

A Systematic Review on Blockchain Technology

Associate Professor and Head Neeraj Prakash Shrivastava, Undergraduate Scholar Vishwaroop Shah

School of Computer Science Engineering and IT
 nprshrivastava80@gmail.com, vishwaroop.shah@gmail.com
 Anand International College of Engineering

Abstract – Blockchain is the emerging technology and is believed to cause disrupt in various field. Although a lot of research is going on in this field but still the blockchain is in its early stage. The distributed ledger and decentralization are the important features of blockchain which ensures data security and privacy. The blockchain have the potential to have a major impact in the various fields like finance, real estate, and music industry but as of now it has played an important role in the cryptocurrency. After going through several standard papers, we have given in here a proper systematic literature of the blockchain technology. In this paper we have discuss about the architecture, categorization, components, consensus algorithms, its features, and various challenges which it faces. We have also given the future directions for the further research in the blockchain technology.

Keywords– Blockchain, cryptocurrency, consensus algorithms, distributed ledger.

I. INTRODUCTION

The Block chain is a chain of blocks in where each block contains a transaction. In the todays scenario whenever we are making any transaction it first has to be verified by a third party then only it gets completed so as to avoid any double spent. If a person A have only \$10, and it gives \$10 to person B and to person C. In order to do so first the third party here the bank first validates the transaction then only it gets completed. In this scenario the bank will abrupt the second transaction as the person A does not have enough funds which he is transferring. This dependency on the third party to validates the transaction can now be removed with the help of blockchain. In a block chain we do not have any third party instead the ledger is known to every node in a network.

In the block chain, all the transaction which are correct gets stored in a block each block is connected to another block. The first block of a chain is called genesis. The advantage is that each block is dependent on the pervious block and each block is cryptographically secured, so if one wants to modify any one block, he first has to modify all the blocks which are present ahead of it and then he can reach that block.

Whenever a new block have to be added it first gets verified and depending upon who is verifying the transaction weather it a private node, public node or a community node.

II. BLOCKCHAIN ARCHITECTURE

In the block chain it consists of the block which contain several transactions and each bock is dependent on the previous block. If the user wants to change a particular transaction, then it first must undo all the transaction till

that block and then it can change the transaction, but it is a computationally infeasible.

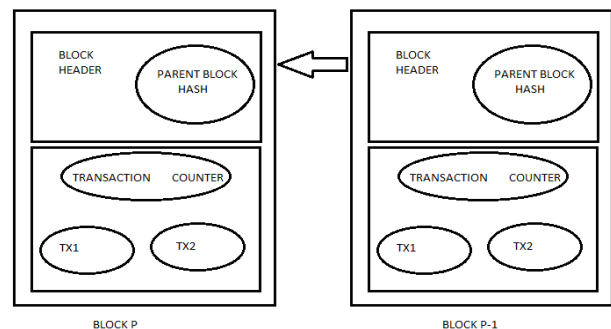


Fig. 1. A series of blocks in a block chain.

In the above diagram we can see that each block is dependent on the previous block and each block contains a number of transactions. In the block chain each node contains the entire list of all the transaction because there is no centralised system so after they approve for a new transaction then only it added up in the block. The first block in the chain is called as Genesis.

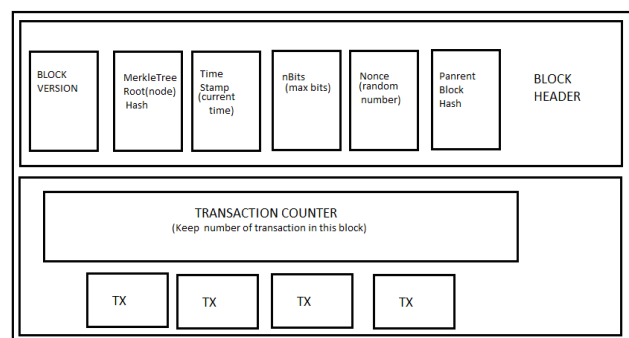


Fig. 2. A structure of a block.

Here in the above diagram we have a block structure which is representing the various components within a block

- **Block Version:** We have already defined a set of protocols and it points out to which set of rules this block is following.
- **Merkle Tree Root:** All the transaction in a node are stored in a Merkle Tree where root node is the starting node and each leaf node represents a transaction it is very effective way to store the transaction.
- **Timestamp:** It represents the current time at which the block was made in seconds.
- **nBits:** It denotes the number of bits which acts as the maximum permissible number of bits for the hash value.
- **Nonce:** It is a number which is used in creating a hash value. It has a greater number of zeros in the starting which makes the computational more difficult to break down.

In the block chain to verify that each block is created by a valid node, the node which created it also append the signature with it using its own private key. The public key of the node is kept in the public domain, so when node wants to authenticate the block it uses the public key if that node and can easily authenticate it.

III. CATEGORIZATION OF BLOCKCHAIN TECHNOLOGY

The blockchain technology can be divided into the following categories:

1. Public Blockchain

In the public blockchain any user can interact with one another. Anyone can buy or sell a coin, yet their identity remains safe. A user does not need any permission. In this it takes time for the consensus and less confidential data is stored on it.

2. Private Blockchain

In the private blockchain only the authorised person can access it which increases the privacy and since there are limited persons there is less effort in the consensus effort. Hyperledger Fabric is an example which is based on private blockchain.

3. Consortium Blockchain

It is based on 'semi-private' and have restriction on the user who can access it but usually works across different organization. In this the companies having similar goals uses this platform, resources to improve workflow, transparency and it also increases accountability.

4. Hybrid Blockchain

A hybrid blockchain combines the benefits of public and private blockchain. In this we have a permissioned blockchain, which means that a layer run on top of the

blockchain network which basically give permissions to the participants who wants to access it. It is restricted yet have the freedom. Some are private yet some are public.

In transaction a problem of double spent arises which means that we are making a same transaction with two different parties. Now the question arises that which one we must be chosen as valid and another one invalid. In the block chain how it deal with this problem is that the entire transaction ledger is shared publicly with all the nodes, so when a new transaction have to be validate a voting system is used where all the nodes participate and if majority of the nodes agree with it then only it gets validated otherwise it is considered as invalid.

IV. CONSENSUS ALGORITHM

Consensus algorithm is mainly used to overcome the Byzantine General Problem. In which when the army have surrounded the entire city then it can only win over it if they all attack on the city at the same time if due to some traitors some part of the army does not attack on them then it will lead to a mission failure. Thus, it is vital for the system to make sure either they want to attack on the city or not. In the case of the blockchain we also have to take a decision weather a transaction has to considered as a valid or not. It means how to make sure that all the untrusty nodes are making up the same decision, thus using various consensus algorithm we can make sure that all the nodes are making the same decision and have the same ledger among all of them.

1. Proof-of-Work

In this algorithm all the nodes create a hash value which is based on a randomly changing nonce and the block header. This value must be less than a threshold value. It requires a lot of resources like electricity, computation power. After a node have created a particular hash value then it must be satisfied by the different nodes, if it gets the green signal then it gets added up to the chain. When two different nodes created the two valid hash values simultaneously then it leads to creating a branch. After some transaction, the one who grows more considered as the main branch and the subbranches are merged into it. To promote the users to do more computational power a reward is given to the nodes who successfully creates a new node and it is called as a Miner.

2. Proof-of-Stake

In this method we have a set of validators. Which makes the decision regarding the block must be consider as valid or not. It uses a voting method which is weighted with their stake. The more a stake of a node have the more priority is given to it. In this method it is believed that the more the stake a person have the less likely it will attack the system. The node in here do not need to do the more computational power instead it needs to prove its stake. It

is kind of a bias method in which the richer gets more priority than the poor. Although it saves a lot of resources.

3. Practical Byzantine Fault Tolerance

It is used to reach to the consensus when some nodes in a system might not send the correct information or are currently not available. A default value is set to those messages which are missing from the node which are down. If out of $2m + 1$ nodes even if 'm' nodes are not working due to some constraint, we can still reach to the consensus that mean two-third nodes have to be vote correctly and remaining one-third is allowed to be faulty.

4. Delegated Proof of Stake

In this method the weight of the votes is assigned according to the stake of the voter. In here we have elected representatives and delegate which carried out the task of validating the transaction. They get elected by the stakeholders and if someone is not working properly then they could easily be replaced. It will be better if we make the base layer using the Proof Of work and then build up the application on top of it using the DPoS, it will lead a very good combination for a certain number of applications.

5. Proof of Capacity

In this consensus method, the more the amount of hard disk you have the more are the chances to mine the new block. In this the reward which a person gets is equivalently to the amount of hard disk a user has. In this we have to store very large files of data items known as plots in the hard disk and the more the number of plots we have the more are the chances of finding the new block.

6. Proof of Activity

The incentives are being given to both the miners and the validators who validated them. In this a user first starts with the Proof of Work approach and if not able to find the new block so then it switches to the Proof of the Stake approach. When all the validators sign the new block then only it gets added into the chain then the reward is the shared between the user and the validator. If the validators are not able to sign it then a new set of validators are chosen, the more the stake a validator have the more the chances of getting selected.

V. FEATURES OF A BLOCKCHAIN

A blockchain is a very powerful technology and have a lot of benefits. Some of the features of the blockchain are as follows:

1. Immunibility

The key features of the block chain is that it is immutable that mean once we have added a transaction then it cannot be modified or deleted because when we are adding a new transaction in a block first we have to take the consensus form the nodes in a network which is done using a particular algorithm then only the transaction is being add

up in the transaction. It is the biggest advantage in the blockchain.

2. Capacity

The block chain has increased the capacity of the network, in the traditional manner the network has dedicated servers but now we have thousands of nodes which are working together although it is in the initial stage but soon it will be going to revolutionize the entire network industry.

3. Security

In here we don't have any centralised system so making any transaction will have to be first consensus by all the nodes then only it can be added up in the transaction. It uses more powerful technique of Cryptography which make the system infeasible to break. On the top of it adds up another security layer of the decentralization which makes the system even more secure. Each node is dependent on the previous on block and each node is cryptographically hashed so when we have to make any modification, we first have to recompute the previous block which makes it computationally infeasible.

4. Anonymity

In the block chain the ledger is in public domain so maintaining the anonymity is a difficult task. In here we use the pseudo-anonymity, which means that we assign a virtual address to each of the node, but it is not related to it physical address or home address. Using the virtual address one node can communicate with the another and in this manner the original identity of the owner is completely hidden.

5. Decentralization

In the traditional banking system where whenever we have to make a new transaction it first has to be get verified by a centralised authority then only it can be considered as a valid transaction but in the blockchain there is no centralised system. All the transaction which have been made up till yet are being shared to every node in a system. Whenever it have to be considered that a new transaction have to be consider as a valid or not so before the validators who are among the nodes , first checks weather it have already occurred or not, if not and the transaction is fine then only it gets considered as valid and adds up in the block .

6. Distributed Ledgers

Since the blockchain does not have any centralised system so the transaction is being shared by each node in a system. It increases the computational power and tracking in the distributed ledger is quite easy in it so creating and malicious activity could easily be filtered out. By distributing the ledger among the nodes, the response time is also greatly improved

VI. TECHNICAL CHALLENGES IN A BLOCKCHAIN

The blockchain have very good benefits like distributed ledger, decentralized system, secure transmission but still there are various challenges which we must face and some of those have been discusses below:

1. Scaling

With the increasing amount of data being produced by the customers, the amount of data stored in a blockchain also increases. This created a problem because the more the amount of data is the more the number of blocks there will be and the more the storage is required at each node because each node contains the list of all the transaction in order to avoid the double-spent scenario. One of the approaches to this problem is to optimize the storage at each node which could be done by storing all the latest transaction and removing the old transaction.

2. Privacy Leakage

Block chain maintains the anonymity by hiding the identity of the user. In this the user uses the cryptographic principle of public key and private key. But the thing is that after each transaction it must be shared among all the different user and it is linked with its public key. In a recent study it has been shown that the user identity is revealed using the transaction details. An approach to this problem is 'Mixing'. In this certain intermediary nodes are used in the transaction so that now the transaction will be first sent to this node and then this will the data to the designated destination. However, this approach also has problem if the middle node becomes corrupt then it could reveal the identity of the users of both the source and the destination.

3. Selfish Mining

In this the group of miners used unfair means. Some of these miners does not tell anybody and keep on mine new block and if only it fulfils some requirement then only it is shared with others. As it is not telling anyone this chain will grows a lot before it is being published publicly, and since it is a longer chain now the users will also add to this chain. That means the honest miners were wasting their resources like computational power, electricity etc. on the branch which is now of no use. Now this is the partiality between the honest and the selfish miners and as a result the selfish miner will earn more.

VII. FUTURE DIRECTIONS

Blockchain have created a lot of interest among the different areas because of the features it is providing and using blockchain a lot of today's market problem could be solved. With this emerging technology it will not only have a major impact on the market but also on ourselves of how we interact with the different commodities around

us. Since nothing is perfect and this technology also have certain ways where we need to innovate new solution.

With the emergence of this technology a lot of different cryptocurrency have also evolved. They promise to give the certain features and performance but the problem which arises here is that how it can be assured that this is an authorized and all the features which it claims also fulfils it. We need a system that can verify that it is correct thus we need a testing mechanism. We have two type of it first one is Standardization phase in which we will describe the standard protocols which it must be fulfilled, and it must be checked at the very beginning phase of it. Another phase is Testing phase, in this we will describe how to test a block in a chain, and it will be kind of application oriented.

The basic principle of the block chain is that it is decentralized and there is no central authority. But if we look at the statistics, we got that the top 5 miners owns more than 51% of the total hash power that is available in the system. We need to innovate in such a way that a fair way must exist between the users.

With the growing demand of the block chain day by day in different application whether it be music or finance industry all of them will be going to use the blockchain. When we are storing huge amount of data in the blockchain then we also need to analyze it because along the blockchain, data science is also emerging at a very fast speed. We need to think of a solution using which we can maintain the huge data in it and can do the analysis part on it efficiently.

VIII. CONCLUSION

In this paper we have given an overall idea of what a block chain is. At the very first we have discussed about the architecture of the block chain, then we have studied the various categories of the block chain then the consensus algorithms what are used to avoid double spending. We have discussed about the distributed ledger in a decentralized environment which increases the security by making the users anonymous. Further-more, we have pointed out the major challenges. We have also discussed about how to optimize the node storage. Block chain is going to create a boom in the market and it on the verge of it.

REFERENCES

- [1]. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", <https://bitcoin.org/bitcoin.pdf>, 1998
- [2]. Zibin Zheng, Shaoran Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", https://www.academia.edu/36208204/An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends

- [3]. L. Venkateswara Kiran, R. Bala Dinakar, P. Siva Prasad,” Blockchain Technology - A Sturdy Protective Shield”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7 Issue-4, November 2018
- [4]. Buterin, “A next-generation smart contract and decentralized application platform,” white paper, 2014
- [5]. Buterin, “On public and private blockchains,” 2015. [Online]. Available: <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>
- [6]. Back, "Hashcash - a denial of service counter-measure," <http://www.hashcash.org/papers/hashcash.pdf>, 2002.
- [7]. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. / Kosba, Ahmed; Miller, Andrew; Shi, Elaine; Wen, Zikai; Papamanthou, Charalampos.
- [8]. NRI: Survey on blockchain technologies and related services. Tech. rep. (2015).
- [9]. Moindrot, O. (2017). Proof of Stake Made Simple with Casper.
- [10].L. Lamport, R. Shostak, and M. Pease, “The byzantine generals problem,” ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.

Neeraj Prakash Shrivastava working as Associate Professor and Head of School at School of Computer Science Engineering and IT - Anand International College of Engineering, Jaipur, Rajasthan, India. Pursued his PhD, he is holding degree of M.tech. & B.E in Computer Engineering, MIE, DBA. He is having 21+ Yrs. Experience in Academia & Industry and has published 14 National & International Publications (Journal & Conferences). Authored 2 Books and granted 2 Projects from Department of Science and Technology.

Vishwaroop Shah is undergraduate scholar pursuing his final semester of engineering in computer science from Anand International College of Engineering, Jaipur, which is affiliated to Rajasthan Technical University, Kota India.