Designing Optimized Scalable Framework for Block Chain Based Applications

Prince Arora[1], Ajay Shriram Kushwaha[2], Girish Kumar[3]

School of Computer Science & Engineering,
Lovely Professional University, Phagwara, Punjab, India.

Abstract:-

In this modern Information Technology World, it is hard to store transactions in a centralized storage way, then the blockchain technology comes into existence, it provides a peer to peer connection and stores the data into a decentralized format. A lot of crypto currencies comes into existence when it comes to blockchain that transaction is possible without third party involvement.

Research Gaps in the Area of Blockchain

The blockchain technology is capable of load balancing of the transactions of the network whereas in centralized transaction,banks or the government bodies hold all the transactions which is a typical task to manage in the cases of power failure or any other issue.Blockchain technology promotes the management of load properly using the concept of crypto currencies.Various hashing algorithms are used in order to maintain the uniqueness of every transaction done.The next level of blockchain would be implement faster algorithms for the hashing so that the basic transactions can also be done with the cryptocurrencies. In the Proposed Research work, we have proposed integrated model using blockchain that supports scalability so that if any block is to added in the chain, it can be easily done.The main issues that are resolved by the framework is that the security of the block is retained through various algorithms so that the data can be transmitted easily from one block to the other block and the integrity of the data can be maintained.

1.Methodology for optimizing block constructions

In this case, we select a master phase to construct the block directly, build and broadcast to all other nodes for verification. Unnecessary calculations can be avoided and it improves the system transaction speed.

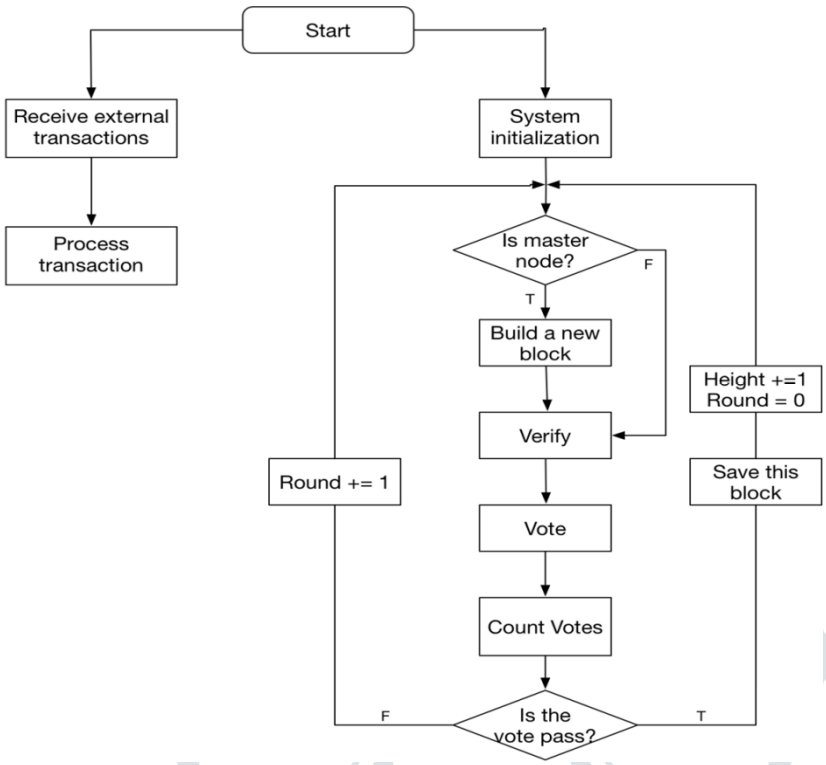

Fig :1

Each node will calculate the master node of current round by calculating hash(height+round)%nodecount, where height is the height of the current blockchain (the total number of blocks), round is the number of the current round (round is initially 0), nodecount is the number of nodes in the private blockchain system. If the node is not the master node, it will enter the waiting state, and wait for the completion of the master node to build blocks and broadcast.

When the master node has completely built a block and broadcasted it, the other nodes receive the block and start to verify its correctness, and then will vote for operation, if the vote is completed after the block does not pass, even more than one third of the nodes vote against this node, then this round needs to re-select the master node, both need to re-through the formula

hash(height+round)%nodecount

to calculate a new master node. At this point, the height variable does not change, only the value of the round plus one operation. After we get a new master node serial number, we then repeat the above block flow process, remind that the new faster than 2/3 of the node recognition will enter the next round of building blocks, both increase the value of the height variable Height + l

2.Optimized scheduling of transaction in blockchain

In the block construction, we designed the following strategies to control the block size and time, the block

size control operations are as follows:

- Set the maximum number of transactions. The maximum number of transactions can trigger the build operation. Otherwise, the system enters the waiting state, and the waiting time is 200 seconds. And set a counter to record the number of times the system waits.
- Set the minimum number of transactions. If the system waits several times but still does not reach the upper limit, but the number of waiting times reaches the limit
- (5 in our current configuration). A build operation is triggered only if the system waits for more than 1 second and the number of transactions still not exceeds the limit and the number of transactions must be at least above the lower limit.

The sample of pseudo-code is shown below:.

1.Begin
2.var<-0
3.While true
4.IF(var>5and transaction count>1)or transaction-count>max_limit)Then
5.Break;
6Else then.
7.var<-var+1
8.sleep(100ms)
9.propose block()
10.END

3.Evaluation of proposed model

The transaction s are done in such a way that if that the throughput of the algorithm is decreased. Say, the minimum time for each transaction is set to 5ms and maximum time is set to 10ms.No transaction can take more than 10ms.

This is the way in which the optimization of the algorithm can be achieved.Limits are set so that the wait time of the algorithm doesnot exceed the described time.

Scope of the study:

The scope of the framework is to make it scalable and robust.By implementing this,a lot of modifications can be done in an easy way so that adding on one device will not be an issue.Since the framework and logic has

been developed so that the security and integrity of the system can be maintained by using the proposed model where transaction can be done

References:-

1. Wenting Li,Alsssandro Sforzin,Sergey Fedorov,Ghassan O Karame, “Towards scalable and private industrial blockchainsm", ACM Workshop on Blockchain, Cryptocurrencies and Contracts, BCC 2017 - Abu Dhabi, United Arab Emirates
2. Enabling Blockchain Innovations with Pegged Sidechains Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille
3. Hashcash - A Denial of Service Counter-Measure Adam Back, https://blockchain.news/Post?id=Hashcash---A-Denial-of-Service-Counter-Measure
4. Blockchain for the internet of things-Present and Future, thttp://www.cypherspace.org/hashcash/.
5. Blockchain meets IOT-An architecture for scalable access management in IOT, IEEE Internet of Things Journal (Volume: 5 , Issue: 2 , April 2018)
6. The quest of scalable blockchain fabric: Proof-of-work vs. BFT replication, International Workshop on Open Problems in Network Security, May,2016.