Pandemic Protocol for Broadcasting in Blockchain

R Shanmuga priya
Department of Information Technology
Madras Institute of Technology,
Anna University
Chennai 600044, India
shanmurajendran2@gmail.com

R Anirudh
Department of Information Technology
Madras Institute of Technology,
Anna University
Chennai 600044, India
anirudhramesh2002@gmail.com

Abstract

In the evolution of technology, the Web 3.0 has become the future of the technological world. The web 3.0, which is still evolving, aims in creating an immersive environment which contains smart applications supported by Artificial Intelligence and aims in decentralization of data. In the upcoming era, the successor of today's transactions is most likely to be the transactions through cryptocurrency, which is built on top of the blockchain technology. It is important to make the upcoming technology more reliable, secure and fast to bring it to real-time use. In order to overcome the low throughput and high latency of broadcasting in blockchain technology this paper comes up with the pandemic protocol for broadcasting. It is a communication protocol used for broadcasting which works on the principle of how the pandemic Covid-19 spread. The implementation of this protocol in the blockchain technology to broadcast the transactions can make the technology more efficient and faster.

Keywords: Web3.0, Decentralization, Transaction, Cryptocurrency, Blockchain, pandemic protocol

I. INTRODUCTION

From read-only web to the internet era, now we step into a new world of web technology, the Web 3.0.The goals of web 3.0 are, to create an immersive world by the development of Augmented Reality and Virtual Reality AR/VR, to bring a revolution in web technologies through Artificial Intelligence and Machine Learning to create adaptive and intelligent applications and to decentralize the data by developing dApps (decentralized apps). The decentralization is done through the blockchain technology or peer-to-peer network. The decentralized environment is free from the control in a single hand. In blockchain, these systems or nodes are taken as immutable ledgers or blocks which are connected through a cryptographic system. The main advantage in the network is that it's highly secured and the tampered data is easily traceable. This makes blockchain technology used in cryptocurrency transactions. The use of the pandemic protocol can help to make the transactions much faster.

II. RESEARCH CHALLENGES

As the web3.0 is still a developing process, there are many doors to be opened in this field. Blockchain and cryptocurrencies are still new technologies in the field and needs more explorations. The main thing about making cryptocurrency into real-time transaction is mainly based on how people are going to trust the technology. The Technology has to be top most secured and should be fast even when many users on to it at the same time. The security is ensured by hashing and the proof-of-work done by the miners. This pandemic protocol can help to make the process faster by broadcasting the transaction to all the nodes of the chain like how the pandemic Covid-19 spread. One more challenge ahead was that the protocol is derived from the gossip protocol which has high latency.

III. RELATED WORK

The Blockchain network is a revolutionary concept which could change the fate of transactions and currency. Today there are over 20,000 cryptocurrencies which are currently available in the market. This growing technology could replace the currency transactions in the near future. The technology is still under development. Transactions through cryptocurrency are done by adding a new block created for a specific transaction between to the blockchain using the address of the blocks. To get a clear understanding of the implementation of the pandemic protocol we must first understand few concepts.

A. Blockchain Network

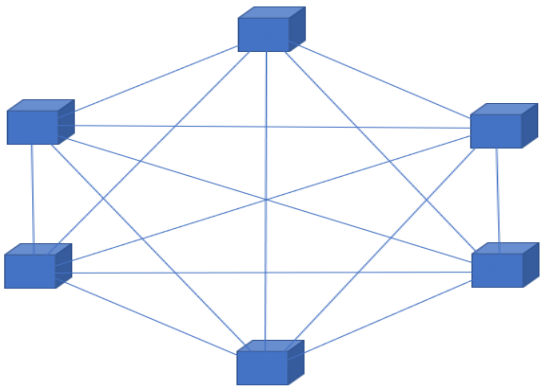

Fig.1 Blockchain network

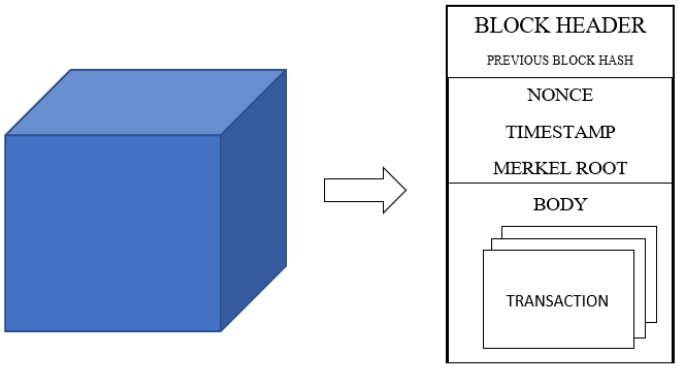

Fig.2 Block structure diagram

Blockchain network is a network which maintains distributed ledgers of the completed transactions as blocks and chains them sequentially using the previous block hash, which is stored in the block header, to maintain the order of transactions, hence modifying the blockchain. Nodes in a blockchain are connected to each other by peer-to-peer (P2P) network.

.

In blockchain, the identity of the blocks is secured through two types of cryptographic keys – Private key and a Public key. The private key is the digital signature of the node which proves the ownership of the cryptocurrency belonging to the node whereas the public key allows you to receive the transactions. The private key and the public keys are generated by the miners using the nonce, timestamp and the merkel root. These generated keys needs to be validated and accepted by the other nodes. To accept that the new block which is going to be added to the blockchain can be trusted, the nodes come under a common agreement which is called the consensus protocol. One of the most popular consensus protocol is the Proof-of-work (PoW).

After validating a block, the node is broadcasted to the rest of the network. The time it takes to broadcast the block depends on many factors, such as the size of a block, the average bandwidth of the nodes, and the maximum hop count or diameter of a network. When the number of nodes in the network is high, the network diameter increases which in turn increases a block broadcast time. Also, when the block size is high, the broadcasting time of block increases which could make the chance of undesirable forks.

B. Transaction of cryptocurrency

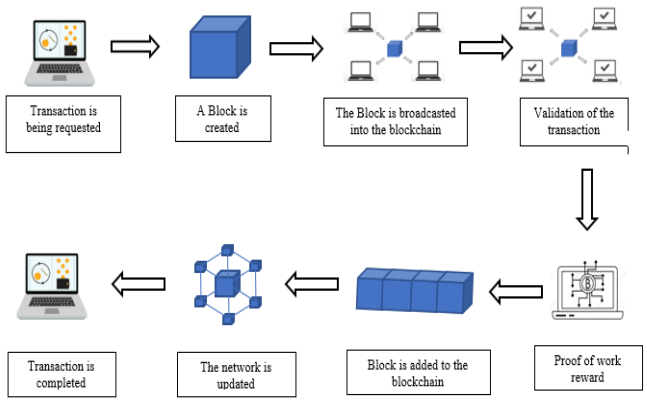

Fig.3 Flow diagram of a crypto transaction

The transaction of a cryptocurrency is a sequence of many processes. To understand how the transaction takes place, we must know the fundamentals of a blockchain. The first step of a cryptocurrency transaction is to initiate a transaction by knowing the receiver's address which is the public key of the receiver node. The most important fact is that the transactions are irreversible and immutable. Once a transaction is made it cannot be undone. So the receivers public key must be given properly to make a successful transaction. On initiating a transaction, a block is created by the miners. The miners are responsible for creating a new block and maintaining it. The miner comes out with the two hashes for the block. Every block which is a part of the blockchain will have the copy of the past transactions with them. The miners generate a hash value which is accepted based on the consensus protocol and the validation of transaction is done. When 51% of the nodes come under the consensus and accept the node, it is said to be validated. The miners are given the reward for mining and the block is added to the blockchain. This updated chain message is broadcasted to every node in the chain.

This makes the transaction decentralized as all the nodes are informed about the additions of blocks. If there is any tampering with the data it can be easily backtracked and found using this blockchain network. This makes the transaction more reliable.

C. The understanding of the Pandemic Protocol

The Covid-19 or the Corona Virus pandemic is an ongoing global pandemic which terrorizes every human being around the world. The main reason for this impact is the high transmission rate of this virus. The virus effectively broadcasts itself making it highly scalable and affected all parts of the world. This idea can be used to broadcast the updated chain messages in the growing blockchain technology. This can be taken as a improvised version of gossip protocol which works on the principle of how rumour spreads. The gossip protocol can as such be used but due to the inefficiency of keeping track of already updated nodes it is propagated again to the same nodes which increases the latency and reduces the throughput of the block. From the keen observations of covid-19, Once a person gets Covid they tend to get immune to the virus and develops immunity and d has less risk of getting the corona virus again. Using this idea we can use a specific data structure which can mark the already visited nodes as they are already updated. This way, we can create a list from which the sender node can choose nodes to broadcast the message.

The effiency of the transmission can be increased by the use of an additional data structure which contains the list of unattended nodes. This data structure must contain the block information and a specified list of all the previous nodes. This list can be created by the following method.

1. Take two lists - an empty list (L_e) and a list of all nodes present in the chain (L_f).
2. Take the orgin node and choose the neighbouring nodes to broadcast the block present in L_f.
3. Add these nodes to the empty list L_e.
4. Now remove the elements present in L_e from L_f..
5. Next take the neighbouring node as the orgin/broadcasting node and repeat the process.

Lets take an example for 6 nodes

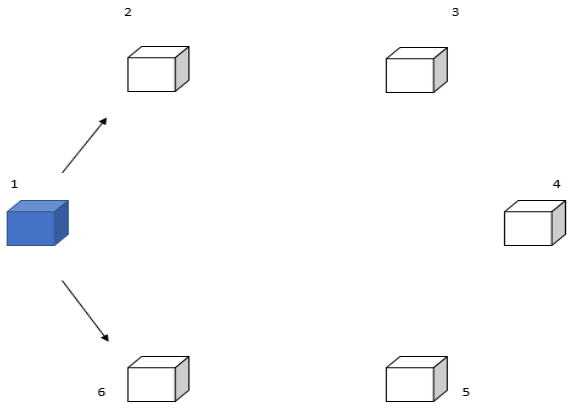

Fig.3 First broadcast graph

L_{f1} = [1,2,3,4,5,6]

L_{e1} = [1,2,5]

Now as the nodes 1 ,2 and 6 are updated

Broadcasting is done from node 2 and 6.

For node 2,

$L_{f2} = L_{f1} - L_{e1}$

$L_{f2} = [3,4,5]$

For node 6,

$L_{f6} = L_{f1} - L_{e1}$

$L_{f6} = [3,4,5]$

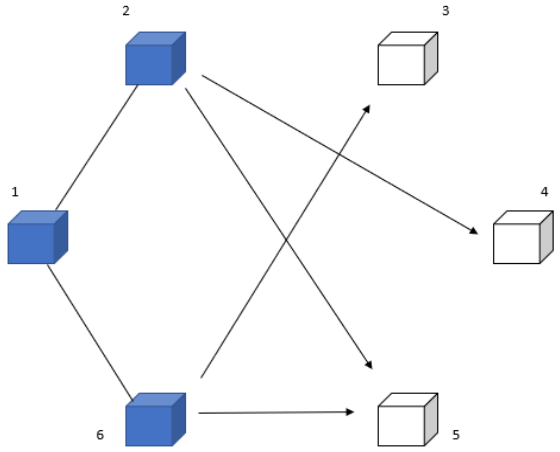

Fig.4 Second broadcast graph

Now as the nodes all the nodes are updated.

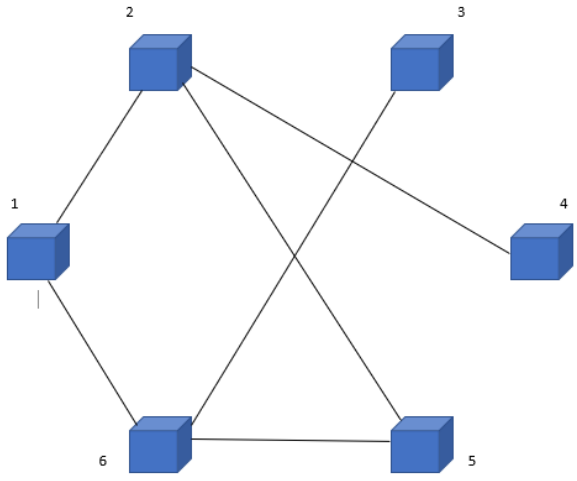

Fig.5 Third broadcast graph

For the Third broadcast the $L_f = [\ ]$ is empty and it shows that all the nodes are updated.

Using this protocol, we can broadcast more efficiently and this can reduce the latency and increase the throughput of the broadcast.

IV. CONCLUSION AND FUTURE WORKS

Ideated from the pandemic covid-19, This protocol can be used to broadcast the messages and updates in the blockchain transaction. This can be used to make the broadcasting highly scalable and much faster. In future, this can be tested on a large real time much complex network and can be fine-tuned. In this protocol the block header can be broadcasted and the hashes can be validated. This enables the miners to have the hashes validated faster reducing the time taken by the transaction to be completed.

REFERENCES

[1] S. Dos Santos, C. Chukwuocha, S. Kamali and R. K. Thulasiram, "An Efficient Miner Strategy for Selecting Cryptocurrency Transactions," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019,

[2] "IEEE Standard for General Requirements for Cryptocurrency Exchanges," in IEEE Std 2140.1-2020 , vol., no., pp.1-18, 4 Nov. 2020,

[3] A. NugrahaTama, H. Kusuma Wardana and S. Nugroho, "Gossip Algorithm Implementation for Network Protocol," 2018 International Seminar on Application for Technology of Information and Communication, Semarang, Indonesia, 2018,

[4] K. Ayinala, B. -Y. Choi and S. Song, "PiChu: Accelerating Block Broadcasting in Blockchain Networks with Pipelining and Chunking," 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, 2020,.

[5] X. He, Y. Cui and Y. Jiang, "An Improved Gossip Algorithm Based on Semi-Distributed Blockchain Network," 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Guilin, China, 2019,.

[6] A. J. Ganesh, A. M. Kermarrec and M. Laurent, “Peerto-peer membership management for gossip-based protocols,” IEEE Transactions, 2003, pp. 139-149

[7] H. A. Harutyunyan and W. Wang, "Broadcasting Algorithm Via Shortest Paths," *2010 IEEE 16th International Conference on Parallel and Distributed Systems*, Shanghai, China, 2010,

[8] A. J. Ganesh, A. M. Kermarrec and M. Laurent, “Peerto-peer membership management for gossip-based protocols,” IEEE Transactions, 2003, pp. 139-149..

[9] J. Kan, L. Zou, B. Liu, and X. Huang, “Boost blockchain broadcast propagation with tree routing,” CoRR, vol. abs/1810.12795, 2018. [Online].Available: http://arxiv.org/abs/1810.12795.

[10] N. T. J. Bailey, “The Mathematical Theory of Infectious Diseases and Its Applications(second edition),” Hafner Press, 1975

[11] D.Y.T.Chino,L.P.S.Avalhais,J.F.Rodrigues,and A. J. M. Traina, “BoWFire: Detection of fire in stillimages by integrating pixel color and texture analysis”,in Proc. 28th SIBGRAPI Conf. Graph. Patterns Images,2015,pp.95–102.

[12] F. M. Beni and I. Podnar arko, “Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph,” Vienna, 2018, pp. 1569-1570..