Comparison Between PoW and PoS Systems Of Cryptocurrency

Mohammad A. AlAhmad, Abdullah Al-Saleh, Fahad A. AlMasoud
Public Authority for Applied Education and Training, College of Basic Education, Computer Science Department, Kuwait City, Kuwait

Article Info

Article history:

Received Dec 29, 2017
Revised Feb 21, 2018
Accepted Mar 11, 2018

Keywords:

Centrilized
Cryptocurrency
Decentrilized
Proof of stake
Proof of work

ABSTRACT

Cryptocurrency subject attracted so many people for the last eight years around the globe. Satoshi's Nakamoto's, the founder of the bitcoin cryptocurrency behind this revolutionary change in digital money market. Bitcoin cryptocurrency uses "Power of Work" or simply PoW system as its mining algorithm. But in January of 2016, Ethereum cryptocurrency has launched which adopted a new system called "Power of Stake" or simply PoS that is used in Ethereum as its mining algorithm. This paper explores and compares PoW and PoS systems that is used widely today in cryptocurrencies digital money, concluding the pros and cons for each system with enabling to decide which one is more suitable and stable in digital money market.

Corresponding Author:

Mohammad A. AlAhmad,
Public Authority for Applied Education and Training,
College of Basic Education, Computer Science Department,
Kuwait City, Kuwait
Email: malahmads@yahoo.com

1. INTRODUCTION

Cryptocurrency is a type of electronic currency that can be employed to exchange goods directly between two parties within peer-to-peer network without any trusted third party or median achieving authenticity and integrity. Thus, with this trend, cryptocurrency is intended to replace traditional dealing with currency for exchanging goods or commodities in E-Commerce era.

The data transmission is in the form of transactions, which includes contracts, records, encryption algorithms and other correlated information. Every block consists of a set of transactions that resides in each network's node where the verification process of those transactions is done. Then those blocks are collected in blockchain, the repository database in each computer's participant. The block structure consists of three fields: linker hash to link to a previous block, time print and data [1], resulting in long encrypted linked blockchains that is permanent and unalterable.

Recent researches in this field had led into two cryptocurrency methods that are widely in use today are Bitcoin (BTC) and Ethereum (ETH). Conceptually, BTC and ETH are agreed, both they use blockchain techniques, however, they differ in the approach. The BTC follows the Proof of Work (PoW), while ETH follows the Proof of Stake (PoS). "Proof of Work" or (PoW) idea was initially conceived and delivered in 1999 [2]. Proof of Work (POW) scheme is a technique used for proving the correctness done by previous transactions to prevent any threats or attacks on networks through requesting confirmation from the initiator. This POW concept had been known before Satoshi Nakamoto [4] came out with this idea; there some articles discussed the concept such as the one presented by Cynthia Dwork and Moni Naor in a 1993 journal article [3]. Therefore, the Proof of work concept existed even before bitcoin, but - the invertor of BTC - applied this technique to himself/herself/ or themselves "by a providing false name to individual or group calling himself/herself or themselves Satoshi Nakamoto (Nakamoto, 2008).” Digital or electronic currency is reshaping the way traditional transactions are dealt with. As a matter of fact, the main idea behind the bitcoin is the Proof of Work, which was presented in a paper by Nakamoto’s that was published back in 2008, in the context of this paper; it provides confidence and accord delivery work together. Confidence and accord delivery system means that money can be transferred electronically with immediate effect and confidentiality between any two parties only, using the existing infrastructure. In the other hand, using traditional methods of payment such as Visa, Masercard, PayPal, etc., a third party is required to complete your transaction. The role of the third partiers is to control their data by maintaining transactions history and balances of each account. We shall illustrate behaviors of BTC when using PoW to better understand the concept: if A represents the first party, sent B which represents the second party $100, then C represents approved third-party would deduct A’s and add B’s, so both (A and B) have to trust C (third-party) when doing the requested transaction. However, with bitcoin (which uses PoW), every participant has a copy of all verified transactions, therefore there is no need for third parties to get involved, because direct verification is obtainable. In proof of stake (PoS) system (or protocol, or function) the details for transactions validation are quite different from those used in PoW. The concept of PoS is the same as of the PoW; however, the approach is different. Proof of stake or PoS, first idea was in conference in 2011 called bitcointalk, and PP-coin was the first digital currency used in 2012, [5].

2. RESEARCH METHOD

2.1 POW in More Details

Satoshi Nakamoto [4] introduced coins electronically as a sequence of digital signatures. The flow of those coins takes off from the owner to the next by digitally assigning a hash of the previous transaction and the public key of the next owner to the end of the coin, and then a payee can review the signatures to verify the chain of ownership as Figure-1 shown below.

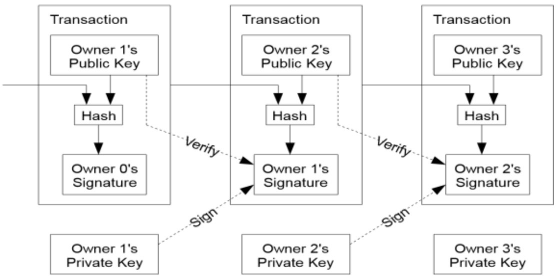

Figure1. Transactions signed digitally [4]

When the payee can't verify a double-spend of the coin if happened, Approved Central Authority, or (ACA for short), will be added, and therefore, once a transaction is completed, each coin has to return back to the ACA. Then the ACA will issue a new one to ensure no double-spent will happen. The problem with this solution is that the whole money system is centralized running the ACA, with every transaction having to go through it. So what is needed is a non-central point of failure system to notify the payee that earlier transactions had not been signed. What needed is the earliest transaction, which is the one that counts only. In the central-based model, it was aware of all transactions and decided which arrived first. Therefore we will adopt a mint-based model, free from any trusted party. To accomplish this, all transactions should be known to all, with a single ordered history of transactions that all participants to agree on. That is, each transaction must be stamped at its arrival time and agreed by most of nodes it was the first. The solution we propose includes a server, which works by taking a hash of a block of items to be timestamped and widely publishing the hash, like when we do in a public announcement. The timestamp will prove that the data must be existed at the time, in order to get into the hash, and also will include the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it as Figure 2 shown below [4].

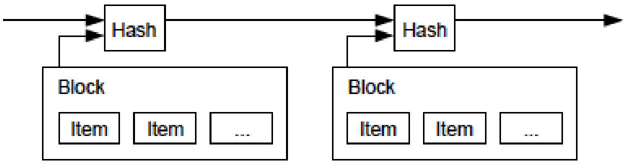

Figure 2. Timestamping each block in its hash [4]

In order to implement accord timestamp server on a peer-to-peer basis, Satoshi Nakamato [4] uses a proof- of-work system similar to Adam Back's Hashcash [7]. Proof-of-work involves scanning for a value that is hashed with leading zero. The work required in an average is rapidly growing in the number of zero bits required and can be verified by executing a single hash. For Satoshiís timestamp network, he/she implemented the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block is unalterable unless redoing the work. As work progress blocks are chained after it, thus to change the block would require redoing all the blocks after it as Figure-3 shown below [4].

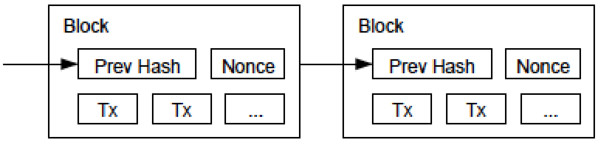

Figure 3. Blocks are chained together forming blockchain [4]

The proof-of-work also solves the problem of determining representation in majority decision-making. One-IP-address-one-vote is not an optimal solution; anyone could allocate many IPs. So, proof-of-work is essentially one-CPU-one-vote. The longest chain represents the majority decision, which has the greatest proof-of-work effort, invested in it and this is found in the honest nodes, which control a majority of CPU power and will grow the fastest and outpace any competing chains. It would require doing the proof-of-work of the block and all blocks after again when any attempt to change a completed block, and then violate the honest nodes. Alternatively, to avoid any hardware overrun, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

Moreover, mining process is needed to create new group of secured transactions on blockchain. So to define an expensive computer calculation, PoW is a required. Mining technique has two roles:

1. Transaction legitimacy verification/avoiding double spending.
2. Digital currencies creation by rewarding miners.

The following will happen when setting a transaction:

1. Every set of transactions bundled into a block;
2. Miners will verify the legitimation of those transactions;
3. To do so, miners will deal with PoW problems;
4. The first miner who solves each block problems will be awarded;
5. Transactions will be stored in the public blockchain, whenever they are verified.

Asymmetry cryptography: (for ex. RSA) is a key feature of proof-of-work problem. Reasonably, it is easy to check for the network, however it is difficult on the receiver side. This scheme is also known as a CPU effort function. Miners in a network will compete to be the first to solve the PoW, and this would require a lot of attempts. Ultimately, if the right solution were found, an announcement would be made to the whole network instantly by the winner miner who will receive a cryptocurrency reward provided by the protocol. Technically, mining process is a technique opposite to hashing: it determines a number, which is less than a given threshold produced by the cryptographic hash algorithm of block data. The competitive nature of mining process is measured by a threshold parameter. When this this parameter increases, the average number of calculations needed to create a new block will increase, resulting in increasing the cost of block creation. This will motivate miners to improve the efficiency of their mining systems to maintain a positive economic balance. Around 14 days, an update should be done to threshold parameter, and every 10 minutes a new block is generated. Many other blockchains use PoW, not only the bitcoin blockchain [6].

2.2 POS in More Details

PoS is a proof of currency ownership. So when its owner consumes a coin, this can be considered as form of proof-of-stake. Every coin has a life span called age. Each node via a hashing scheme generates the age of the coin within proof-of-stake.

The implementation of proof-of-stake can be done via two common proposals; one of them currently working in practice is PPCoin (Peer-to-Peer Coin) created by Sunny King [8]. This design works by showing the capability of future peer-to-peer crypto-currencies independent from consuming any energy.

PPCoins proof of stake algorithm works in the following manner: As soon as a block of PoS is created, a miner will construct a coin stake transaction in order to send some money in their hand to themselves with predefined reward. Based on the following parameters: transaction input, some additional fixed data, and the current time (as an integer representing the number of seconds since Jan 1, 1970), the SHA256 hash is calculated. Then the calculated hash is checked against a proof of work requirement, much like Bitcoin, except one different issue that is this hash figure is inversely proportional to the coin age of the transaction input. When currency amount factor multiplied by the holding period factor, this is what we call the coin age. Hash is basically depends on time and static data, so doing extra work will not make hashes quickly. Each PPCoin transaction output could generate a correct work proportional to its age and the quantity of PPCoins it contains. The mining power of every PPCoin goes up in straight line over time but resets to zero whenever it finds a valid block.

To prevent miners from re-using their coins multiple times, coin age is used since coin age has unalterable data such as holding period. PoS picks a PPCoin up randomly every second, so it gives its owner the right to create a block. There is a complex debate in coin age’s favor, that is, the longer you fail to create a block; your chance of success will go up. Miners can expect to create blocks more regularly, reducing the incentive to lower the risk by creating the equivalent of centralized mining pools [9].

Etheruem is the other proposal of Power of Stake, which is designed by Vitalik Buterin and intended to function as decentralized system in terms of networking such Internet and applications. All systems that support this Etheruem functionality aren’t free. So, networks that need to run an application or program have to pay for unique piece of code. Etheruem classified as a digital carrier. It is well known that cash does direct transaction process between two parties without a third party, so does Etheruem. The Etheruem has some good featurs that makes it an attractive cryptocurrency PoS system: it supports the decentralized applications; in the economic side, the cost of running a transaction is reasonable comparing it to other solutions in the cryptocurrency world, its capital assets is solid and consolidated with 21 million bitcoins, it has good announcements and distribution (users in a 2014 crowdfunding campaign purchased 60m), good researches and development to improve the underlying technology.

The following are some statistical data about the productions & services by Ethereum system: Five Ethereum (ETH) are allotted to the miners that verify transactions on the network every 12 seconds. Every year, 18m Ethereum are mined at most. Five Ether are created roughly every 12 seconds, whenever a miner discovers a block, or a bundle of transactions. So, based on the above statistical information, it is obvious that no one knows the total number of Ethereum yet, and the pace of Ethereum creation will be less clear after 2017 when Ethereum plans to move to a new proof-of-stake harmony algorithm. Consequently, this will probably lead to a change in the rules of Ethereum creation, and thus the mining subsidy might decrease [10].

2.3 Comparison between POW and POS

While there are countless aspects to this debate, in my view, it all boils down to two things: security and economics. Conceptually both agreed to achieve consensus, however, they differ in the approach, that is, the methodology each of them follows.

Will PoW be considered scalable in terms of mining & reliability (i.e. security) while maintaining cost? What about the same for PoS? Of course growing up needs more resources and thus more cost to improve the tools such as the security? How attractive will one system be, versus the other? It's useful to pause here and ask what mechanism Bitcoin uses to achieve consensus.

Table 1. Describes PoW and PoS functionality

System Function	PoW	PoS
Mine	The probability of mining block depends on how much work is done by the miner	Person can mine depends on how many coins he/she holds
51% Attack	Less incentive to avoid 51% attack	51% attack is more expensive
Energy	High consuming	Less Consuming
Centralized vs Decentralized	Have very powerful mining communities which tends to become centralized over time	Need to grow its mining communities to keep the decentralized network
Block target time	Generate every 10	Generate every 15 sec

It'Bitcoin makes it very expensive to amass a majority of the hashing power. This does provide a level of security: A lone hacker will have no chances to gather the mining power necessary to disrupt the Bitcoin network. But there are also disadvantages. The first is economic: Most of the value of newly mined Bitcoins flows out of the ecosystem into purchasing hardware and power. We pay for this with Bitcoin's inflation, and it is not farfetched to attribute much of the price decline this year to the inflation rate. It is true that the inflation rate will decrease over time, and if Bitcoin succeeds, the adoption rate will far outpace the inflation rate. Moreover, sometimes the inflation rate cannot be decreased due to unavoidable circumstances such as wars, natural disasters, political conflicts, etc. But this only gives rise to another question: Will a decreasing mining reward provide sufficient security? The second problem is that mining introduces risk factors that cannot be controlled because they are not parameters of Bitcoin itself. Just imagine that, due to some technology breakthrough, one manufacturer is able to produce ASICS (Application Specific Integrated Circuits) at one-tenth the cost of their competitors. Wouldn't this present a huge security risk for Bitcoin? PoS aims to address these issues and improve on Bitcoin by using the coins themselves, instead of hashing power, as the scarce resource to achieve consensus. With PoW, an attacker has to either purchase lots of hashing power, or at least obtain control over it; for example, by bribing mining pool operators. The design of PoS reduced some of the concerns of Bitcoin's 51% assumption in regard to the system security. That is, the system is considered secured when a minimum of 51% and above of good nodes takes over network mining power. When this is achieved, this will make the cost of controlling significant stake might be higher than the cost of acquiring significant mining power, which will result in making the cost of attacking the system much higher. Moreover, attacker's coin age is consumed during the attack, which may render it more difficult for the attacker to continue preventing transactions from controlling mining power. So any attempt of attack would drive up the price dramatically and make it prohibitive. Imagine what would happen to the Bitcoin price if someone tried to buy 7 million coins. There is also an economic advantage to PoS.

Transaction fees and a possible block reward can be paid to the coin holders so that there is no monetary dilution. No money has to flow out of the system to buy external resources that provide security, and that could be great for the price of the currency [11]. Table 1 below compares the PoW and PoS systems with respect to their main functionality.

3. CONCLUSION

Lately, PoW and PoS systems attracted so many people around the globe. Every system of PoW and PoS has its own cons and pros. In my point of view, the original idea behind Satoshi Nakamoto invention is to construct a decentralized network, which eliminates banks and governments role and regulation obligations towards their clients. PoW and PoS systems provided a peer to peer network with no third party in between. Table1 shows a scary fact that might become real, since PoW is a system that is growing very fast, its decentralized network might become a centralized one since one or two people might own the network coins, for ex, banks. However, PoS system has a decentralized network despite of the number of miners.

REFERENCES

[1] Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press. ISBN 978-0-691-17169-2.G. Bertoni, J. Daemen, M. Peeters, and

[2] Jakobsson, Markus; Juels, Ari (1999). "Proofs of Work and Bread Pudding Protocols". Communications and Multimedia Security. Kluwer Academic Publishers: 258–272.

[3] Dwork, Cynthia; Naor, Moni (1993). "Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology". *CRYPTO'92: Lecture Notes in Computer Science No. 740*. Springer: 139–147.

[4] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
[5] Grinberg, R. (2012). Bitcoin: An innovative alternative digital currency. Hastings Sci. & Tech. LJ, 4, 159.
[6] Blockgeeks, blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/.
[7] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.
[8] King, S. (2013). Primecoin: Cryptocurrency with prime number proof-of-work. July 7th.
[9] Buterin, Vitalik, “What Proof of Stake Is And Why It Matters.” *Bitcoin Magazine, Bitcoin Magazine*, 26 Aug. 2013, bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463/.
[10] Alyssa Hertig. “What Is Ether?” CoinDesk, 21 Apr. 2017, www.coindesk.com/information/what-is-ether-ethereum-cryptocurrency/.
[11] Crane, Fabian Brian. “Proof of Work, Proof of Stake and the Consensus Debate.” *Cointelegraph*, 20 Dec. 2014, cointelegraph.com/news/proof-of-work-proof-of-stake-and-the-consensus-debate.
[12] Alahmad, M. A., I. Al-shaikhli, et al. (2013). “Jouxmulticollisions attack in sponge construction”. *The 6th International Conference on Security of Information and Networks (SIN), 2013 6th International Conference on, ACM.*
[13] AlAhmad, M. A., & Alshaikhli, I. F. (2013). Broad view of cryptographic hash functions. *International Journal of Computer Science Issues*, 10(4), 239-246.
[14] S. Wu, D. Feng, W. Wu, J. Guo, L. Dong, and J. Zou. “(Pseudo) preimage attack on round-reduced Grøstl hash function and others.” In Canteaut [9], pages 127–145.
[15] Wang, Xiaoyun, Hongbo Yu, and Yiqun Lisa Yin. "Efficient collision search attacks on SHA-0." *Advances in Cryptology–CRYPTO 2005*. Springer Berlin Heidelberg, 2005.
[16] Nandi, M. and S. Paul (2010). "Speeding up the wide-pipe: Secure and fast hashing." *Progress in Cryptology-INDOCRYPT*, 2010: 144-162.
[17] Eli Biham and Orr Dunkelman, "A Framework for Iterative Hash Functions - HAIFA," *Cryptology ePrint Archive*, 2007. [Online].http://eprint.iacr.org/2007/278.

BIOGRAPHIES OF AUTHORS

Mohammad Abdulateef AlAhmad received his bachelor degree in computer engineering from university of the pacific in 2002, his master in computer engineering from Gulf University in Bahrain in 2011, and his PhD degree in computer science from international Islamic University Malaysia (IIUM) in 2015. His research area is information security, which focuses on cryptographic algorithms and protocols. My favorite specific research topics are designing and analysis of hash functions, cryptocurrency and cryptography in general. My favorite hash functions are Gear, Double A and Titanium cryptographic hash functions.

Abdullah Nazeeh Saleh received his bachelor degree in Education, Computer from Public Authority for Applied Education and Training – PAAET, Kuwait State in 2016. He is a Master degree student, Computer Science – International Islamic University of Malaysia, IIUM and working for Bank Boubyan – Kuwait as I.T. Service Desk Engineer. Abdullah is interested in cryptography researching, developing and has published papers on cryptography topics.

Fahad Abdulaziz AlMasoud received his Bachelor degree in Computer Engineering from university of the pacific in Stockton, CA, USA 1984, his Master in Computer Engineering from Kuwait University in Kuwait in 1999, and he is currently PhD candidae in computer science from international Islamic University Malaysia (IIUM) in 2017. His research area is information security, which focuses on cryptocurrency, cryptographic algorithms and protocols. Another interested research topics are analysis of rliable multicast protocols, design and implement mobile computing protocols.