A survey on various techniques and proposals for improving the cryptocurrency protocol

Dr Geetha J, Raviteja Jagadish, Sri Venkatesh, Varun BV, Nitesh Kumar J

Department Of Computer Science and Engineering Ramaiah Institute of Technology
Bangalore, India
geetha@msrit.edu, varunbeekanvk@gmail.com, srivenkatesh1999@gmail.com,
ja.raviteja.11@gmail.com , niteshsingh2097@gmail.com

Abstract

It is the time where the cryptocurrencies are gaining more and more attention among many individuals and company, Because they have some advantages over centralised currency system, like they are scarce, divisible, transportabile, durable, counterfeitable, there are a variety of cryptocurrencies, and a number of protocols which lie behind the working of these coins, with blockchain and cryptography as the underlying technology and concepts, but there are many advantages and disadvantages of each protocols, and the factors which are taken into account are privacy, scalability , efficiency , anonymity, efficiency, speed of transaction, security. These factors are very crucial and necessary in deciding the choice of cryptography protocol, in this paper we summarize the various protocols and its features and techniques which govern the working of various cryptocurrencies**.**

Keywords*: bitcoins, cryptocurrencies, blockchain, digital signatures, security*.

1. INTRODUCTION

Proof of work: [1] explains this protocol where the computation work done is considered as a proof to add valid transactions into the block, nodes also called miners competent with each other to solve the mathematical problem using computation power, and the first who solves with the most computation power is considered as the best trusted miner, and he receives a reward, POW also checks double spending , coins which use Proof of work as underlying technology is litecoin and ethereum, advantages of pow is that finding solution for the math problem is hard, but verification is easy, it is the oldest protocol used, there are few disadvantages of this protocol, it is vulnerable to 51% attack, also the electricity consumption for mining is very large, hence leaving a lot of carbon footprint.

Proof of stake: [2] explains that Unlike proof of work, in proof of stake the node which will mine the next, is chosen based on its stake in the network, stake here means number of coins it has, but there is a problem , what if the same miner keeps getting more stake and always gets

selected next, to counter this problem several methods are proposed, select nodes in random based on highest stake and lowest hash value, but in this method we can predict the next node because the stake is present in public, another method is that the next node is selected based on how long a node has held its stake, there are many advantages of this protocol, the electricity consumption is greatly reduced, it is environmental friendly, it also allows mass participation of miners, in the network, also reduces stress on the nodes in network it is secure against 51% attack, disadvantage is that the node with highest stake can have influence on the network.

Delegated Proof of Stake: this is a little different from Proof of stake, here [3] tells that they try to improve the scalability and productivity by reducing the number of nodes which does validation, the nodes which are called validators are selected by means of voting, this way the strain on the network is reduced, nodes which owns token are eligible to vote, the weightage of votes is based on their stakes in the network, there is also one more mechanism where the tokens can be transferred to another node in the network, here the voters can vote for witness and also vote for delegates if they find out there is any kind of malicious activities happening, by this way we can use the word democracy and equal weightage to poor and rich nodes, advantages are it uses less computational power and are much more scalable, equal opportunities to all, and offers digital democracy. Disadvantages are it is vulnerable to 51% attack since a small number of nodes are responsible for validation.

Proof of Elapsed Time: PoET was developed in 2016, by intel as mentioned in [4], it uses less computer resources, since there is not much computation required, the main idea in this protocol is that at every node there is a timer which decides whether the node is going to participate in mining the block or not.
But before this elapsed time which decides the node takes place, there is a protocol called Software guarded extension, which acts as the verifier and does the attestation, it protects the code and secures it from outside interaction, it makes sure the nodes download the correct code and also attest it , and generates a pair of security keys, the nodes signs and forwards this signed attestation, the advantage of this protocol is that it uses a random timer which chooses the next miner to add a new block, those no high computation work is needed and improves efficiency. It has no scalability issues and can manage a huge number of participants, since the next block leader is chosen at random there can't be any bias in selecting the same node as the leader again and again. The disadvantage is that the SGX software is a third party and is against the basic law of blockchain.

Practical Byzantine Fault Tolerance: Byzantine fault tolerance means even though there are faulty or malicious nodes in the network, the distributed system still reaches the consensus this skill of the distributed network is called the Byzantine fault tolerance, In [5] the practical Byzantine fault tolerance, is used as giving an immunity against these faults due to the malicious nodes in the network also called traitors, to provide the immunity against this fault, all the honest nodes, come together and make sure all the messages are valid and coming from a specific node, this is doen ins sequentially arranging the node and selecting one node as the leader and other nodes as backup nodes, also the condition assumed is that the fault nodes

cant exceed one third the population of honest nodes, or equal to one third, the advantages of this protocol is that there is much less power consumed, transaction finality is achieved with less number of confirmation unlike POW, the disadvantage of this protocol is that it is prone to sybil attack,and is not a much scalable protocol.

Proof of Authority: In [6], In this system of protocol, a group of nodes or individual users who wish to become authorities have to go through a strict selection, also it should be equally likely for all the long term committed nodes to be the validators or the authorities , those who wish to be at the authority position will have to reveal all the information such has their holdings and stakes to the public, also the number of such authority nodes must be small, of course this looks like decentralised system so the POA is applicable in only small private network rather than in public chains or networks. There are various advantages of this protocols are, unlike Proof of work , the proof of authority uses less computational power and hence dont require more intense resources, it is not vulnerable to 51% attack, the rate of validation of a block is faster in POA algorithm, the disadvantages of this protocol are this algorithm is more like centralized than a decentralized network hence is more scalable, also all the information of the validators is seen by everyone, this is also one of the major problem, any other outside competitors might interfere and make the validators act dishonestly.

Leased Proof of Stake (LPoS): [7] explains that this protocol is similar to proof of stake with a slight change, here the stakeholders can lease or we can call as “recruit” other small miners to mine a full node or a part of the node and get a percentage of reward, this allows the stakeholders to get rewarded without mining, this concept of leasing is the major concept of this protocol, This LpoS is done on WAVES platform, where the token holders can lease tokens for the wave nodes, due to this protocol we can have advantages like other miners get a chance to mine, whereas in POS the main disadvantage is the same high stake holder repeatedly getting a chance, LPoS consumes less energy and are faster, since less number of nodes are required for validating and also lease process can be done with a small computational capability device hence saving energy, due to the distribution of work, it enhances the security of distributed network. Since LPoS is a new technology there are many disadvantages and attacks on this. One being the repeating getting of chance to mine.

Proof of Importance (PoI): [8] tells that unlike proof of work and proof of stake where the miners or nodes are given the chance to mine based on the computation power they have or based on the amount of cryptocurrency they hold also know as stake, so this is a clear picture of biased decentralised working nature, hence in 2015 an foundation called NEM.io introduced proof of importance, in the proof of importance to overcome this partiality the nodes which have a history of more transactions and is active in the network, and using many such factors like the amount of money vested, net transfers, cluster activity, , they give each node a importance score, based on these score, they are given the chance to mine, this also encourages more use of cryptocurrency and hence makes it more fungible in the future.

Proof of Activity: Proof of Activity [9] is attempting to combine the best aspects of proof of work [3] and proof of stake[4] . In this mechanism initially the protocol follows the proof of work concept to create a block to be added next, in this step miners have to compete using their computation power, and for an attack to take place, any single entity should have more than 51% of the computation power. Now after this initial stage they we make use of the PoS concept to select the next miners, as described in the PoS, the next miner is chosen based on his stake , here stake means the number of coins that node holds, but to avoid the same node being chosen again and again, they use a random selection process, which is a part of PoS protocol. So the first step PoW is used to find a block, the second step PoS protocol is used to validate or sign a block, Since this protocol uses PoS and PoW , it is very difficult for anyone to attack since the attacker should have both properties such as, more than 51% of the computation power and more than 51% of the stake, which is nearly impossible to have. The disadvantage of this protocol is that it still needs lot of computation power for mining, since it uses PoW

Proof of Capacity:
This protocol was created to counter the energy considerations of PoW and hoarding of coins in the PoS protocol, in this protocol as explained in [10] the miners in the network are allowed to use their own computer hardware to store the possible solutions values, so that they can match later with the hash value required, its similar to a lottery winner, if a person can collect or have as many as lottery tickets his probability of winning will be more, of course here the miner with a lot of harddrive size will be a dominant one, but unlike the GPU it doesn't consume as much as energy and don't produce much heat, thus makes this protocol much more greener than POS and PoW, the examples of where PoC is used are Storj, Burst, Chia, and SpaceMint. Basically this protocol has 2 steps namely plotting where the set of all possible nonce values are plotted and the next step is the mining part.

Proof of Burn:
In [11] the Proof of Burn is an alternative consensus algorithm with minimal energy consumption, compared to other proof such as PoW . On proof of burn, the coins are burned in the process by sending the coins to an eater address. It uses virtual mining rigs to validate transactions, miners initiate coin burns as a way to show their participation in the network and be allowed to mine. The more coins burned by the miner, the bigger their virtual mining rig will be. The eater address is a verifiable un-spendable address, which does not consume many resources and ensures the network is active. The proof of burn also prevents early participants from gaining unfair advantage by periodic burning of cryptocurrency coins. This ensures the network is agile and participants are rewarded fairly.

Proof of weight:
This protocol works with almost similar concept of the PoS as discussed earlier, but there are various other changes and additional data which has been taken into consideration and not just the amount of tokens a node has, to choose it as the miner of the next block. In this protocol , weight is assigned to a randomly selected group of nodes , For example In the Filecoin ,weight is based on the interplanetary file system data stored among the nodes.The advantage of this protocol is that is it customizable , and can be made scalable , the random group of nodes in the

network which are selected run a consensus algorithm while obeying the rules of decentralization and security, but the only disadvantage of this protocol is that it is very difficult to make users use this protocol since there is no incentives given for any work done here.

Table 1: Shows the applications of various protocols which are used.

Sl No:	Protocol	Applications
1	Proof of work	Bitcoin, Litecoin, ethereum
2	Proof of Stake	ShadowCash, Qora, Black coin, peer coin, ethereum 2.0, Nxt
3	Delegated Proof of Stake	BitShares, STeem, STeemit, EOSIO
4	Proof of Elapsed Time	Hyperledger, sawtooth
5	Practical Byanzitine Fault tolerance	Zilliqa, Ripple, Hyperledger fabric
6	Proof of Authority	Aura, clique, microsoft azure
7	Leased proof of Stake	Waves Platform
8	Proof of Importance	NEM
9	Proof of Activity	Decred espers
10	Proof of capacity	Storj, burst, chia, spacemint
11	Proof of burn	Slim coin, TG coin, Bootstrapping auxiliary currency
12	Proof of weight	File coin

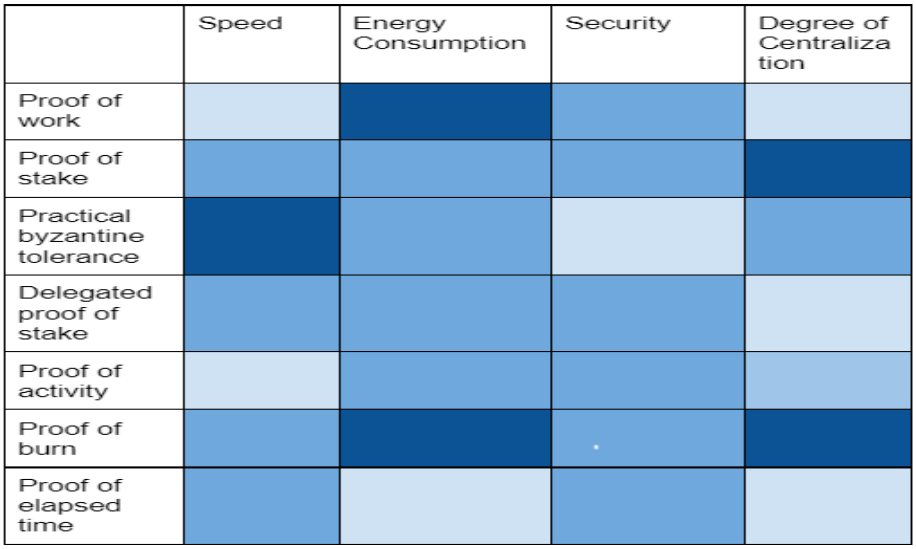

Figure 1: Shows the comparison of protocols wrt various parameters.

LESS
MORE

Future Work:
The next upcoming work, is implement a new protocol by making use of the extensive literature survey done on many protocols, and capturing the advantages of the existing protocols, which can be more secure, scalable, environmentally friendly, faster and fungible, The goal is to make use of crypto currency as a normal mode of transactions to transfer assets , similar to an UPI for daily goods and services.

Conclusion:
Though there are various upcoming protocols for the cryptocurrency mining , we have discussed some of the most important protocols used in the cryptocurrency, and also have discussed its applications in various different crypto coins ,its related issues, advantages and its features. This paper helps in understanding the basic working or the glimpse of each protocol used in the cryptocurrency. Each protocol has its own tradeoffs and we cannot conclude which has the best protocol but there are hybrid protocols like Proof of activity which takes the advantages of both POS and POW protocols.

References:
[1] M. Andreas, Mastering Bitcoin: Unlocking Digital Crypto- currencies, O'Reilly Media, Inc., London, UK, 2014.
[2] A. Kiayias, A. Russell, B. David, and O. Roman, "Ouroboros: a provably secure proof-of-stake blockchain protocol," 2017.
[3] K. Qin and A. Gervais, An Overview of Blockchain Scalability, Interoperability and Sustainability, Hochschule Luzern Imperial College London Liquidity Network, New York, NY, USA, 2018.
[4]A. Corso, "Performance analysis of proof-of-elapsed-time consensus in the sawtooth blockchain framework," 2019.
[5] M. Castro and B. Liskov, "Practical byzantine fault tolerance," OSDI, vol. 99, pp. 173–186, 1999.
[6] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," Future Generation Computer Systems, vol. 107, pp. 841–853, 2020.
[7] X. Liu, G. Zhao, X. Wang et al., "Mdp-based quantitative analysis framework for proof of authority," 2019.
[8] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, ''On blockchain and its integration with IoT. Challenges and opportunities,'' Futur. Gener. Comput. Syst., vol. 88, pp. 173–190, Nov. 2018
[9] NEM Foundation. (Feb. 23, 2018). NEM: Technical Reference. Accessed: Jul. 14, 2018. [Online]. Available: https://nem.io/wpcontent/themes/nem/files/NEM_techRef.pdf
[10] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, ''Proof of activity: Extending bitcoin's proof of work via proof of stake,'' IACR Cryptol. ePrint Arch., vol. 452, no. 3, pp. 1–19, 2014
[11] S. Gauld, F. Von Ancoina, and R. Stadler, ''The burst dymaxion an arbitrary scalable, energy efficient and anonymous transaction network based on colored tangles,'' in Proc. CryptoGuru PoC SIG, 2017
[12] F. Tschorsch and B. Scheuermann, ''Bitcoin and beyond: A technical survey on decentralized digital currencies,'' IEEE Commun. Surveys Tuts., vol. 18, no. , pp. 2084–2123, 3rd Quart., 2016
[13] CoinCodex. *coincodex.com.* https://coincodex.com/article/2617/what-is-proof-of-weight