IJCCN International Journal of Computing & Communication Networks

Vol. 2, Issue 1, February 2020

Blockchain Consensuses Algorithms based on Proof of Work: A Comparative Analysis

Amal Alrashid Mohamed[1] and Ashraf Osman Ibrahim[1,2]

[1] Faculty of computer science, Future University, Khartoum, Sudan

[2] Faculty of computer Science and Information Technology, Alzaiem Alazhari University, Khartoum North 13311, Sudan

** Corresponding Author:* Amooly5151@gmail.com, ashrafosman2@gmail.com

Received 30 December 2019; Revised 25 January 2020; Accepted 5 February 2020; Published 24 April 2020

Abstract: This paper presents the comparison of the alternatives that are either hybrid with the proof of work or work as the same way as it. The algorithms that satisfies these criteria was proof of capacity, proof of activity, and trinity consensus algorithm. The research is conducted to specify which consensus algorithm has provided a better enhancement for the limitations of proof of work consensus algorithm. Current investigation focused on the enhancements in energy and electricity consumption, possibility of majority attack, and the efficiency of the cryptographic algorithm within each of the selected consensus algorithm. Comparison results show that trinity consensus algorithm which has achieved 25.01% better hardware energy consumption, and better scalability by 400% bigger block size, 128571.4% more transaction rate, instant block and transaction times, and 33.3% less confirmations. While having the maximum costs of maintaining the majority of the network resources but it recorded the lowest efficiency of encryption algorithm of 527ms run time, 76.4 CPU utilization, and 4.357 memory utilization. From the given results we can conclude that the trinity consensus algorithm is a great alternative that could enhance the Proof of Work Blockchain limitations impressively, and it could one day dominate the world of Blockchain as more efficient alternative to Proof of work.

Keywords: *Blockchain, Consensus algorithms, Proof of work, Proof of work alternatives*

1. Introduction

Blockchain is widely known as the technology behind bitcoin crypto-coin [1]. The Blockchain concept is proposed by Satoshi Nakamoto [2] and has sparked controversy in the world and considered as a distributed ledger. This technology uses Peer-to-Peer (P2P) networking architecture where computers are connected with equal permissions and responsibilities (in case of public Blockchain); all the machines connected to the network are equal (peers) and that means that any computer in the network can act as a client or server. This situation eliminates the need for a trusted third party by using cryptographic proof instead of trust [3, 4]. This method of work avoids the problem of a single point of failure. Consensus algorithms in Blockchain are those algorithms that aim to allow all the nodes in the network to reach an agreement about the current state of the chain, since the appearance of the Blockchain concept many consensus algorithms which found following different protocols to organize the Blockchain and its participants. The first and most widely known consensus algorithm is the proof of work, this consensus algorithm allows a participant of a group to exploit their computational power to solve a mathematical puzzle with a difficulty level that varies according to the overall hashing power in the network. The proof of work has faced some limitations such as the massive amount of energy consumption due to its requirements of specialized hardware, its lack of ability to scale and its ability to handle a limited amount of transaction per second, and its vulnerability to the majority attacks. These limitations may in the future jeopardize its security, so in this paper, we are investigating the alternative Blockchain consensus algorithms that are based upon the Proof of Work. Another major take back is due to the reward halving ongoing in the proof of work Blockchains such as Bitcoin someday reaches the point of relying on transaction fees only which reduces the ratio of investment reward so that it will be useless to spend a huge amount of money on a Blockchain that won’t reward me enough to cover my loss, as a result of a major part of the participants in the Blockchain leave to reduce the total hashing power that is protecting the proof of work Blockchain and making it vulnerable.

This paper is organized as follows: Section 2 provides a background about the consensus algorithms under investigation briefly, Section 3 discusses the steps taken to implement the research, Section 4 displays the data collected from the main network of a crypto-coin representative for each algorithm under investigation, Section 5 shows the results of the comparison and discussion, finally, the limitations that affected the research addressed in this paper and recommendation for enhancement are discussed.

2. Research background

a. Proof of work

The Proof of Work (PoW) algorithm is used to achieve consensus, where all nodes have to solve a cryptographic puzzle [5]. This is easy to verify but extremely expensive to solve because difficulty increases over time, and the first node which solves this puzzle and the other miners agree on the validity of the block [6]. These coins are assured to go to the right miner via the public address they provide, the miner signs the coins with its corresponding private key, this assures that only the correct miner can spend their earned coins [7].

b. Proof of activity

The Proof of Activity (PoA) is proposed by Bentov, et al. [8] to mitigate some threats from the POW algorithm by combining it with proof of stake. PoA starts to work as same as a PoW where the miners compete to create a block where the difference is that in the case of the PoA, the created block does not contain any transaction, it has only the header and the mining reward address. Then the Proof of Stake (PoS) [9] role emerges, based on the header details where a random group of validating miners are selected to sign the block. Once the block is signed it gains the complete status, gets identified, and added to the chain where the transactions are added to it. The mining reward is split between the miners and various validators.

c. Proof of capacity

Proof of Capacity (PoC) is miners in the network which utilize the free space in their hard drive to mine the free coins. POC provides decentralization of storage. However, the actual mining is done similarly to that of PoW. One major difference is a result of the hashing algorithm Shabal-256 which is slow compared to SHA-256 used in PoW. Hashing data repeatedly including the miner account; instead of doing a lot of work for block verification in real-time. The work is done beforehand where you have to generate a number of nonce, each nonce contains 8192 hash value organized in pairs called scoops, each scoop is numbered from 0 to 4095. This process is known as plotting. In the next step, the mining starts the miner which calculates a scoop number and uses the data of the scoop to calculate a deadline, the deadline represents the amount of time in seconds which is spent since the last block is forged. If no other miner could achieve a less deadline the miner gets to add the block to the chain and receive the reward [10].

d. Trinity consensus algorithm

As discussed in white paper [11], it must be noted first that the blocks in the Blockchain are based on trinity vary in size, between 4KBs and 4MBs. In Trinity consensus algorithm, the transactions are made through three following stages or three consensus algorithms, PoW, PoA, and PoS respectively.

The first stage where the PoA takes place, can be done in two approaches, the first requires the POW miners to search for proper hash for blocks in parallel. After the hash is found a miner fills, the block translates it to the network for transaction verification by PoA miners. The second approach requires the PoW miners to find a proper hash, open a macro-block and hold it for a team of PoA miners to fill the macro-block where the micro-blocks are containing the transactions.

In the second stage POA miners performs in response to the chosen PoW approach described in stage1. PoA miners in the case of the first approach are responsible to check the hash in the translated block's header and to verification of the transactions on the block.

In the case of the second approach, the PoA miners are responsible to check the hash of the translated macro-block then creates 62 micro-blocks with 40 included transactions for each block, and send them to the macro-block then depending on the transactions where the miners attach it to one of the system branches, this operation of verification done by POA miners which does not require large computational capability and can be performed even using smart phones.

In the third stage, the PoS miners repeatedly check the balance of all the wallets in the system, as a result the PoS miners receives a percentage of the mining reward emission. The reward depends on the PoS miners balance in two ways: first the system set minimum and maximum balance boundary which outside it as a miner and cannot receive a reward, second, the reward grows as the PoS miner balance grow from minimum to maximum.

3. Implementation

Figure 1 shows the complete implementation of all applied steps where extraction of the statistics from the main network for each algorithm are involved, perform the experiments for encryption algorithms and then perform the analysis and drive the results.

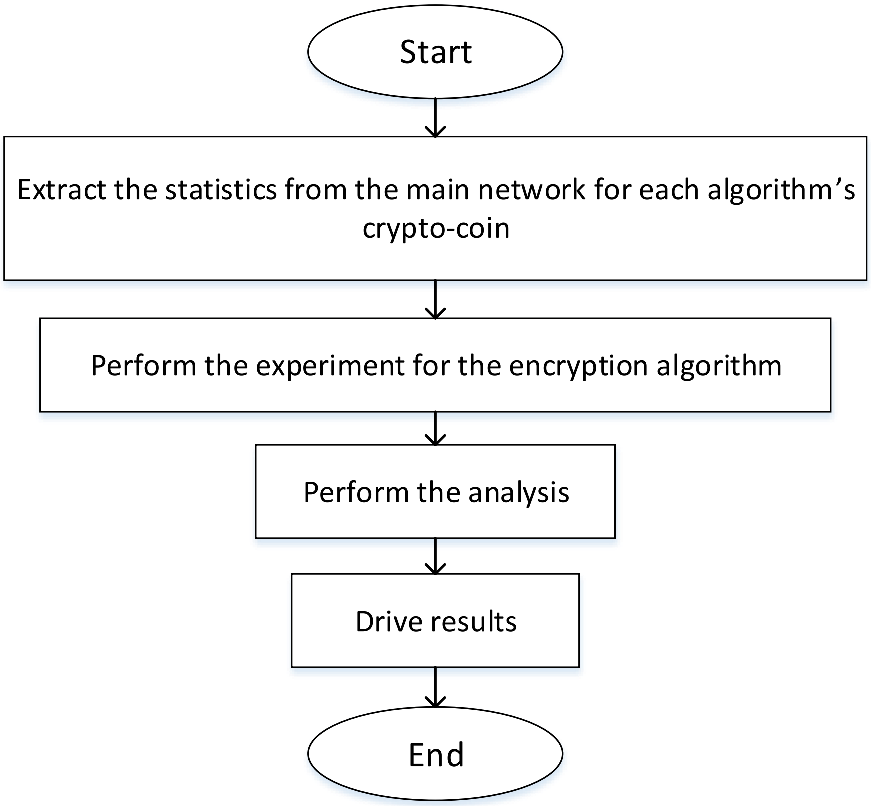
Start
Extract the statistics from the main network for each algorithm's crypto-coin
Perform the experiment for the encryption algorithm
Perform the analysis
Drive results
End

Figure 1: Implementation steps

The relevant data is collected from scientific papers and multiple websites to collect the required metrics for the analysis. And for the purpose of analyzing the efficiency of the cryptographic algorithm running within each type of Blockchain, the algorithms of SHA-256, SHABAL-256, and BLAKE-256, Eclipse IDE 8.0 are used to run each algorithm code in order to measure the metrics of time to encrypt the text, memory utilization and CPU utilization. Each algorithm is run using sample text of size 4 KB where the metrics of the results are collected using the internal measurements of the Eclipse IDE 2018-12 that uses JDK 8.2 which can measure the running time, memory utilization and CPU utilization.

a. Energy consumption

Energy consumption is compared according to a widely used mining hardware example for each crypto-coin Blockchain algorithm. Table 1 shows the hardware energy consumption requirements.

Table 1: Hardware energy consumption

Algorithm	**Crypto-coin**	**Hardware example**	**Average energy consumption rate by watts**
Proof of work	Bitcoin	SP35 Yukon Power	3650 watts
Proof of capacity	Burst coin	Raspberry PI	5.5 watts
Proof of activity	Decred	Seagate Barracuda 7200 + SP35 Yukon Power	1825 watts
Trinity consensus algorithm	Enecuum	Cubot Z100 Smartphone	913 watts

b. Network Scalability

The specification of the network that is related to the block size, number of transactions per second, block generation time, number of block confirmations, and network number of nodes and collected from the main network of each algorithm cryptocurrency gathered from [12-16]. Table 2 shows the scalability statistics in each consensus algorithm.

Table 2: Scalability statistics in each consensus algorithm

Metric	**Proof of work**	**Proof of capacity**	**Proof of activity**	**Trinity consensus algorithm**
Average Block size	1 MB	918 KB	558 KB	Variable 4KB – 4MB
Number of transactions per second	7/30 TPS	80 TPS	14 TPS	9000 TPS
Block generation time	10 mins	4 mins	5 mins	Instant
Time to add transactions to the block	30 mins – 16 hrs.	Instant	Instant	Instant
Confirmations per block	6	4	2	2

c. Costs of majority attack

In order to provide a fair comparison to the prices here we assumed that the total hash of all the network is equal to the hash rate of Bitcoin which equals to 37146820.728 TH/S then it calculate the price of acquiring 51% of the total hash power. Table 3 shows the costs of majority attacks.

Table 3: Costs of majority attacks

Algorithm	**Majority attack price**
Proof of work	633,585,4610,4195 $
Proof of capacity	947,054,479.76429 $
Proof of activity	637,220,0975.4419 $
Trinity consensus algorithm	633,649,183,05170.44 $

d. Efficiency of cryptographic algorithm

Table 4 shows the efficiency of cryptographic algorithm.

Table 4: Efficiency of cryptographic algorithm

Algorithm	Time taken to encrypt data	Memory utilization	CPU utilization
Proof of work	303 ms	3.576mb	48.3ms
Proof of capacity	527ms	4.357mb	67.4mb
Proof of activity	248ms	3.211mb	34.9mb
Trinity consensus algorithm	527ms	4.357mb	67.4mb

4. Results and discussion

a. Energy consumption

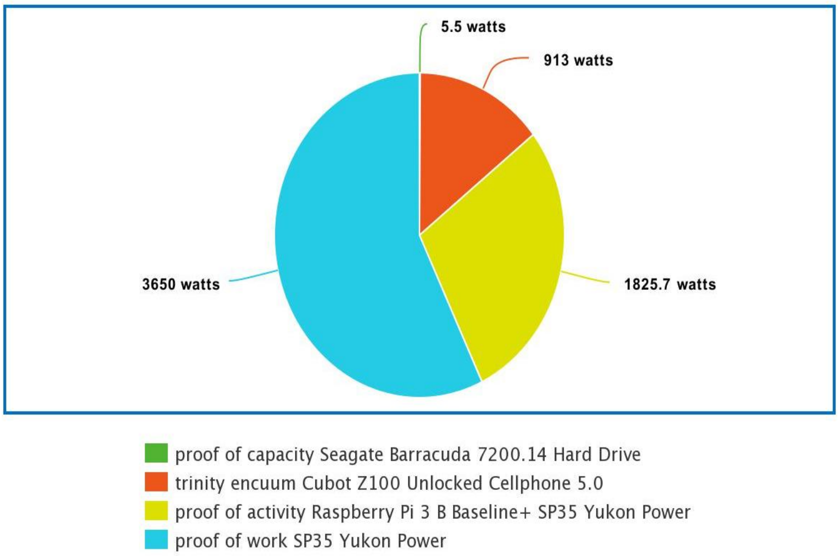

Figure 2: Hardware energy consumption rates

The energy consumption of proof of work's hardware is still higher than the energy consumption of the combined energy consumption of the rest of the algorithms. As showed in Figure 2, the POC using only 5.5 watts, the second lowest is trinity consensus algorithm having 913 watts' overall hardware energy consumption than proof of activity by average hardware consumption of 1825.7 hardware consumption. The percentage of enhancements are showed in Figure 3.

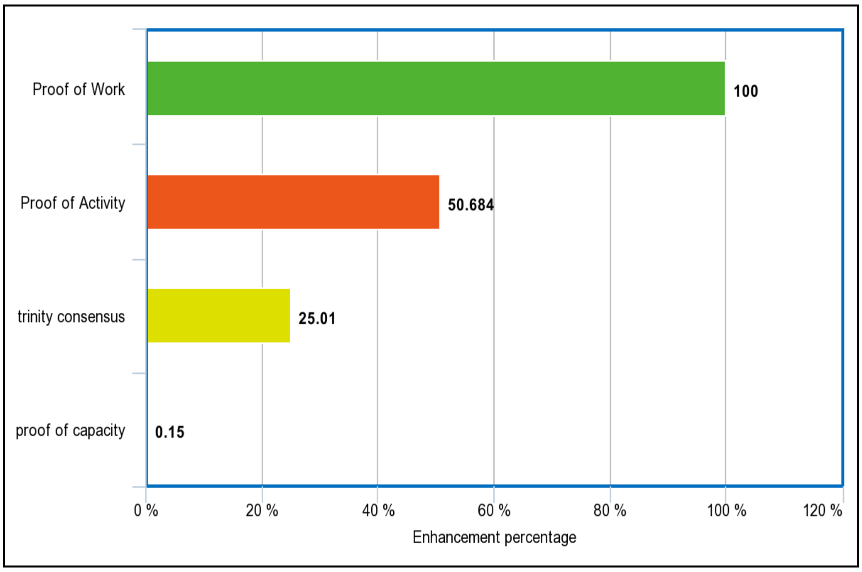

Figure 3: Percentage of enhancement in hardware energy consumption

b. Blockchain network scalability

Since its first proposal in 2009, the Blockchain has been in a quest for scalability enhancement. A lot of proposals have been proposed to enhance the problem of the number of transactions per second of Bitcoin Proof of work such as the soft fork which proposed the implementation of Segregated Witness which raised the number of transactions from 7 TPS to 30 TPS. The scalability will be evaluated according to the highest block size, the highest amount of transactions per second, the lowest block generation time, the lowest time to add transactions to the block, the lowest Confirmations per block. As shown in Figures 4 and Figure 5 the one satisfying these criteria will be the trinity consensus algorithm.

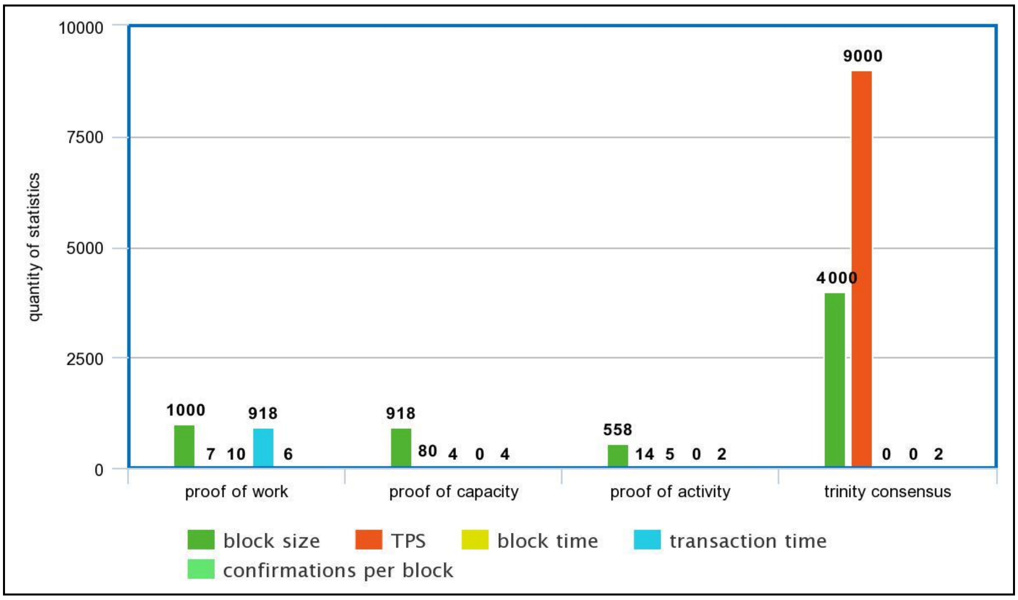

Figure 4: Scalability comparison

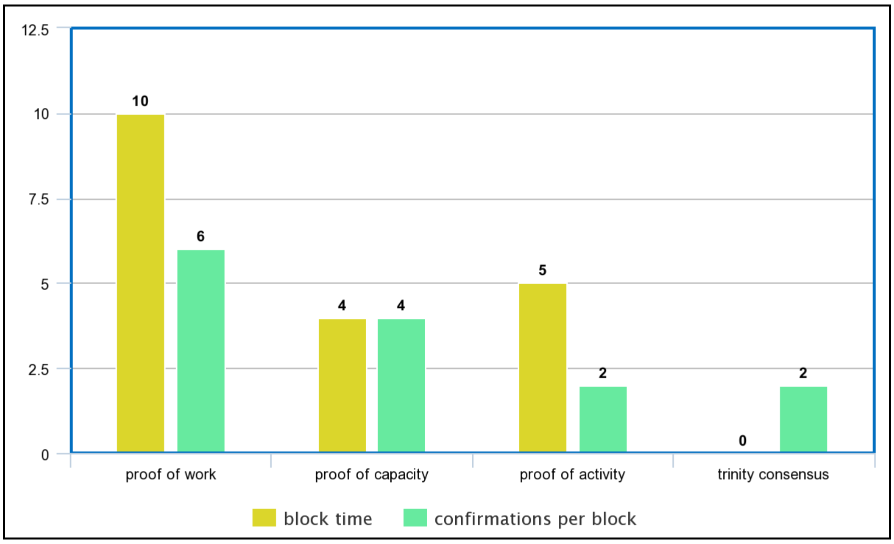

Figure 5: Scalability comparison of block time and confirmations per block

c. Possibility of majority attack

One of the aspects of security on POW is the high costs of maintaining more than half of the hash power on the network as discussed above. The current hash rate of bitcoin is 37146820.728 TH/S.

In POC given the amount of memory power consumed in the network, it's found that it's necessary to obtain the amount of at least 51% of 148,372 TB which is 94029.72 TB, which means that you'll need 4700545.7028$ in order to attack the current network.

In the POC that combines the PoW and PoS, assuming that a malicious participant can have the more than 50% of the Proof of work hash power it's still possible to get his tickets selected as one of the five voters from the ticket pool. Speaking in numbers at the time of writing, the total hash rate decreased is 216444.05 THs/S, and the total stake is 4285471 DCR (PoA crypto-coin), the total amount of attacking the current network is <51% of the hashing power which is 2185590.21 DCR coin in order to have the majority of the resources in the network.

d. Efficiency of cryptographic algorithms

Figure 6 shows the efficiency of encryption algorithm comparison.

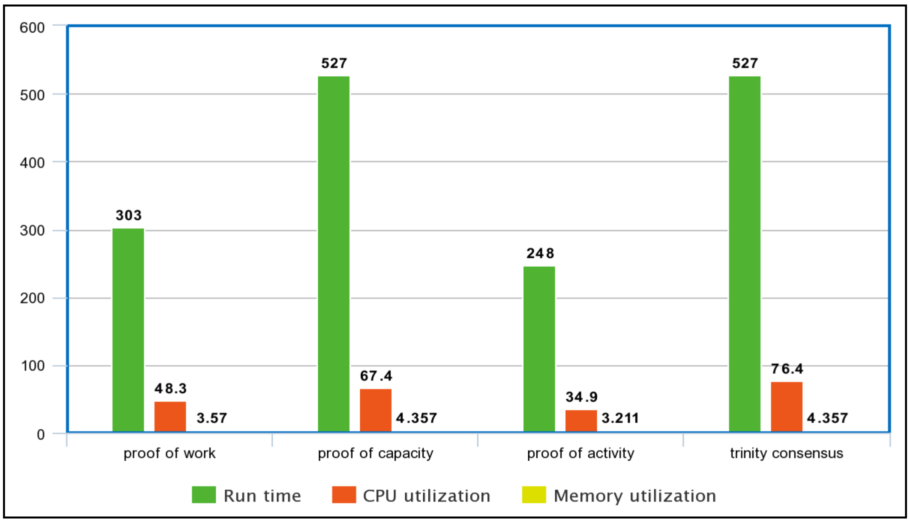

Figure 6: Efficiency of encryption algorithm comparison

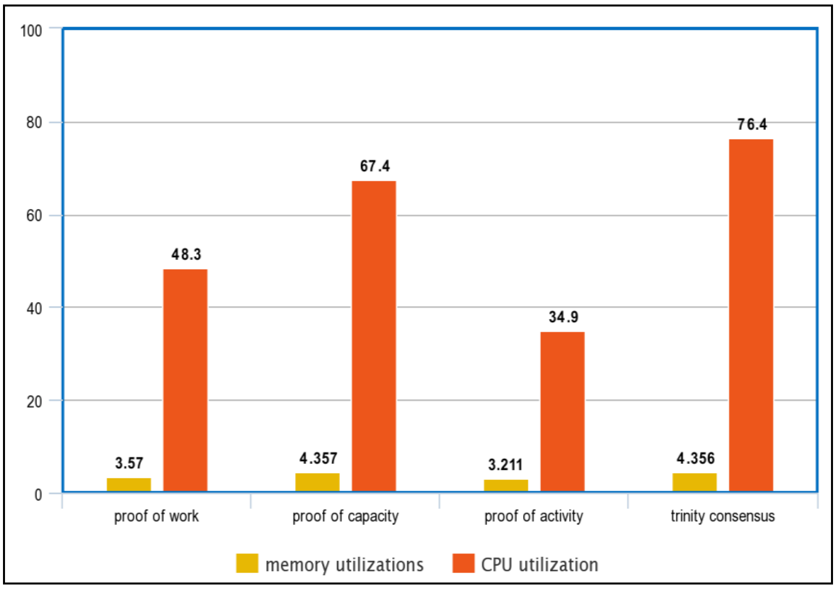

Figure 7: Memory and CPU utilization

Figure 6 represents clarifications to the CPU and memory utilization quantities shown in Figure 6. As shown in Figure 6 and 7 running the codes it was found that the BLAKE-256 that run the proof of activity algorithm has recorded the fastest results among the other algorithm as shown in Table 4, the second-lowest was the SHA-256 which runs the proof of work then SHABAL-256 that run the proof of capacity and trinity consensus algorithm. We can conclude that the trinity consensus algorithm achieved the maximum enhancement among the algorithms under investigation especially since it achieved a massive enhancement in the scalability section. Let us take it to step by step, when it comes to hardware power consumption trinity consensus algorithm has achieved the second best energy consumption after the proof of capacity and that’s due to the emergence of the technology of mobile mining that reduced the energy consumption according to the trinity coin official website; the mining application of Trinity uses approximately the same energy as the standard messenger applications. About the scalability it could achieve 4 times bigger block size in addition to the ability to create a macroblock that contains the number of the micro block according to the need, ~128,517% more transactions per second than a proof of work Bitcoin, trinity consensus achieved the optimum block time and transaction time with an instant block generation time, and lastly 33% fewer confirmations than a proof of work which means less work to achieve security. On the possibility of the majority attack, it costs “$633,649,183,05170.44” to attack the trinity consensus algorithm network assuming that the trinity consensus algorithm crypto-coin will replace the Proof of work so the calculations assumed the same hashing rate of bitcoin in addition to the proof of stake miners that rechecks the wallets in the Blockchain balances in comparison to the balances on the chain and that will prevent any chance of double-spend attacks. Although the Enecuum (official crypto-coin that uses trinity consensus algorithm) according to our experiment achieved the slowest statistics of encryption algorithms efficiency (refer to Table 4) it still didn’t affect the scalability factors.

5. Conclusion

In this research, we addressed the problem of Blockchain consensus algorithms comparative analysis selecting the algorithms of Proof of Work, Proof of Capacity, Proof of Activity, and trinity consensus Algorithm which are chosen as a result of being based on the PoW concept of work as in the case of Proof of Capacity, or a hybrid which consists of Proof of work as a part of its algorithm. Using the analysis of the limitations of the proof of work. Doing so it was found that the trinity consensus mechanism has solved the majority of the limitations of the proof of work. And we might soon see a great turnout to this network after its official launch this year. It could be foretold that the Trinity consensus algorithm has great potential since it was one of the first coins that used mobile mining, hence there will be a great deal of scalability and nearly impossible to maintain the majority of the network. For the future work, scalability measures are recommended to be implemented properly using Blockchain evaluation tool such as the tool developed by Hyper-ledger which are soon to have a release that can evaluate the given types of Blockchain.

References

[1] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—a systematic review," *PloS one,* vol. 11, no. 10, p. e0163477, 2016.

[2] S. Nakamoto, "Bitcoin open source implementation of P2P currency," *P2P foundation,* vol. 18, 2009.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot2019.

[4] K. N. Qureshi, S. S. Rana, A. Ahmed, and G. Jeon, "A novel and secure attacks detection framework for smart cities industrial internet of things," *Sustainable Cities and Society,* vol. 61, p. 102343, 2020.

[5] B. Laurie and R. Clayton, "Proof-of-work proves not to work; version 0.2," in *Workshop on Economics and Information, Security*, 2004.

[6] B. B. Half, "Bitcoin Block Reward Halving Countdown," ed: Preuzeto s: www. bitcoinblockhalf. com (25.06. 2019.), 2019.

[7] I. Bentov, C. Lee, A. Mizrahi, and M. J. A. S. P. E. R. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y," vol. 42, no. 3, pp. 34-37, 2014.

[8] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y," *ACM SIGMETRICS Performance Evaluation Review,* vol. 42, no. 3, pp. 34-37, 2014.

[9] P. Vasin, "Blackcoin’s proof-of-stake protocol v2," *URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf,* vol. 71, 2014.

[10] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in *Annual Cryptology Conference*, 2015, pp. 585-605: Springer.

[11] C. Li, P. Li, D. Zhou, W. Xu, F. Long, and A. Yao, "Scaling nakamoto consensus to thousands of transactions per second," *arXiv preprint arXiv:1805.03870,* 2018.

[12] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys & Tutorials,* vol. 20, no. 4, pp. 3416-3452, 2018.

[13] J. Bonneau, "How long does it take for a Bitcoin transaction to be confirmed," ed: November, 2015.

[14] S. Buchko, "How Long do Bitcoin Transactions Take?," *Coin Central,* vol. 12, 2017.

[15] R. Qazi, K. N. Qureshi, F. Bashir, N. U. Islam, S. Iqbal, and A. Arshad, "Security protocol using elliptic curve cryptography algorithm for wireless sensor networks," *JOURNAL OF AMBIENT INTELLIGENCE AND HUMANIZED COMPUTING,* 2020.

[16] K. N. Qureshi, F. Bashir, and A. H. Abdullah, "Provision of security in vehicular ad hoc networks through an intelligent secure routing scheme," in *2017 international conference on frontiers of information technology (FIT)*, 2017, pp. 200-205: IEEE.