International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

Different Blockchain Platforms And Algorithms

Neethu Gopal[1], Jibi Mariam Biju[2],Vani V Prakash[3]

[1]M.Tech. Student, Computer Science and Engineering, Sree Buddha College Engineering, Kerala, India.
[2]M.Tech. Student, Computer Science and Engineering, Sree Buddha College Engineering, Kerala, India.
[3]Assistant Professor, Computer Science and Engineering, Sree Buddha College Engineering, Kerala, India.

Abstract – *Now a days the demand of blockchain increases, everyone began to experience the potential of this technology. Initially, blockchain brought disruption in the financial sector, but now its uses have been scrutinize across various industries. Blockchain technology is a distributed public ledgers that holds unmodifiable data in a secure and encrypted way and ensure that transactions can never be modified. A **blockchain** can be permissioned, permission-less or hybrid. A distributed ledger is a peer-to-peer network, that uses a consensus mechanism to prevent alteration of an ordered series of time-stamped records. This paper briefly discuss about different blockchain platforms available in various industry.*

***Key Words*: Blockchain, Cryptocurrency, Bitcoin, Solidity, Consensus.**

1. INTRODUCTION

Blockchain technology was announced by Satoshi Nakamoto in 2008[1]. But he does not specifically use the word "blockchain". It mentions about a "purely peer-to-peer version of electronic cash". This open source technology defines a blockchain as a peer-to-peer network. Which records transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record or block that can be changed only by redoing the proof-of-work. A blockchain can be classified into permissioned, permission-less or hybrid. The blockchain technology, that uses a defined consensus mechanism[2] to prevent modification of an ordered series of time-stamped records. Consensus mechanisms include Proof of work, proof of stack, Federated Byzantine Agreement etc.

A **distributed ledger** database is shared, duplicated, and synchronized among the nodes (members) of a decentralized network. The database records the transactions, such as the exchange of data or electronic cash among the participants in the network. Members in the network govern and agree by consensus on the updates to the records in the ledger. No central coordinator, authority or third-party mediator, such as a financial institutions like bank or clearinghouse, is involved. Every blocks in the blockchain has a timestamp and unique cryptographic hash, thus making the ledger an auditable, immutable history of all transactions in the network. **Blockchain** technology in Bitcoin is nothing more than transactions secured and executed using cryptographic methods by the help of a scripting language. That means **blockchain** is a **platform** with a scripting language which can solve many use cases other than just cryptocurrencies.

2. BLOCKCHAIN

BLOCKCHAIN is the fundamental technology underlying the emerging cryptocurrencies including Bitcoin [2]. The main advantage of blockchain is widely considered to be decentralization, and it can help establish disintermediary peer-to-peer (P2P) transactions, coordination, and cooperation in distributed systems without mutual trust and centralized control among individual nodes. Blockchain can be considered as the next generation of cloud computing, and is expected to radically reshape the behavior model of individuals and organizations, and thus realize the transition from the Internet of Information today to the future Internet of Value.

Blockchain is a distributed type of database that is widely used for recording distinct transactions. Once a consensus is reached among different nodes, the transaction is added to a block that already holds records of several transactions. Each block contains the hash value of its last counterpart for connection. All the blocks are connected and together they form a blockchain. Data are distributed among various nodes (the distributed data storage) and are thus decentralized. Consequently, the nodes maintain the database together. Under blockchain, a block becomes validated only once it has been verified by multiple parties. Furthermore, the data in blocks cannot be modified arbitrarily.

3. MAJOR PLATFORMS

3.1 BigChainDB

It is initially designed as an open source system with a distributed database that can hold big amount of data and then adds blockchain characteristics like decentralized control, immutability and the transfer of digital assets**. BigchainDB**[4] tries to attain performance of 1 million writes per second throughput, storage of petabytes of data, and sub-second latency. The key features of this platform include**:** Each write is recorded on the blockchain database without the need for Merkle Trees or sidechains, It also support for

custom assets, transactions, permissions and transparency, Federation Consensus Model as well as public and private networks, Has no native currency—any asset, token or currency can be issued, Set permissions at transaction level, It is open source.

3.2 Chain Core

A blockchain platform is an infrastructure software for issuing and transferring financial assets on a permissioned blockchain infrastructure. Built specifically for the financial services industry, Chain Core[5][16] features financial assets in a digital medium, Instant settlement, Permissioned network access, scalability and reliability, Full-stack security, Reference data, immutable ledger, transaction privacy. It runs on the open-source Chain Protocol and its Developer Edition is free while the Enterprise Edition is a commercial product. The inception, control and transfer of assets are decentralised among participants on Chain blockchain networks. The operation of the network is supervised by a federation—a designated set of entities. The Chain blockchain networks include currencies, securities, derivatives, gift cards, and loyalty points as assets**.** The key features of Chain core include**,** Native digital assets—currencies, securities etc. Role-based permissions for operating, accessing, and participating in a network, Support for multi-signature accounts, Federated consensus, Support for smart contracts and Transaction privacy.

3.3 Corda

Corda [6] is a distributed ledger platform for recording and processing financial agreements with pluggable consensus. It is the only distributed ledger platform with pluggable consensus and is specialized for use with regulated financial institutions. It is inspired by blockchain systems, but without the design choices that make traditional blockchains inappropriate for many financial scenarios. Corda enabes an institution to transact directly using smart contracts, while ensuring the highest levels of privacy and security thus it removes costly friction in business transactions. From its creation, Corda was built specifically for business. Corda's key features include[5][6]**,** no global broadcasting of data across the network, pluggable consensus, Querying with SQL, join to external databases, bulk imports.

3.4 Domus Tower Blockchain

Domus Tower Blockchain[5] is designed for securities trading where participants know each other and can decide whom to trust. Domus Tower Blockchain has been "benchmarked at ingesting over 1 million transactions per second and its on hardware costing less than $50 per hour on Amazon's Web Services with the potential to scale more than 10 million transactions per second" as per its whitepaper. Data storage is done in a Merkle directional acyclic graph (MerkleDAG)[7] and each node referred as blocks. The data is digitally signed and verified before it is written to a block that is then being transmitted to the blockchain**.** Its features are creation of linked blockchains where the assets of an account on one blockchain must match the liabilities on the account of another blockchain. Transactions can be recorded in a scalable manner. Recording are done by double-entry balance sheet that tracks credits and debits.

3.5 Elements Blockchain Platform

Elements is an open source[5][8], the Bitcoin functionality is extended by a protocol-level technology. Features of elements are confidential assets—issue multiple assets who's identifiers and amounts are blinded yet auditable. Confidential Transactions—keep the amounts transferred visible only to participants in the transaction and to designated entities, new DETERMINISTICRANDOM operation that produces a random number within a range from a seed and new CHECKSIGFROMSTACK operation that verifies a signature of a message on the stack, rather than the spending transaction itself. Deterministic Pegs that allows cross-chain transactions to be constructed in a decentralized fashion and tokens are moved from one bc to another. Signed Blocks—this allows blocks can be cryptographically signed, thereby allowing the creator of the block to verify their identity in the future. Segregated Witness, Bitcoin transactions contain two things i.e. information and data proving that the transaction is authorized. witness segregation is used, transaction IDs are redefined to only depend on the effect information and blocks commit separately to the witness data. This eliminates all known forms of transaction malleability. Relative Lock Time which keeps tracks the transaction and are time-locked.

3.6 Ethereum

Ethereum is an open and decentralized platform featuring Turing completeness and supporting various derivative applications. Most smart contracts and decentralized autonomous organizations are created by using Ethereum [9]. If the Bitcoin blockchains are considered a global payment network, Ethereum would be the global computing system. Furthermore, Ethereum is an open-source platform similar to Android (developed by Google). It provides an infrastructure that enables developers to create applications. The infrastructure is developed and maintained by both Ethereum and those developers. The major characteristics of Ethereum are as follows:

1) Incorruptible: third-parties are not able to modify any data;
2) Secure: errors derived from personnel factors are avoided because the decentralized applications are maintained by entities rather than individuals;
3) Permanent: blockchain does not cease to operate even if an individual computer or server crashes.

Ethereum Virtual Machine (EVM) is a programmable blockchain. Unlike Bitcoin, which provides a fixed set of commands, the EVM allows developers to run any programs in the manner they wish. Developers instruct the EVM to execute applications by using a high-level language called Solidity[10]. It was founded in 2013 by Vitalk Buterin, a 22-year old Russian-Canadian programmer. Ethereum Virtual Machine (EVM) provides the run-time environment to smart contracts in Ethereum. Every node within the network has to run an EVM implementation.

Though enterprises have adopted Ethereum widely, it is essential to understand that Ethereum is a public (permissionless) blockchain platform, built for restricted access versus mass consumption. it is a PoW (Proof of Work) based platform, which is comparatively slower in terms of speed. But it might change its consensus algorithm to Proof of Stake in the coming years. Ether is the cryptocurrency used in Ethereum.

3.7 Ripple

Discovered in 2012, Ripple[11] is aimed at connecting payment providers, digital asset exchanges, banks, and corporate via blockchain network, RippleNet without any chargebacks. It allows global payments through a digital asset called "XRP or Ripple," which is now one of the popular cryptocurrencies like Ether and Bitcoin. Highly scalable and faster than other blockchains. It uses probabilistic voting which is used to reach the consensus between nodes.

The Ripple Protocol consensus algorithm (RPCA), is applied every few seconds by all nodes, in order to maintain the correctness and agreement of the network. Once consensus is reached, the current ledger is considered "closed" and are called the last-closed ledger. Thus the consensus algorithm is successful, and that there is no fork in the network, the last-closed ledger maintained by all nodes in the network will be identical.

3.8 Quorum

Founded by J.P. Morgan, Quorum[5] is an enterprise-focused version of Ethereum and modifies Ethereum's core therefore, can incorporate the Ethereum updates seamlessly and quickly.

Just like Ethereum, Quorum is also open-source, free to use blockchain platform in perpetuity. Different vote based algorithms to process hundreds of transactions per seconds. Quorum is permissioned, the networks using Quorum won't be open to everyone. It can be used in applications requiring high throughput processing and speed of private transactions.

Quorum resolves the issue of the confidentiality of records that Ethereum and other blockchains failed to handle by introducing private and public on-chain transactions.

3.9 Hyperledger Sawtooth

Hyperledger Sawtooth[12] framework is a blockchain with an aim to set the business enterprise by setting all the parties on the blockchain and maintaining the track of all the parties related to the business [13][14]. The consensus algorithm, transparency rules, and the permissions can be designed according to the requirement of the application. Different SDKs are available in different languages like Python, Go, Javascript, Rust, C++, and Java. With Sawtooth, we can write a smart contract in any language of our choice. AREST API is also provided for the development.

3.10 Hyperledger Fabric

Hyperledger Fabric is another framework for building blockchain based solutions or applications which uses a modular architecture. The modular architecture enables network designers to plug in their components like membership services and consensus, distinguishing it from other blockchain solutions.
This Fabric framework is designed for permissioned networks, allowing known identities to participate within a networked system. The participants should be authorized and have credibility in capital to take part in the blockchain. Firstly Digital Asset and IBM contributed to Hyperledger Fabric platform[5][12] as a result of the first hackathon. BC companies prefer building enterprise-grade applications using this blockchain platform.

3.11 Hyperledger Iroha

The main difference between IROHA[5][12] and other blockchain is that every participant is not allowed to store all the data history. The users can only query the data if they have been authenticated and have the permission. This system is developed for the clients having diverse application and peer hardware from embedded system to enterprise-class servers. The consensus algorithm used is Byzantine fault Tolerant consensus Algorithm called sumeragi which is highly influenced by the B-Chain algorithm. The goal of Iroha is to provide C++ libraries to the hyperledger projects. These libraries are Sumeragi consensus library, SHA-3 hashing library, API server library, Javascript library, etc. The cryptographic method used by IROHA is SHA256. Chain code is used to apply the transaction rules and validations. Java based chain code is supported. It is a simple and modularized distributed ledger system based on a highly secure and fast consensus algorithm called Yet Another Consensus, protecting Iroha networks from adversary nodes or failures. Being portable and supporting macOS and Linux environment, the platform is highly applicable for supply chain and IoT use cases.
The National Bank of Cambodia and Soramistu Co. Ltd. are working together to develop the distributed ledger project, i.e., Hyperledger Iroha.

Why Hyperledger Blockchain?

- **Modular Architecture**
  The plug and play nature of Hyperledger allows developers to build components more advantageously.
- **Transparent Process**
  The transactions on Fabric might be unclear, while the development process is not. The core teams behind Hyperledger have worked hard inorder to create a healthy balance between transparency in the development process and also attaining important milestones.
- **Smart Contracts**
  Like Ethereum Hyperledger also uses (chain code) smart contracts.

3.12 EOS

Launched in June 2018 as an open-source software, It was founded by a private company, Block.one. It is designed for the development of Decentralized applications(dApps). The company distributed one billion ERC-20 tokens to allow widespread distribution of their cryptocurrency and also allow anyone to use EOS[4] blockchain after it was released. The goal is to offer hosting of decentralized application's, storage of enterprise solutions and smart contract capability decentralized, solving the scalability issues of Ethereum and Bitcoin. Also, free of cost i.e., no one needs to pay to avail the benefits of a EOS based dApp.
It accomplishes consensus by using multi-threading as well as a delegated proof-of-stake algorithm. They use community forum named as EOS Forum, enabling developers and investors to discuss the platform and EOS Talk for their users based on the steem blockchain.

Why EOS blockchain for app development?

- **Free to use**
  Free of use means simply free of cost, the end user need not pay via micropayments to perform various tasks on the EOS platform.
- **Features**
  The platform enables the producers with a governance system in which they can use to vote on to validate transactions, modifications can be made to the source code of the platform and check whether an application is perfectly working.
- **Authenticity**
  A fully-featured authentication platform to the users where each account have different permission level to save data in a secure manner.

3.13 OpenChain

Openchain is an open source distributed ledger technology. It is used by organizations wishing to issue and manage digital assets in a robust, secure and scalable manner. Features of Openchain include: 1. Instant confirmation of transactions. 2. No mining fees. 3. Extremely high scalability. 4. Secured through digital signatures. 5. Immutability: Commit an anchor in the Bitcoin Blockchain to benefit from the irreversibility of its Proof of Work. 6. Assign aliases to users instead of using base-58 addresses. 7. Multiple levels of control8. Hierarchical account system allowing to set permissions at any level. 9. Transparency and auditability of transactions. 10. Handle loss or theft of private keys without any loss to the end users. 11. Ability to have multiple Openchain[4][15] instances replicating from each other.

4. CONCLUSIONS

This paper describes a brief idea of different blockchain platforms and its importance in the growing technical industrial applications. There are few more platforms like Steller, Neo, Hedera Hashgarph[4][5] etc. Steller is used for facilitating cross-asset transfers of value. Stellar Consensus Protocol (SCP) records the financial transactions. NEO is designed to develop scalable decentralized applications, the base asset of NEO BC is NEO token. It uses **Delegated Byzantine Fault Tolerance** as its consensus algorithm. It allows better performance and scaling. Hedera Hashgraph platform is fast, fair and secure platform that does not need to compute a heavy proof of work algorithm. This is also scalable.Fast interms it is capable of handling thousands of transactions per second and authenticate more than one million signatures per second. Hedera Hashgraph is asynchronous Byzantine fault tolerant and has high level of security. Day by day the scope for blockchain in the industry is drastically increasing and it will lead to a great change in the digital life.

REFERENCES

1. S. Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System - Bitcoin.org
2. https://pdfs.semanticscholar.org/0afd/a615470760dd1cd661fe4b5f7d3e9b39cdf3.pdf
3. A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital. Sebastopol, CA, USA: O'Reilly Media, 2015.
4. https://www.leewayhertz.com/blockchain-platforms-for-top-blockchain-companies/
5. https://medium.com/blockchain-blog/17-blockchain-platforms-a-brief-introduction-e07273185a0b
6. M. Hearn, "Corda: An introduction," 2016.
7. Merkle Tree. [Online]. Available:https://en.wikipedia.org/wiki/Merkle_tree (visited on05/02/2018).
8. Elements official website: https://elementsproject.org/
9. Benyuan He, "An Empirical Study of Online Shopping Using Blockchain Technology", Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.
10. Chris Dannen, Introducing Ethereum and Solidity, https://www.apress.com/br/book/9781484225349
11. ripple.com/files/ripple_consensus_whitepaper.pdf
12. Chinmay Saraf, Siddharth Sabadra,"Blockchain Platforms: A Compendium".
13. Hyperledger Sawtooth. [Online]. Available:https://www.hyperledger.org/projects/sawtooth (visitedon 05/02/2018).
14. Hyperledger - Blockchain Technologies for Business.[Online]. Available: http://www.hyperledger.org(visited on 05/02/2018).
15. https://media.readthedocs.org/pdf/openchain/latest/openchain.pdf
16. https://chain.com/
17. M. Macdonald, L. Liu-Thorrold, R. Julien, The Blockchain: A Comparison of Platforms and Their Uses Beyond Bitcoin .

BIOGRAPHIES

Neethu Gopal, she is currently pursuing Master's Degree in Computer Science and Engineering in Sree Buddha College of Engineering, Elavumthitta, Kerala, India. Her research area of interest includes the field of Security and Blockchain Technology.

Jibi Mariam Biju, she is currently pursuing M.tech in Computer Scinece and Engineering in Sree Buddha College of Engineering, Elavumthitta. Her research areas include the field of data mining, cryptography and security.