithm, use cases of the blockchain and when to use Blockchain. We also discuss the InterPlanetary File System a protocol for peer-peer content-based addressing method for storing and sharing files and how can able to use it with the Blockchain.Keywords: Blockchain, distributed ledger technology,Blockchain consensus ,IPFS*

I. INTRODUCTION

Blockchain is the backbone Technology of CryptoCurrency such as BitCoin. The blockchain is a immutable distributed database of records of all transactions or digital event that have been executed and shared among participating parties. Now a days the blockchain technology is called as DLT (Distributed ledger technology).Simply Blockchain is an append only Data structure maintained by a network where each node in the network contains a copy of the blockchain and uses a consensus to decide which block should be accepted next.Thus in Bitcoin blockchain the system states are transaction of coins from one account to another. But blockchain can be used to store User defined state machines thus its use case grow beyond cryptocurrencies where it can be used in Finance Industries, Supply chain, Fraud detection and many other Industries.Smart contract are self executing contracts In this format, contracts could be converted to computer code, stored and replicated on the system and supervised by the network of computers that run the blockchain and change the state.The Blockchain can be permissioned network, Permissionless network, Hybrid networks.Cryptocurrencies uses a Permissionless network where anyone can join, Participate and see the transactions in the network.The permissioned network in which only the Authorized entities can participate.Hybrid network where it contains properties of both permissioned and permission less network.

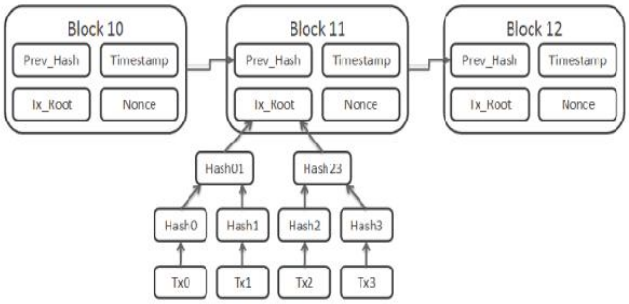

Fig.1 Blockchain structure

Table 1 Comparison between Blockchain and Traditional Database

	Blockchain	Database
Performance	slow	fast
Confidentiality	Not reliable	reliable
Immutability	Immutable records (Append only architecture)	Mutable records (Add,delete, manipulate)
Control	Centralized Control	Decentralized Control
	Master copy	Each node has a copy

II. BLOCKCHAIN NETWORKS

Blockchain Network consists of multiple nodes which do not know or trust each other and it is possible that some nodes may behave in Byzantine manner, but there must be the majority of honest nodes in order to keep safe. Thus all these nodes in the network are responsible for maintaining the global state of the records in the blockchain. These nodes can be able to read, write and validate the blocks in blockchain based on the permission given for the nodes by which there are three types of Blockchain network available.

2.1 Permissionless Blockchain

Permissionless blockchain is also known as public blockchain network. The bitcoin is an example of the public blockchain network where anyone can join network without permission.

Anyone can run public node in their local device download whole copy of the block record till date, reading, writing, auditing, send transactions, mine blocks and participate in consensus. Another thing is that these types of blockchain are open and transparent hence anyone can review anything at a given point of time on a public blockchain.

2.2 Permissioned blockchain

Permissioned blockchain is also known as private blockchain network.Hyperledger is an example for the private blockchain implementation.Unlike public blockchain here there is an in charge who looks after of important things such as read/write or whom to selectively give access to read or vice versa.Here the consensus is achieved on the whims of the central in-charge who can give mining rights to anyone or not give at all.It is more faster then permissionless network.

2.3 Consortium or Federated Blockchain

Consortium or Federated blockchain offers the benefits of both public blockchain and private blockchain thus we can provide read-only access to their certain users and write access to others which improve transparency and reliability of network. There are numerous benefits to using a hybrid blockchain like the speed of private blockchains combined with the security of public blockchains. The private blockchain is used to generate a hash of transactions which is later verified using the public blockchain.

III. CONSENSUS

The Blockchain consist of long chain of blocks which is replicated over a network of nodes and new blocks are generated and added at frequent intervals of time or when certain event is occured based on the network architecture thus they need an mechanism in order to agree which block should be appended next.Major problem with the blockchain is that nodes does not trust each other thus nodes may behave Maliciously(byzantine manner).Thus consensus protocol must be able to tolerate “Byzantine fault tolerance(BFT)”.Byzantine fault tolerance achieve overall system reliability in the presence of a number of faulty nodes.In case of Cryptocurrencies an addition problem is to stop double spending.The first consensus protocol which resolves BFT and double spending for digital currencies is Proof Of Work(POW) proposed by Satoshi Nakamoto.Then there are many consensus protocols proposed such as Proof Of Stack, Proof of Burn and other.But for Permissioned network different set of consensus protocol have been used Since they concerned only about malicious nodes.some consensus protocol are PBFT, RAFT, POA and others.Each of these consensus protocol proposed has different properties in terms of performance,Scalability,Safety,Liveness and many.

3.1 Proof Of Work

In POW miners need to find solution to cryptographic puzzle using hash function.In Such a way it should be difficult to find the solution but easy to verify.The only way in which block will be accepted is to correctly guess the nonce, or a pseudo-random number generated by the network to be solved in a certain amount of time. Thus solution is to find an special number called nonce.

$H(a \| n) > t$

Which satisfy the equation where n = nonce, a = content of the block , t = mining difficulty(threshold),Bitcoin uses SHA256 hash function,Ethereum uses Dagger-Hashimoto

Simply miner wants find a nonce so that the resultant hash should contain certain number of zero at prefix.Main problem with POW consensus is power consumption

3.2 Proof of Stack

POS protocol reduces the energy consumption by selecting miners who needs to solve the puzzle based on their stake.In POS it maintains a single chain of blocks(without branches like POW) by selecting which miner can solve puzzle(create the block) from the available miners in a randomized manner by changing puzzle difficulty to be inversely proportional to miners stake in network.In this protocol only selected miner will mine the block so other miners wait for their turn.Stack is basically an locked account with certain balance representing miners commitment to keep the network healthy.Provides increased protection thus executing an attack needs more balance in the stack thus if an miner behaves malicious it affects him also since he wons certain currency of the network.The more stake one has, the higher should be his or her interest in preserving the system

Table 2
Comparison between POW and POS

POW	POS
Do some work to mine a new block	Acquire sufficient stake to mine a new block
Consumes Physical resources like CPU time and power	Consumes no external resource but participate in transactions
Power consumption is high	Power efficient

3.3 Proof of Authority

PoA consensus is essentially an optimized Proof of Stake model that leverages identity as the form of stake rather than actually staking tokens. The identity is staked by a group of *validators* that are pre-approved to validate transactions and blocks within the respective network. The group of validators is usually supposed to remain fairly small in order to ensure efficiency and manageable security of the network.It does not depend on nodes solving arbitrarily difficult mathematical problems, but instead uses a set of "authorities" - nodes that are explicitly allowed to create new blocks and secure the blockchain. The chain has to be signed off by the majority of authorities, in which case it becomes a part of the permanent record. This makes it easier to maintain a private chain and keep the block issuers accountable.POA can be used for private chain setups

3.4 Practical Byzantine Fault Tolerance

PBFT protocol is used for permissioned blockchain in which nodes/participants are known users but we need to be secure against malicious nodes.In PBFT only a single chain of blocks are maintained unlike POW it has block finality.Here the number of transactions per block and block generation needs to be more faster since it is used for enterprise use cases.But in order to tolerate byzantine problem they need to in sync and many network message needs to be flooded this affects the scalability of the protocol.

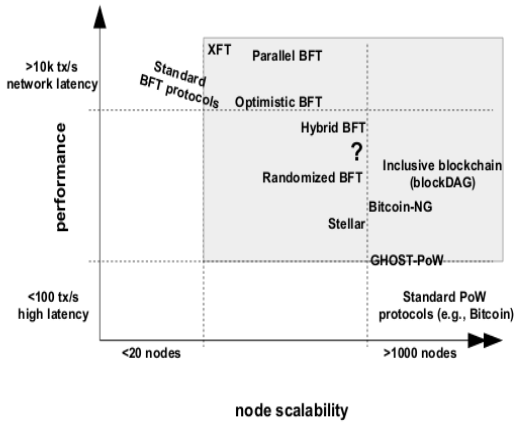

Fig 2 Comparison graph of consensus from
Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication paper

From the graph, we can clearly see that PoW and BFT are indirectly proportional to one another in terms of scalability of nodes and performance. Thus PoW-based consensus offers good node scalability with poor performance, whereas BFT-based blockchain offers good performance for small numbers of nodes. Other protocols are proposed and used such as GHOST protocol is a conflict-resolution strategy, it offers performance benefits over the standard longest chain rule of Bitcoin.Bitcoin NG which uses standard PoWfor leader election, and leader can mine blocks and many more.

Tabel 3
Comparison of Consensus Protocols

Consensus Protocol	Network Setting	Description
Proof of Work(POW)	Public	Bitcoin uses pure POW
Proof of Stack(POS)	Public	Tendermint uses POS where miner ability to mine the block is based on the stack
PBFT-based	private	Hyperledger uses original BPFT. Other variant of PBFT are scalable PBFT, Parallel PBFT
Proof of Authority(POA)	Private	Parity Uses POA where pre-defined nodes are considered as validators

VI. CRYPTOGRAPHY

Blockchain uses a ton of cryptography technique in order to ensure the Integrity of the DCT and user identity,

transaction identity use public-key cryptography.Using Merkle tree we can able to store only root hash of block and very the all transaction of block with it.

4.1 PUBLIC KEY INFRASTRUCTURE

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store & revoke digital certificates and manage public-key encryption.PKI(Public Key Infrastructure) is the framework for encryption, confidentiality and authentication protects communications between the server (your website) and the client (the users).When communicating, the client uses the public key to encrypt and decrypt, and the server uses the private key.A set of policies, Software/hardware and procedure which is required for the creation, management, and distribution of the digital certificates is known as public key infrastructure (PKI). Yes, encryption is performed in PKI.

4.2 DIGITAL SIGNATURE

A digital signature guarantees the authenticity of an electronic document or message in digital communication and uses encryption techniques to provide proof of original and unmodified documentation attached to an electronically transmitted document to verify its contents and the sender's identity.A digital signature is also known as an electronic signature such as Notary.Usually the blockchains can work on single signature but they can include Multi signature. Thus in multi signature mostly three keys can be used for safer and helps recovery from a disaster or accidental loss of private key. This is called a multi-signature system or 'multisig' or funds can be transferred when two or more people sign it can be used for business like a board of directors of three maintaining funds for an organization.It is usually a set of potential signees and minimum required signatures for a valid transaction

4.3 HASHING FUNCTION

A string of characters into a usually shorter fixed-length value or key that represents the original string. Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value.Hashing is generating a value or values from a string of text using a mathematical function . A hash is created using an algorithm, and is essential to blockchain management in cryptocurrency. A hash algorithm turns an arbitrarily-large amount of data into a fixed-length hash ,Like all computer data, hashes are large numbers, and are usually written as hexadecimal. Bitcoin uses the SHA-256 hash algorithm to generate verifiably random numbers in a way that requires a predictable amount of CPU effort.

4.4 MERKLE TREE

Blockchain data structure is a linked list of transaction connected back to one another by hashed links Actually it is a sequence of blocks and each blocks contains many transactions. Blockchain use merkle tree a method that uses hash of the whole set of transactions is left..that last transaction is called the merkle root

- Ability to verify whether a transaction is include in a block
- Able to provide Light-clients (don't need to download the entire chain)
- Overall performance and scalability

4.5 ZERO KNOWLEDGE PROOF

A zero knowledge proof is a game between a prover and a verifier. For a given assertion, the goal of a prover is, through the conversation with the verifier, to show the correctness of the assertion to the verifier without revealing the actual proof. If proving a statement requires that the proof the secret information, then the verifier will not be able to prove the statement to anyone else without possessing the secret information

V. SMART CONTRACT

A smart contract is a concept introduced by the Ethereum blockchain network. It is a computer program that is capable of self-executing and running a set of predefined functions when a specified condition or set of conditions occurs. The program is stored on the distributed ledger and is capable of appending the resulting change to the distributed ledger.The main aim of a smart contract is to automatically execute the terms of an agreement once the specified conditions are met.The smart contract is designed to function without reliance on a centralised authority.

VI. DISTRIBUTED LEDGER TECHNOLOGY

Blockchain is type of a distributed ledger. Distributed ledgers use many heterogeneous computers (referred to as nodes) to record, share and synchronize transactions in their respective ledgers. A ledger is a data structure that consists of ordered list of transactions. For example a ledger may record monetary transactions between multiple banks or goods exchanged amongs knows parties. In blockchain ledger is replicated over all nodes. The most successfully adoption of

blockchain technology is crypto currency in the wake of bitcoins success multiple competing currencies appear. Crypto currency is one instance of digital assets pieces of data with attached real-word values. Most blockchain are designed to protect transactions integrity but they do not consider transactions privacy. A blockchain is said to have transactions privacy when transactions cannot be linked form one to another when transactions contents is knows only to its participants.DLT is a digital system for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time. Unlike traditional databases, distributed ledger have no central data store or administration functionality.

VII. INTERPLANETARY FILE SYSTEM

InterPlanetary File System (IPFS) is a protocol and network designed to create a content addressable peer to peer method of storing and sharing hypermedia in a distributed file system.. IPFS is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files. IPFS could be seen as a single Bit Torrent swarm, exchanging objects within one Git repository. In other words, IPFS provides a high-throughput, content-addressed block storage model, with content-addressed hyperlinks Distributed Content Delivery saves bandwidth and prevents DDoS Attacks which HTTP struggles withThe filesystem can be accessed in a variety of ways, including via FUFE and over HTTP In 2014, the IPFS protocol took advantage of the Bitcoin blockchain protocol and network infrastructure in order to store unalterable data, remove duplicate files across the network, and obtain address information for accessing storage nodes to search for files in the network.

VIII. CONCLUSION

Blockchain Technology in recent years become more popular due to its nature of make multiple parties work together without conflicts. We have seen the basic concepts of blockchain such as cryptography,smart contract, Blockchain platforms,consensus algorithms and their performance comparisons.Then we seen what IPFS and how it can be utilized.From this we gained knowledge about what is blockchain and technologies that make it possible

REFERENCE

[1] Satoshi Nakamoto ,"Bitcoin: A peer-to-peer Peer-to-Peer Electronic Cash System" 2008.
[2] S.Eskandari, D.Barrera,E.stobert and j.clark "A first look at the usability of bitcoin management" (at ArXiv in 2015)
[3] Mr. Hari Krishna K Ms. Aaradhana Deshmukh Mrs. Vaishali Maheshkar Dr. N.M. Nandhitha Bhupendra Pratap Singh "Tendermint:blockchain app development simplified" (2017)
[4] POA Ethcore,"Parity:Nextgeneration ethereum browser" (2017)
[5] M.castro and B.Liskov "practical byzantine byzantine fault tolerance" (545 Technology Square, Cambridge, MA 02139)
[6] "Hyperledger , Sawtooth distributed ledger" 2016
[7] "Ethereum blockchain app platform" 2017
[8] "untangling blockchain, A data processing view of blockchain system" (2018)
[9] Marko Vukolic "The quest for scalable blockchain Fabric: proof of work vs BFT replication "(conference paper may 2016)
[10] MassimoDiPierro(Journal&Magazine:Computing in Science & Engineering in 2017)
[11] Valentina Gatteschi, Fabrizio Lamberti, Claudio Demartini, Chiara Pranteda,Víctor Santamaría(Journal & Magazine:IT Professional in 2018)
[12] Brian A. Scriber "A Framework for Determining Blockchain Applicability" (Journal & Magazine: IEEE software in 2018)