IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Study of Blockchain and Hyperledger

PARTHEESH MARWAH	POONAM MISHRA	ROBIN THAKUR	SONIA SETIA
MRIIRS,	MRIIRS,	MRIIRS,	MRIIRS,
FARIDABAD	FARIDABAD	FARIDABAD	FARIDABAD

Abstract

Blockchain plays an important role in Artificial intelligence Development and in financial sector. It makes easier to create a reliable technology which is enabled with decision making system. Many companies and banks are applying test and scale the reach to Blockchain in controlled environment. Blockchain solves many problems related to data as it is digital, decentralised and distributed with most virtual currencies. By the use of Blockchain, the data can be accessible to everyone on the open distributed network system which bring an end to the data hoarding trend lead by big web companies. This paper focuses on the growth, security, how it works , what are the uses and about the projects of Blockchain.

Keywords: Blockchain, decentralised, cryptocurrency, security, hyperledger

Introduction

Blockchain is on high trend where there is a secure computing without any centralised authority. It is based on two perspective – data and security. For data perspective data is stored in the blocks which are connected together and form chain where each new data is stored in every new block. And for security perspective, Blockchain has peer to peer network so that only data is transfer from one person to other without any intermediate and secured through decentralised cryptography.

Trend of Blockchain increased day by day and it will reach $19% in 2025. IT is quite often used in most of technologies and industries like Accenture, IBM, Citibank, CISCO, Microsoft. It is giant network. Machine learning, artificial intelligence, Blockchain become a market trend in next coming years. Company – IBM and apache foundation sponsored and making a project of Hyperledger. Ethereum and file coin provide a platform for research and development.

Overall, Blockchain has change the way of transaction, overcome the problem of traditional transactions like people do transactions through banks that have a mediators between them. But Blockchain has many challenges related to throughput, latency, security and many more. Scalability also has challenges in this.

Key concepts – Blockchain, Consensus, Bitcoin, Hyperledger

1. OVERVIEW ON BLOCKCHAIN

Let first talk about the Blockchain, what it is?

When you heard about bitcoin you would also heard about Blockchain. Basically, Bitcoin had started in 2008 with a pseudo name Satoshi Nakamoto (which is an individual and a group of individuals). Blockchain is a shortland for a whole suite of distributed ledger technologies that can be programmed to record and track anything of value like financial transactions, medical records , land titles. The Bitcoin uses the blockchain for online transaction with peer to peer network. Bitcoin is a public ledger that maintain the transaction integrity. Blockchain technology was first used when bitcoin was introduced. Bitcoin maintains its value in digital without any organisation or governmental authority in control. Now there are many more digital currency come across to world eg; USD,EUR,KRW for exchanging but Bitcoin seeks attention of many communities and leads to successful digital currency for exchanges with using blockchain technology. Bitcoin contains PKI mechanism. In PKI, it works on basis of keys- public key and private key. Public key is used for address and private key is for authentication. If sender sends data it contain one public key and it tends to receive it contains multiple keys. When each transaction done, data of each transaction is stored in a new block that is firstly verified by POW(Proof Of Work) and through consensus, it is add to chain, and this chain of block is bitcoin technique called Blockchain.

Blockchain is decentralised form for transaction of Cryptocurrency between the users without any third party. It is public hyper ledger that can't be modified, we can't delete or, modify the data once a transaction has done and add on blockchain. In addition to know about the transaction, it can achieve by hash value, in which every block contain one hash value, plus value of hash with preceding one which can be seen as its cryptographic image.

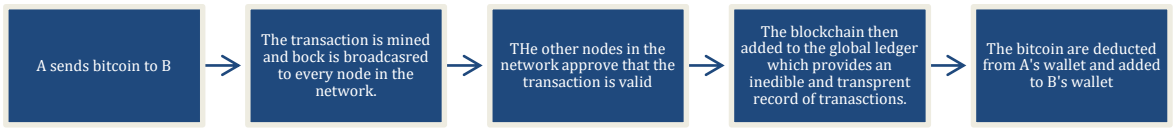
You may be think about that we already have tracked to store data, what's so special about blockchain? Let's break down your confusion:

(a) The way it tracks and stores data in a form of blocks that are connected together and form a blockchain is quite different.
(b) It has trust building in real time. Based on trust, blockchains can be divided into permissioned and permission-less blockchains.

It doesn't contain intermediates in real time.

Fig 1. Everything will be computing and connected by a blockchain one day. [Ref 1]

1.1 How does blockchain work?



(This figure shows how transaction performed)

Three basic capabilities that are support by blockchain (a) Hash Storage (b)Digital Signature (c) By Consensus by adding new block.
Due to these techniques, transactions easily done and new block add to the chain.

1.2 Hash Chained Storage –

It contains two fundamentals point one is hash pointer and other is merkle tree.

(a) Hash pointer: It is hash of data by cryptography, pointing to the location where data is stored. It helps to check whether data is tampered or not. Hash pointers helps to organise the blockchain. Each hash contains address of predecessor of predecessor block.

(b) Merkle tree: it is a type of binary tree where each node of tree connected together by hash pointers. Merkle tree has the ability of preventing data from tampering, it is done by traversing down through the hash pointers to any node in the tree. The member of merkle can be verified in logarithmic time by computing hashes on path and check the hashes value against the root.

1.3 Digital Signature –

It check the validity of data, it is done by cryptographic algorithm. It is used to check whether the data is not tampered.

It contain scheme which contain three steps- (a) key algorithm, which contains two keys one is private and other is public key.

(b)Signing algorithm, data or input is passed through private key.

© verification algorithm, it takes signature, public key, data and validates the data as output through public key.

Blockchain is decentralised so all depend on user which key is used as public or private key.

1.4 Consensus

What is consensus? It is basically employed for add block to seek for majority of network to agree on single state update in order to secure the data and prevent from malicious attack.

In addition for securing the transaction so that no one can tampered the network, consensus algorithms are use for it and it ensure that all nodes simultaneously maintains the identical chain of blocks.

The role of blockchain is basically to replace centralised database with certain authorities aspects. Once data is saved or record in chain ,it would be impossible to make change and by enforcing the majority agreement of update validity through consensus, it ensures the consistency state and prevents the double spending problem.

Most famous algorithms of consensus are : POW (Proof Of Work) and POS (Proof of Stake)

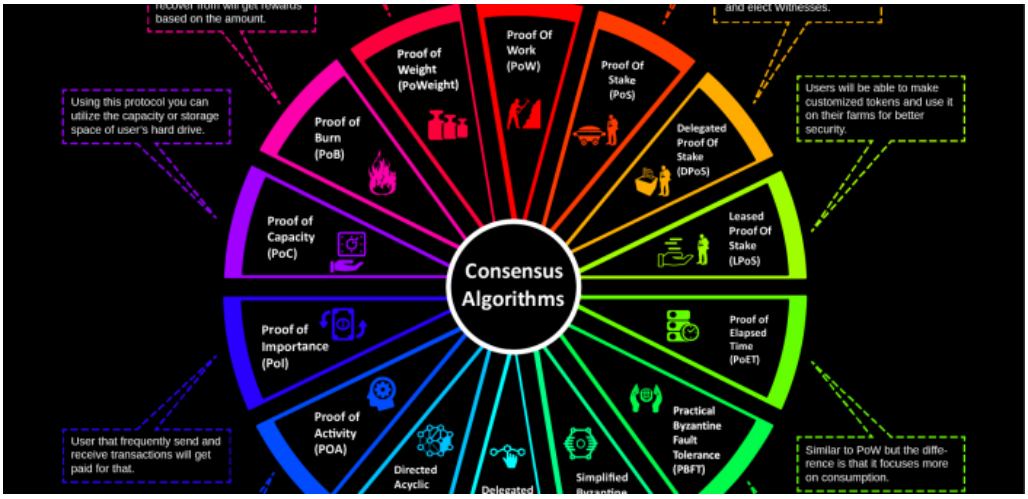


Fig 2 (Various consensus algorithms)

2. Blockchain level Transaction Model

Blockchain is created and maintained by distributed ledger for online transactions which consist of two model. The two model on which blockchain consist on :

(a) Unspent Transaction Output Model(UTXO) and

(b) Account based transaction model i.e Ethereum.

UTXO Model: Users store the total amount of bitcoins as unspent instances which are not used yet and store for future. The entire history of transactions is store as a unspent outputs, such that each of has owner and a value. The sum of all unspent bitcoin instances that the user has key to access as owner of bitcoin wallet. UTXO transaction can be done if it fulfil following requirements : (a) Every referenced input in transaction must be signed by its owner. (b) If transactions has multiple inputs then each input is verified with the owner through digital signature matching. (c) A transaction is only legal when number of inputs are equal or exceeds the total value of output.

For eg; Person A and Person B send 5 BTC- 5 BTC to Person C then Person C get these BTC as output. When Person C put all two instances into one , it means Person C gets 10 BTC and marks as unspent instances , so Person C can use it for later transactions.

It has many benefits like : high degree of scalability , high degree of privacy and security.

If there are benefits then there are drawbacks too. For eg; Person A has 100BTC and wants to sends 10 BTC to person B, it is quite difficult for transactions due to its complexity . Here Person A has to do 2 transactions, one for person A(10 BTC) and one for itself(90BTC). Sometimes it leads to leaks of private information.

Ethereum : In contrast Of UTXO, Ethereum come to be an extensions which work on account of sender only not depend on the unspent transactions which increases the efficiency of consensus but with a cost of high risk.

Vitalik Buterin is an inventor of Ethereum . We have a concept there i.e is EVM which stands on Ethereum Virtual Machine. Ethereum is mode for decentralised applications and shortly we can call as " Dapps". It is a platform not a cryptocurrency. Here the cryptocurrency for Ethereum is Ether. It is an open source platform where we can make applications and language is Solidity for it.

The transactions is same as the transactions done in bank today. It is only valid when it fulfil its three constraints : (a) Token is signed by message sender (b) the writer's ownership of token value can be attested (c) the writer sender has sufficient balance in the account.

In this , if Person A has 1ETH and also A get 2 ETH from Person B. now current balance of Person A is 3 ETH, without the need of another transactions for combining the instances. A global state contains with list of accounts, codes, balances and internal storage. It is possible but more difficult to track individual transactions as they are added to receiver balance and subtract from sender balance.

3. Hyperledger

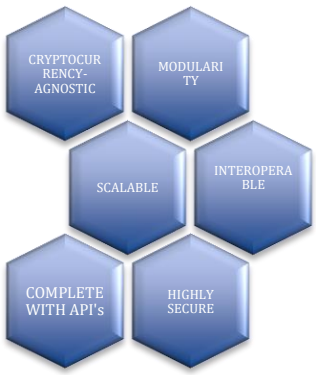
Data surrounds us, which is the reason we need databases to store it in the best possible way. You can think of a database as an organised set of information where you can find and possibly update items. As companies called for more speed and power, databases became relational with information stored inside tables. Now due to interconnectivity, different people might want to access the same data. It led to what we call distributed databases. But shared databases raised some concerns regarding trust and conflicts.

So what's the Hyperledger is?

Enough with the play of words. In the words of Brian Behlendorf, *"Hyperledger is an open-sourced community of communities to benefit an ecosystem of Hyperledger based solution providers and users focused on blockchain-related use cases that will work across a variety of industrial sectors"*. Quite complicated to comprehend. Isn't it? Let's break it down andfirstly understand what Hyperledger is not. Hyperledger is not a cryptocurrency, neither a blockchain nor a company. It is a hub community comprised of various companies that are working closely to develop blockchain-based applications to satisfy their use-cases. It began in 2015 when companies like IBM, Accenture, etc decided to pool their resources and create open-source blockchain technology for enterprises. Now let's get deeper into Hyperledger. Shall we?

3.1 Hyperledger Philosophy

The modular approach helps developers to explore different components as they develop and to change individual components without affecting the rest of the system. All Hyperledger algorithms, protocols, and cryptography are viewed by security experts, as well as the open source community on a regular basis.
Hyperledger delivers seamless portability among smart contracts and applications across many different blockchain networks.



Hyperledger projects have widespread use cases. I'm going to talk about one of the use cases in the banking sector.

Banking Applying for a Loan

Banks lend only to borrowers who are a good risk. Banks collect detailed personally identifiable information (PII) from everyone who applies for a loan. Retaining PII makes bank a target for hackers. Every new application is accepted with the risk of being tampered or attacked by a hacker.

3.2 : How Hyperledger Indy resolve the problem?

Indy incorporates a strong, distributed ledger-based identity that establishes a global source of truth. Instead of disclosing any PII, applicants can share only information the banks need to make a decision, in a way that guarantees the truth and build confidence in the lender.

3.3 Hyperledger Frameworks

Hyperledger design philosophy encourages the re-use of common building blocks, enables rapid innovation of components, and promotes interoperability between projects.

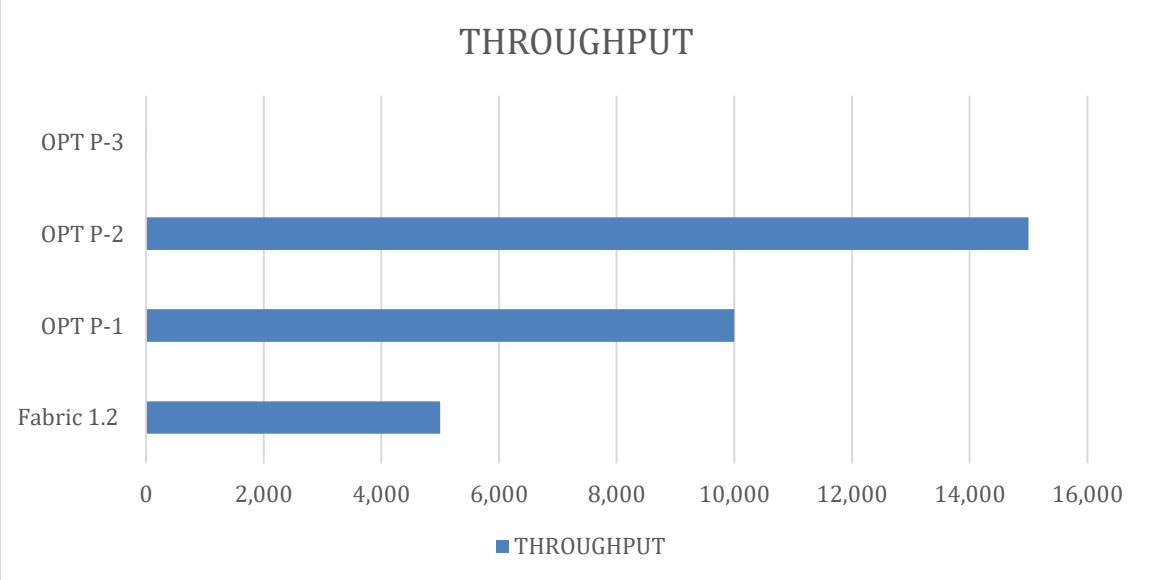
Some of the current Hyperledger Projects are

(a) Hyperledger Burrow
(b) Hyperledger Fabric
(c) Hyperledger Indy
(d) Hyperledger Sawtooth

In this we focus on Hyperledger fabric, it is an enterprise grade project which is an open source platform that is maintained by IBM and Linux Foundation. Unlike the bitcoin and Ethereum, it does not have a cryptocurrency where it is network restricted. The mode of validate transaction and create a block in Hyperledger fabric is PBFT. Transaction is controlled by chain code which consist of program code and has the ability to create and manage the applications and interact with network. The privacy of transaction is maintained by channel. It ensures that data and transaction is between the members of specific organization only. The main component of Hyperledger Fabric architecture are peer nodes, ordering nodes and clients application.

3.4 Hyperledger Growth

A report indicate the performance of hyperledger fabric is at high speed. It is reported that transaction has been done more than 35000 transaction per second with latency less than one second. The performance numbers obtained that hyperledger fabric deployed in a single cloud data center.
Due to its speed, is also called fast fabric.



4. CONCLUSION

The paper represents the study of blockchain, how the use of it increase day by day. Also we study about the project that started by IBM and Linux Foundation. We described the attributes of blockchain like its application and with various consensus algorithms, mixing, digital signatures, encryption, secure multiparty computation and secure verification of smart contacts. We believe that only bitcoin will not on market trend, the applications of blockchain will be on wide range in future. We already found some paper that studied the possibility of using IOT, smart properties in blockchain environment. Taking this in consideration, with it's popularity this technology get adopted by industries and academics, it will generate a significant amount of research.

But, with popularity of blockchain technology, it leads to increase number of users that trigger the number of challenges and limitations. We have to look after the security features for this technology.

We conjecture that with various cryptographic algorithms as well as other security measures will be a key enabling technology in future development of blockchain.

References

[1.] Blockchain In Transaction Management- A Quick Guide

https://www.blockchain-council.org/blockchain/blockchain-in-transaction-management-a-quick-guide/

[2.] Security And Privacy Of Blockchain https://arxiv.org/pdf/1903.07602.pdf

[3.]Comparative Analysis OF Consensus Algorithms https://ieeexplore.ieee.org/abstract/document/8400278

[4.] On Federated Proof Of Validation Based On Consensus Algorithms https://iopscience.iop.org/article/meta

[5.] Hyperledger https://www.hyperledger.org/

[6.] Performance analysis of hyperledger platform fabrics https://www.hindawi.com/journals/scn/2018/3976093/

[7.] Research leading blockchain top cases uses

https://www.ibm.com/blockchain/use-cases/

[8.] Projects of Hyperledger

https://www.hyperledger.org/