ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Analysis of Blockchain Algorithms

Vikas Narkhede[1], Satpalsing D. Rajput[2]

PG CSE Student, Department of Computer Engineering, SSBT's COET Bambhori, Maharashtra, India[1]

Assistant Professor, Department of Computer Engineering, SSBT's COET Bambhori, Maharashtra, India[2]

ABSTRACT: A blockchain is a sequence of block that utilize to appropriate trust records over the network also valid transaction and transaction made securely because of the fact that every block has its own hash and previous block hash it doesn't any change or alter its hash. It is distributed control or managing .In this network main role has consensus algorithm maintaining the secure and efficient of blockchain. when new block is added to blockchain trust that is agreed by all the nodes in blockchain. In this paper to study different types of consensus algorithm and it principals.

KEYWORDS: Blockchain, proof of work , proof of stake ,proof of burn, merkle root.

I. INTRODUCTION

Blockchain is a chain of blocks it contain the information. It's nothing but a timestamp digital document. blockchain is a distributed ledger which completely opens to any one In this the data has been recorded inside a blockchain it becomes very difficult to change it. In Bitcoin blockchain network the each block contain previous block, time stamp, nonce and a merkle root. The Blockchain should be work on the basis that each block has Data, hash of the block and hash of previous block. blockchain stores the transaction which stores in the forma of Sender receive and that amount to be send. A block itself has hash which calculate the value based on the Data inside the block means change inside the hash reflects on change in the hash value. hash is unique identification to detect the block [1]. This hash is no longer of the block means its change as the Data updated in block then change the hash.the third element of the block is previous hash value which effectively creates the block. If chain of three block present then it has hash and hash of the previous block. means eventually last block point to block two and block to points block one. If the first block newly created then its denoted as genesis block. If we change the middle block then its hash value get change so for auditing purpose the last block which points to previous block not match the hash value. it means someone tampered the hash or data and that transaction permanently suspended for future use[1]. here to calculate a single hash is not to check the validity of block but its check thousands of block.

II. CONSENSUS ALGORITHMS

In this section shows the algorithm mechanism and steps.

1. PROOF OF WORK

The proof of Work mechanism a slow and study in bitcoin it requires approximately ten minutes to calculate ach block. it requires P2P network if someone join to this network if someone create a block then it sends to everybody in the network. each node verify the block to make sure each block. All the nodes that consensus to check which block is valid. to successfully tampered the block chain means legitimate intruder to change all the block in the network. this Consensus algorithm use to select the next block generation.

In Blockchain if there will be new block then who is responsible to add the block in blockchain so first prerequisite is to verify the transaction which is quite easy but who will add this block in a blockchain so it is important for us that node should not be legitimate node because it can alter the data. If in blockchain to change nth block then it change the hash of all the remaining block then recalculculate hash of remaining block.for validating the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

block it has some miner process which provide the puzzle and require a largest difficulty factor to avoid legitimate attack [2]. So the following miner process to avoid the attacks.

1.1. MINER PROCESS

Step 1:Start

Step 2:Pending transaction place in a block

Step 3: Solve the puzzle

Step 4:Brodcast the Solution into network

Step 5: If Solution Match

Step 6: Then Repeate Step 8 to 9

Step 8: Miners receives the reward

Step 9:Successfully Mined Block add as a new block

Step 10: Else reject transaction

Step 11:Stop

1.2. PUZZLE SOLVING STEPS

The Miner require some basic Information for header i.e Blockchain version, Previous hash, merkle root, timestamp, Difficulty target and nonce. here miners take all this stuff and then he hashes to twice then it followed with challenge string that time network gives some difficulty factor which is puzzle to find the combination to take your challenge string with that add any number which rear with nonce since here challenge tree is nothing but hash or header that OR with nonce or number that should number with prefix of so many zeros then the difficulty factor is more and then broadcast it. here the nonce

2. PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)

There must be atleast 3m+1 processors to deal with F faults.atleast require 2F+1 Communication path and In order to find out the traitors exchanging the messages in agroup F+1 round of message must be exchanged.ti find out the faults[3].

Step 1: Start

Step 2: Configuration of replicas is M=3F+1

Step3:Each replica starts with same initial state

step 4:the state of each replica includes the state of service,message log and view number

Step 4:Stop

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

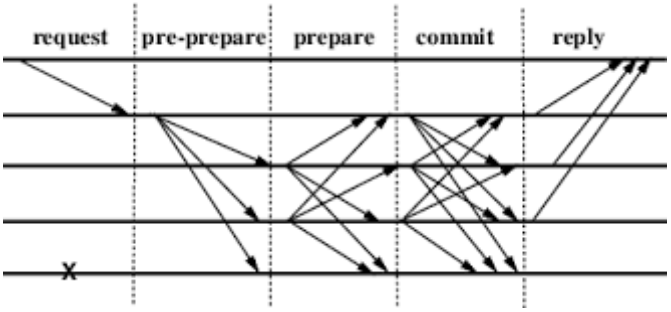
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

2.1. NORMAL CASE OPERATION



Normal Case operation

Pre-prepare :Acknowledge a unique sequence number for the request.Purpose: acknowledge a unique sequence number for the request

SEND:The primary assigns the request a sequence number and broadcasts this to all replicas

A backup will ACCEPT the message

IF d,v,n are Valid

(v,n) has not been processed before for another digest (d)

Prepare:The replicas agree on this sequence number.Purpose: The replicas agree on this sequence number.After backup i accepts <PRE-PREPARE> message

SEND:multicast a <PREPARE> message acknowledging n, d, i and v

A replica will ACCEPT the message if

d,v,n are valid

Commit:Establish total order across views.Purpose: Establish total order across views

Once prepared(m,v,n,i) = T for a replica i

Send:multicast <COMMIT> message to all replicas.

All replicas ACCEPT the message if d,v,n are valid

3. PROOF OF STAKE

Proof of stake is Consensus algorithm which launch in 2011 to solve blockchain problem in algorithm, this process is simply pseudo random election process. to select the node of validator of next block it will includes Staking age,randomization and the nodes wealth it contain block forging.Cryptocurrency used proof of stake[2].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

3.1. Coin-age based selection

A proof of Stake system Combines randomization based upon calculating Coin age.This algorithm basically depends upon the multiplication of number of coins with number of days since n is number of coins and m is multiplier and d is number of days then coin age Ca =nm *d.

Step 1 :Start
Step 2: if coins spent <30 days
Step 3: Then BEGIN next block
Step 4:IF coins_set>Probability of Next block
Step 5: Where Probability to find next block limit goto step 8 to Step 9
Step 6: Then Stake used to Sign a Block where coin_age==0
Step 7:ELSE Wait(30 days)
Step 8: if next_block limit==90 days
Step 9: Then Accomodate Old and Large blocks
Step 10:Stop

This process secures the network and gradually produces new coins over time without consuming significant computational power

3.2. Random block Selection

The best validator is nothing but the less computational time for verification so that can be chosen based on Combination of lowest hash value and Highest Stake

RB=Lowest Hash value*Highest stake

4. PROOF OF BURN

proof of Burn is a method of Distributed Consensus it is an alternative to proof of work and proof of Stake. It can also be used for bootstrapping one cryptocurrency with other.All proof of burn cryptocurrencies work by burning proof of worked mined cryptocurrencies.So the ultimate source of scarcity remains the proof of work mine.A specific portion of coins in circulation sent to a wallet no one has access it[5].This effectively eliminates these coins from being spendeble although they will still be a part of all of the existing coins ever to be generated.the advantage of this is very low energy consumption, No need to invest in powerful hardware, lesser artificial price swing beacause of the mining hardware investment cycle or the influence of multiloops

5. PROOF OF CAPACITY

Proof of Capacity (POC) is consensus algorithm has been around since 2014,Which act as base protocol of Burst Blockchain.The miners used a difficult factor with large number of nonce which requires the large amount of space [6].This technique Given that the operation of hard disks requires considerably less energy (5–10 W), the processing on one transaction on the Burst blockchain uses less electricity than the processing of one Bitcoin transaction by several orders of magnitude (~100.000).

III. MERKLE ROOT

Merkle root are the part of blockchain technology. Merkle trees are produce by repeatedly hashing pairs of nodes until there is only one hash left. This hashis called Merkle root. All transaction in a block by producing a hash of set of transaction in merkle tree. Each leaf node contain hash of transaction data.(tx0,tx1,tx2,tx3....). Merkle tree provide integrity and validating of data[8].

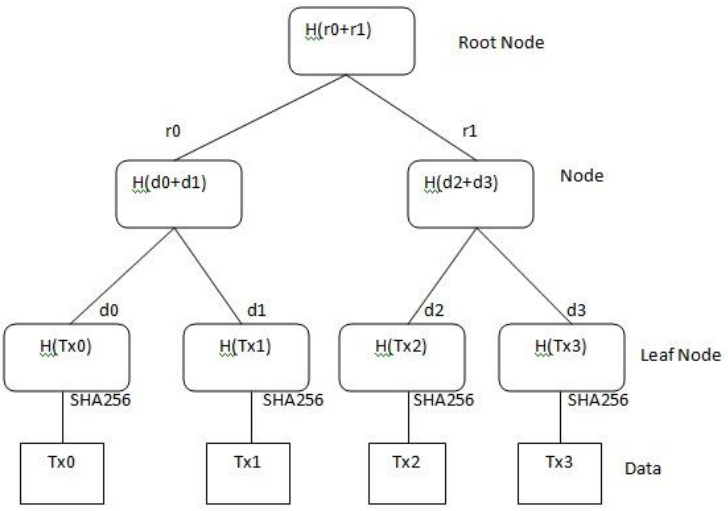
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020



Merkle Tree

A Merkle tree is a tree structure in which each leaf is a hash of a block of data and each non-leaf node is its children. This generate a single hash called merkle root. It every node has two children this called the binary hash tree. A merkle tree has the number of leaves is always 2^n.
Where the n is 0,1,2,3..... every node has 0 or 2 children all the leaves are same level.
Total leaves l = (N+1)/2
Total Nodes N = 2l-1
And level are $\log_2(l)+2$
Using a Merkle tree can significantly reduce the amount of data that a trusted authority has to maintain for verification purposes. It separates the validation of the data from the data itself.

IV. CONCLUSION

We have study the Consensus algorithm provides security of the blockchain system. In this paper we discuss and analysis of various different types of consensus algorithm. Proof of work required more computation calculation and power. proof of stake, creating a new block using deterministic way. Proof of burn consensus algorithm less power consumption and Merkle tree provide integrity and validating of data. In this way study of consensus algorithm.

REFERENCES

[1] S.S.N.L Priyanka, A. Nagaratnam " Blockchain Evolution - A Survey Paper" IJSRSET vol. 4 pp. 27-30, 2018.
[2] Giang-Truong Nguyen, Kyungbaek Kim " A Survey about Consensus Algorithms Used in Blockchain" ,Journal of Information Processing System. Vol.14, No.1, pp.101~128, 2018
[3] Wenbo Wang, Dinh Thai Hoang, Zehui Xiong, Dusit Niyato, Ping Wang, Peizhao Hu, and Yonggang Wen " A Survey on Consensus Mechanisms and Mining management in Blockchain Network",arXiv, 2018
[4] Lakshmi Siva Sankar, Sindhu M., M. Sethumadhavan, "Survey of Consensus Protocols on Blockchain Applications".,IEEE 2017
[5] Karim Sultan, Umar Ruhi1 and Rubina Lakhani "Conceptualizing Blockchain : Characteristics and Application.",Researchgate, pp49-57.,2018
[6] Jake Frankenfield "Proof of Capacity (Cryptocurrency)" https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp 2018
[7] Jia Kan,Kyeong Soo Kim "MTFS: Merkle-Tree-Based File System". IEEE,pp.43-47,2019
[8] Raasi Manasa Annavajjala, Vijay Anand " Partition based Hash tree -An Efficient Certificate Revocation System" IEEE pp 551-556, 2017.
[9] Brihat Sharma,Chandra N Sekharan, Fanyu Zuo " Merkle-Tree Based Approach for Ensuring Integrity of Electronic Medical Records" ,IEEE pp 983-987, 2018.