International Journal of Pure and Applied Mathematics
Volume 118 No. 18 2018, 2965-2970
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

On Blockchain Applications: Hyperledger Fabric And Ethereum

Sajana P.
TIFAC-CORE in Cyber Security
Amrita School of Engineering, Coimbatore
Amrita Vishwa Vidyapeetham, India
sajana.sajuj29@gmail.com

Sindhu M.
TIFAC-CORE in Cyber Security
Amrita School of Engineering, Coimbatore
Amrita Vishwa Vidyapeetham, India
m_sindhu@cb.amrita.edu

M. Sethumadhavan
TIFAC-CORE in Cyber Security
Amrita School of Engineering, Coimbatore
Amrita Vishwa Vidyapeetham, India
m_sethu@cb.amrita.edu

***Abstract*— Blockchain is a tamper-proof digital ledger which can be used to record public or private peer to peer network transactions and it cannot be altered retroactively without the alteration of all subsequent blocks of the network. A blockchain is updated via the consensus protocol that ensures a linear, unambiguous ordering of transactions. Blocks guarantee the integrity and consistency of the blockchain across a network of distributed nodes. Different blockchain applications use various consensus protocols for their working. Byzantine fault tolerance (BFT) is one of them and it is a characteristic of a system that tolerates the class of failures known as the Byzantine Generals Problem. Hyperledger, Stellar, and Ripple are three blockchain application which uses BFT consensus. The best variant of BFT is Practical Byzantine Fault tolerance (PBFT). Hyperledger fabric with deterministic transactions can run on the top of PBFT. This paper focuses on a survey of various consensus mechanisms and makes a comparative study of Hyperledger fabric and Ethereum.**

Keywords*— consensus; hyperledger fabric; ethereum; byzantine fault tolerance;

I. INTRODUCTION

Transactions are the basis of all types of communications in the world. A safe and secure transaction is the necessity of the humans at present. Third-party transactions were the best possible method used earlier, but they were proven insecure. The distributed ledger was introduced to reduce the dependency on third parties and to remove associated issues like double spending [8], which is nothing but the success full spending of some money more than once. Blockchain or distributed ledger technology (DLT) [13] is a technological protocol that enables data to be exchanged directly between different participating parties within a network without the need for intermediaries or third parties. It can also be described as a tamper-evident ledger [11] where tamper-evidence is achieved by using cryptographic hash functions. Blockchain records the transaction in a fixed structure called "block". Each block is secured and linked using hash functions.

A blockchain is the underpinning technology that maintains the Bitcoin [8] transaction ledger. Implementation of blockchain for Bitcoin solved double spending issues without any help of an administrator. Each block is a fixed structure that records the bitcoin transaction in a blockchain. Transactions are encrypted and stored in the blocks. Blocks are secured and connected using hash functions. Merkle tree [11] is a tree in which every node is labeled by the hash of its child. If a single data in any of the transaction changes Merkle root also shows the change, thus system can maintain integrity. Consensus [3] is the procedure to have an accurate blockchain in every node participating in the transaction and the protocol form the core of validation process in the blockchain, prevent centralization issues. Further, blockchain 2.0 technologies were also developed and it goes beyond the transactions of data. Exchange of values with the help of blockchain is faster, cheaper and secure. Also, Russian

Federation has announced a project which uses blockchain 2.0 technology for the automated voting systems [22].

II. Types of blockchain

The blockchain is broadly classified into three, public blockchains, federated blockchains or consortium blockchains and private blockchains [13]. A Public blockchain is completely decentralized, anyone can read and write the data stored on it. Participants are unknown to each other and trust rise from game-theoretical incentives [7]. The protocol based on proof-of-work consensus algorithms are public and permissionless. Internet users can start running the public node on their local device. They can validate the transaction by participating in the consensus process. Anyone can send the transaction through the network and they can expect them in the blockchain if the transactions are valid. Public blockchain uses mathematical computations, so it is very hard to hack. As the cost of hacking becomes too high for a system where every node is connected with the entire blockchain. Bitcoin is the first public blockchain which is used for currency exchange, followed by Ethereum. Dash, Lisk, Factom, Blockstream, Monero, Litecoin, Dogecoin, are other examples of the public blockchain.

Consortium [13] is a permissioned blockchain which operates under the leadership of a group. It has a predetermined set of nodes which controls the consensus process. Permissioned blockchains are Partially decentralized and a hybrid between the low-trust and single-highly trust network. They are highly scalable and provide more transaction privacy. Banking sectors are commonly using consortium network which maintains the privacy of a user's data, without merging power with a single organization. Few examples are R3 (Banks), EWF (Energy), B3i (Insurance), Corda, and Ripple.

The participants are known and trusted in a private blockchain network. All permissions are kept centralized to one organization. Verification of transaction is done by less number of devices internally, thus it is faster. The network reduces the cost of transactions and data redundancies, that replaces legacy systems. Internal process is managed by adding cryptographic auditing. But because of centralization, there should be some security risks. Private blockchains come under the category of permissioned [7] blockchains, it is energy efficient and easily implementable compared to permissionless blockchains. Blockstack, MONAX, Multichain are the common examples.

Another dimension by which the blockchain platforms are characterized is generic and specific[7]. Bitcoin and Hyperledger are specific blockchain platforms which are optimized for a specific task such as tracking assets, transferring values. Ethereum and Eris are general purpose blockchain platforms, which allow users to write their own algorithmic code and running customized logical processes.

III. Consensus Mechanisms In Blockchain

Generally, Consensus is a way by which a diverse group makes a decision without any conflict. In distributed systems, the consensus is reached by a majority of network members who agrees on the value of a piece of data and which then update the ledger. In a permissionless [7] setting anyone can join and participate in the process. Nodes can leave from the network dynamically where they may not have the knowledge of each other. Distinct consensus algorithms are build based on the requirements like performance, scalability, data capacity, consistency, decentralized governance, fault tolerance and security [11]. Proof of work, Proof-of-stake (PoS), Byzantine fault tolerance algorithm (BFT), Delegated proof-of-stake algorithm (DPoS), Proof of activity, Proof of capacity, proof of storage, proof of burn, Proof of elapsed time, Deposit based consensus, Federated Byzantine Agreement (FBA) [1], Proof-Of-Importance, Proof-of-Identity, KSI consensus, Leader based consensus, Round robin, N2N etc. are some existing consensus mechanisms in blockchain.

Bitcoin cryptocurrency, first known blockchain application, use hashcash proof of work [8] based consensus mechanism, this ensures the global consensus across thousands of public nodes. In proof of work [3] mechanism, each block contain nonces, the miners set a predefined target in such a way that the hash of the entire block is smaller than a known target, which is typically a very small number. The difficulty of block mining is inversely proportional to the target, and it made with respect to block mining rate, but indirectly with respect to the computational power of nodes participating in mining. This is to maintain the block mining rate of one block every 10 minutes and it is referred to as block frequency. In proof of work, one node has one vote and the majority decision is represented by the longest chain which has the greatest effort on proof of work, so the honest chain will grow faster. But if an attacker tries to hack Bitcoin network, he will gain 51percentage [8] of the computing power from the entire network. This is the reason behind centralization of mining power takes place. In order to solve the issues of computing power and wastage of energy, a new cryptocurrency consensus mechanism, Delayed Proof of Work (dPoW), is introduced. It is as secure as proof of work and is achieved by notarizing blocks created in the initial Bitcoin blockchain. Proof of stake [3] is a different way to validate transactions and achieve the distributed consensus. It is a form of ownership of the currency and the coin age [12] consumed in a transaction is one of the forms. It can't be easily forged like Bitcoin. Ethereum, a public blockchain platform, wants to exploit the proof of stake method for a better and cheaper distributed form of consensus.

State-machine replication protocols which particularly interested for blockchains is the Byzantine-fault-tolerant (BFT) protocol [3,6]. It distributes an application over many processes for tolerating faults, attacks, and misbehavior among a subset of the processes. It promises consensus in the network despite the participation of malicious (Byzantine) nodes. BFT

protocol prototypes have been shown to be practical, reaching practically minimal latencies allowed by the network, and supporting thousands of transactions per second. The state-machine replication paradigm inherently requires the application to be deterministic. PBFT is the best-known variant of BFT, used by Hyperledger Fabric. This algorithm requires " $3f+1$" replicas to be able to tolerate " f " failing nodes.

A new method of securing cryptocurrencies network is Delegated proof of stake [16]. It is the fastest, most decentralized, most efficient, robust and most flexible consensus model available. It has the power of stakeholder approval voting to resolve consensus issues in a democratic way. Stakeholders can elect a number of delegates to generate blocks. All network parameters such as transaction size, block intervals are tuned by the delegates and the transaction to be held in seconds because of deterministic selection of block producers. BitShares [12] is first and foremost globally distributed database that is used as a ledger to track ownership of digital assets.

IV. Hyperledger

Hyperledger [20] is a project of open source blockchains by the Linux Foundation, to support the collaborative development of blockchain-based distributed ledgers. The project has an objective of advance cross-industry collaboration [9] by developing blockchains and distributed ledgers, with a particular focus on improving the performance and reliability of these systems. Currently, there are five business blockchain framework hosted by Hyperledger. They are Fabric, Burrow, Iroha, Sawtooth, Indy [17].

A. Hyperledger Fabric

Hyperledger Fabric is being actively developed under Hyperleger project by IBM. It is a distributed ledger platform for running chaincode [19] (smart contract in Fabric), and proven technologies. The modular architecture delivers high degrees of resiliency, flexibility, confidentiality, in design and implementation. The flexibility in design leads to achieving scalability, privacy, and other desired attributes. The fabric is designed to support pluggable implementations of a different function, it also allows to use any programming language to implement chaincodes, commonly use Go language and run within Docker containers. Transactions in the fabric are private and confidential, channelization [3] will make sure about this capabilities. Since the network is permissioned, every user participating in the transaction must register in the network for getting their corresponding enrollment ids. Fabric ledger also provides auditability [21] in order to meet the regulatory needs.

In Fabric architecture, it is logically organized based on the service provided. These include blockchain services, membership services, and chaincode services. The current version of Hyperledger Fabric is v1.0, but it is not stable. However, the other version v0.6 is available and is stable.

***Blockchain service*:** The core part of Hyperledger fabric is Blockchain service [5]. Consensus manager, distributed ledger, peer to peer protocol and ledger storage are the components under this category. Consensus manager is responsible for providing the interface to the consensus algorithm, and it receives the transaction from other Hyperledger network and executes according to the type of consensus algorithm chosen. The consensus is pluggable, and currently there are three types of consensus algorithm in Fabric, they are PBFT protocol, SIEVE algorithm [9], and NOOPS. Distributed ledger is a database used by smart contracts to store relevant state information during transaction execution. These transactions contain chaincode, which runs transactions that can result in updating the world state. Each node saves the world state on disk. The block structure of Fabric having a number of fields such as version, timestamps, transaction hash, state hash, previous hash, consensus metadata and non-hash data. The other component Peer to peer protocol is built by using googleRPC [5]. Structure of the message in Fabric is defined by protocol buffer. Using different messages, network discover the peers and execute confidential as well as public transaction. The Ledger storage saves state using RockDB [5].

Membership service: Membership services [5] have the functions like user identity validation, user registration and assign appropriate permissions to the users depending on their roles. These functions together form access control for the fabric users. In order to support authorization and identity management operations, they use public key infrastructure [5]. There are three certificate authorities, in which Enrolment certificate authority [4] will issue a long-term certificate to registered participants in order to provide the identity. Transaction certificate authority issues transaction certificate for the participants to send the transactions on the network. TLS certificate authority [5] issues TLS certificates to secure the network level communication between fabric nodes.

Chaincode services: Chaincodes execute within the secure container that are created by this service. It has two components - secure container and secure registry.

The distributed ledger protocol in fabric network is run on peers. There is two type of peers: *validating peer* and *non-validating peer* [4]. Validating nodes or peers are responsible for running consensus in the fabric network. They validate a transaction and maintain the ledger. Non-validating nodes issues transactions for validating nodes, other than executing and verifying them.

Validating peers run BFT (Byzantine fault tolerance) as consensus protocol that executes replicated state machine. Deploy transaction, invoke transaction and query transaction [4] are the type of transactions accepted by the replicated state machine.

Deploy transaction: Take the installed chaincode written in Go language from peers, and ready to be invoked.

Invoke transaction: Invoke the transactions of a particular chaincodes which are installed earlier. Chaincode executes the

transactions and updates the state, then it indicates whether transaction succeeded or failed.

Query transaction: It returns an entry of the state by reading the persistent state of peers and it may not be linear**.**

BFT consensus ensures the validation of the transaction by executing replicated state machine, ie; if there are " n " validating nodes in which " f " are faulty nodes, assume at most $f < (n/3)$ behave arbitrarily, but all other node executes chaincode properly. To execute on the top of PBFT the chaincode transactions must be deterministic. The security infrastructure for fabric includes enrollment and transaction authorization through a public key certificate. Confidentiality for chaincode realized through in-band encryption [4] and states with a blockchain-specific key is available to all peers with an enrollment certificate for the blockchain.

V. Ethereum

Ethereum [18] is an open blockchain platform that allows anyone to build and use decentralized applications that run on blockchain technology. Financial interactions or exchanges in the different industry could be carried out automatically and accurately using code running on Ethereum. It was designed to be flexible and adaptable and has a powerful shared global infrastructure. The movement of assets around the network represents the ownership of property. In some ways, Ethereum is similar to that of Bitcoin, but there some technical differences between them. Bitcoin offers peer to peer electronic cash system, while Ethereum blockchain focuses on running the smart contract code of any decentralized application. Miners work to earn the crypto token Ether, this is also used to pay transaction fees and services in Ethereum network. Sometimes loss of Ether occurs due to loss of private keys, owner's death without transmission of private keys, or purposeful destruction of an intruder by sending to an address that never had associated private key.

Ethereum virtual machine: Ethereum virtual machine (EVM) [10] is the heart of Ethereum. Each and every node in the Ethereum network runs EVM, which can execute the complex algorithmic codes written in friendly programming languages designed on existing languages like JavaScript and Python. Parallelization of computing across Ethereum network using EVM makes it slower and expensive. Rather, running of EVM in every node maintain the consensus in the entire blockchain. This decentralization of consensus confirms the extreme level of fault tolerance.

Mining in Ethereum: Ethereum has a proof of algorithm called Ethhash [20], and involves in finding a nonce input to the algorithm so that the result is below a certain difficulty threshold. Time needed to find a nonce depends on the threshold. On an average, a block mining takes 15 seconds in Ethereum. The winning miner will get a consistent block reward of 5.0 Ether [10]. All the gas consumed by the execution of transactions in the block is paid by the senders of each transaction, the gas cost acquire is credited to the miner's account as part of the consensus protocol in the form of Ether.

Ethereum is vulnerable to different kind of attacks. In mining itself, it undergoes 51% attack if an attacker possesses more than half of network mining power. Here smart contracts are visible to all users of blockchain and it leads to the situation where security holes and bugs are visible by everyone, so it is difficult to fix the problems. The DAO (decentralized autonomous organization) [2] is a crowd funding platform, which underwent an attack by an adversary using the concept used by DAO. The step taken by the adversary was to publish the contract Mallory in which the adversary donated ether and himself made a withdraw, this create a fallback [2] for Mallory. This scenario created an event that appeared as if a person had credited ether, but then he had actually stolen the ether along with what he had invested. In case of DOS attack, the scenario is different, where the low gas price of Ethereum network had given the attacker an ability to threaten the network with the continuous request.

VI. Comparison of Hyperledger fabric and Ethereum

The significant difference between Ethereum and Hyperledger is the way they are designed and their target audience. Ethereum, with its EVM, execute codes of arbitrary complexity and publicly accessible to any user without permission. This blockchain target towards distributed applications. On the other hand, the Hyperledger fabric has a modular architecture that ensures the flexibility, hence scalability with a permissioned mode of operation. Both the applications run smart contract codes. In Fabric it is known as chaincode, and there exist specific channels for clients where they can see the messages and associated transactions of the connected channels. By this way, access to the transactions are restricted, that provide confidentiality to the transactions. In order to reach the decision, both are using different consensus mechanisms. Ethereum use proof of work as consensus, where all participating nodes agree upon a common ledger. Now it is trying to move towards proof of stake for the next release. The consensus in Fabric can be "pluggable" [14]. That is depending on application-specific requirements various algorithms can be used. In Fabric, nodes have different roles and tasks in the process of reaching consensus. This contrasts to Ethereum where nodes have identical roles and tasks in reaching consensus. Smart contract code in Fabric can be written in Go or Java, where Solidity [18] for Ethereum. The built-in cryptocurrency for Ethereum is Ether, but Fabric does not require any built-in currency as there is no mining. After all, Ethereum has a generic platform that runs powerful smart contracts which is public and transparent, modular architecture of Fabric allows a customized platform for a specific mode of operation. A comparison between Ethereum and Hyperledger Fabric is given in table below

TABLE I.

Characteristics	Ethereum	Hyperledger Fabric
Description	Generic blockchain platform	Modular blockchain platform
Governance	Ethereum Developer	Linux Foundation
Mode of Operation	Permissionless, public or private	Permissioned, private
Consensus	Mining based on proof of work	Pluggable PBFT
State	Key-value database	Account data
Currency	Ether	None
Mining reward	A static block reward for the winning block consisting of exactly 5.0 ether	None
Transaction	Anonymous or Private	Public or Confidential
Smart Contract	Solidity programming	Smart contract Chaincode
Language	Go, C++, Python	Java, Go
Scalability	Claim to be scalable	-

VII. Conclusion and Future Work

Blockchain was invented in the context of the digital currency. Now it is one of the emerging technology in financial services, supply chain industry as well as in banking. People are educating on the nature of blockchain technology in order to fully utilize it, and many of the financial services have already built their blockchain applications. Some industries using blockchain solution as a payment component, but other industries, will use it as an immutable record [15] and maintain it securely. Different applications use different blockchain protocols. Certain solutions need public and open blockchain applications based on the protocols like Bitcoin and Ethereum, but other solutions need permissioned ledger like Hyperledger. In this paper, we made a survey on various consensus protocols used in the blockchain, and a comparative analysis of two applications of blockchain that uses different consensus protocol for their working. Hyperledger fabric having a key property of its extensibility, and in particular, it also supports multiple ordering services for building the blockchain. The v1.0 of Fabric launched without an implementation of a Byzantine-fault-tolerant (BFT) ordering service. So we can introduce a better consensus such as Delegated proof of stake in order to reduce time consumption to make decisions. Ethereum is vulnerable to various kinds of attacks such as DOS attack and DAO attack. The next release of Ethereum will use proof of stake as a consensus, for improving the performance of the system. The features of Blockchain technology can be extensible to a wide verity of areas such as healthcare, science, literacy, publishing, economic development, art, and culture.

References

[1] 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

[2] 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.

[3] Baliga, A., Understanding blockchain consensus models. Tech. rep., Persistent Systems Ltd, 2017.

[4] Cachin, C., Architecture of the hyperledger blockchain fabric. In Workshop on Distributed Cryptocurrencies and Consensus Ledgers, (2016).

[5] Imran Bashir, Mastering Blockchain, Distributed ledgers, decentralization and smart contracts explained, (2017)

[6] KPMG, Consensus immutable agreement for internet of values, https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf

[7] Mattila, J., The blockchain phenomenon. (Berkeley Roundtable of the International Economy, 2016, edn.), (2016).

[8] Nakamoto, S., Bitcoin: A peer-to-peer electronic cash system, 2008.

[9] 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-ledger-technologies-in-general/.

[14] Comparison between hyperledger fabric and ethereum, http://www.techracers.com/hyperledger-vs-ethereum.

[15] Consensus in blockchain, https://www.coindesk.com/short-guide-blockchain-consensus-protocols/.

[16] Delegated proof of stake, https://bitshares.org/technology/delegated-proof-of-stake-consensus/.

[17] Different hyperledger platforms, https://blockgeeks.com/guides/what-is-hyperledger/.

[18] Ethereum basics, http://ethdocs.org/en/latest/introduction/what-is ethereum.html.

[19] Hyperledger burrow, https://www.hyperledger.org/projects/hyperledger-burrow.

[20] Hyperledger introduction, http://hyperledger-fabric.readthedocs.io/en/release/blockchain.html.

[21] Hyperledger whitepaper, http://www.thedata.co/sites/thedata.co/files/u1/Hyperledger%20Whitepaper.pdf.

[22] Blockchain and Payment, https://www.linkedin.com/pulse/blockchain-payments-ramalingom-sundaram-pillai