FPoW: An ASIC-resistant Proof-of-Work for Blockchain Applications

Mahmudul Hassan Ashik[1], Mirza Mohd Shahriar Maswood[1], Abdullah G. Alharbi[2], Deep Medhi[3]
[1]Department of ECE, Khulna University of Engineering & Technology, Bangladesh.
[2]Department of Electrical Engineering, Faculty of Engineering, Jouf University, 72388, Saudi Arabia.
[3]University of Missouri–Kansas City, MO-64110, USA
Email: ashik1509031@stud.kuet.ac.bd, mmnt7@mail.umkc.edu, a.g.alharbi@ieee.org, dmedhi@umkc.edu

***Abstract*—Blockchain is a public ledger which is distributed in nature and has become highly popular. Bitcoin is the most successful application of it. The reason behind Bitcoin's success lies in its Consensus mechanism which ensures the security from any kind of attack. Because of this, no dishonest miner can affect the chain to manipulate it according to their wish. Also, the double spending problem does not occur and there is no need to trust a third party in this network. The most common consensus protocol in bitcoin technology is Proof-of-Work (PoW) which entirely depends on the computation power of miners. Because of this dependency, Application-specific Integrated Circuits (ASIC) is designed for bitcoin mining. Thereafter, it has become a threat to its decentralized nature and has been monopolizing the validation of new blocks. It is not possible to halt the production of ASIC-based devices even if it threatens the decentralized applications. So, different types of consensus protocols are proposed to nullify this threat whereas all of them have failed to fully nullify it. ASIC devices are costly, so only a few miners can afford it and monopolize over blockchain network. In our work, Filtered Proof-of-Work (FPoW) is proposed and its ASIC-resistivity has been evaluated to make it a future-proof ASIC-resistant consensus protocol.**

***Index Terms*—Blockchain, 51% attack, Consensus, ASIC, Proof-of-Work, Mining nodes**

I. Introduction

Blockchain technology can maintain transaction records which are immutable and without any central authority and without trusting anybody [1]- [3]. The cryptocurrencies depending on blockchain are growing rapidly and generating huge sum of revenue. For this, more effective protocols are coming and improving the performance of the cryptocurrencies. Blockchain technology is now considered as one of the hottest interests among companies as it is bringing revolutionary changes in business operations. The main reason of the success behind blockchain is the consensus mechanism which secures the chain from any malicious node and establishes an agreement about who should add a new block. Proof-of-Work is a widely adopted consensus protocol which is also used in Bitcoin. This mechanism needs high computation power or it may never mine any block. A miner's CPU or GPU can be used to mine but of course GPU is computationally faster and has better chances of mining.

Ever since its starting, 51% attack has been the biggest threat to blockchain network. This is a scenario where a group holds more than 50% of network capacity which can eventually be threatening for the network itself. Recently, Application-specific Integrated Circuits (ASICs) are used to mine the blocks. Such ASICs are specially designed for mining blocks and faster than general purpose CPUs or even GPUs [4]. This is more threatening against the decentralized nature of blockchain compared to the 51% attack. ASIC-based mining nodes participate in disguise of other common nodes and they needs to be eliminated. To prevent this ASIC-based malicious mining, many types of consensus protocols are introduced. However, since, there is no basic difference between general purpose and application specific computing platform, it is not possible to completely prevent these ASIC-based mining. Therefore, our research goal is to implement an ASIC-resistant Proof-of-Work mechanism. The detail implementation technique of this mechanism and evaluation of its ASIC-resistivity will be discussed later.

In our work, we propose Filtered Proof-of-Work (FPoW) that modifies the basic Proof-of-Work to make it more resistant to ASIC-based mining. In this regard, at first, we used general Proof-of-Work mechanism but filtered out a percentage of the mining nodes that were computationally faster, assuming all ASIC-based devices are faster than general purpose mining devices. Second, we create a blockchain network where all the nodes for mining are refreshed over time to add new nodes and to remove filtered out nodes. Thus, that particular network will be mostly free of high computing ASIC-based mining and a level playing field will be created for all general miners. Our proposed FPoW can be applied to secure the cutting edge technologies such as cloud data centers by preventing DDoS attack as mentioned in [5], fog computing and many more.

The rest of the paper is organized as follows: Section II discusses the related works and our novel contributions beyond state-of-the-art techniques. Section III explains how Bitcoin's Proof-of-Work is implemented. Section IV presents our proposed mechanism FPoW. Section V shows the performance evaluation of our work. Finally, section VI concludes the paper mentioning the possible future works.

II. Related Work

Many Proof-of-Work mechanisms are proposed to be ASIC-resistant, due to the threat of ASIC-based mining. Multi-hash PoW uses multiple hash functions and thus compute a block. There are varieties of these algorithms for example X11 [6],

978-1-7281-7366-5/20/$31.00 ©2020 IEEE

X14 [7], X17 [8], X11EVO [9], X16S [10], X16R [11], Quark [12], TimeTravel [13].

ASIC-based devices are of lower memory. Considering this fact, Memory-hard PoW such as Ethash [14], Scrypt [15], CryptNote [16] are developed. At a time, they were more ASIC-resistive than bitcoin's SHA256d [17]. However, eventually ASIC devices that can counter the Memory-hard PoW were released in the market (Antminer E3 and Antminer L3+ for Ethash and Scrypt respectively).

Alternative to Proof-of-Work, the Proof-of-Stake (PoS) [18] consensus mechanism was also proposed which highly reduces the waste of energy. However, new possible threats come with PoS such as Nothing at Stake and Bribe Attack problem [19]. However, some approaches were proposed to prevent those threats on PoS [18], [20]. Other less popular consensus mechanisms were also proposed such as Practical Byzantine Fault Tolerance (PBFT) [21], Proof-of-Useful-Work [22] etc.

III. Proof-of-Work (PoW)

In blockchain mining, massive amount of transactions is collated into a block and every block is linked to the previous block. The process of adding a block into the chain is called block mining. This mining is done by many distributed nodes around the world in a peer-to-peer basis. To secure the chain from dishonest nodes and to support all the nodes, a very reliable consensus mechanism is needed. This mechanism involves the nodes to solve a very hard but easily verifiable mathematical puzzle. The node which successfully solves the problem first, then add a block to the blockchain which is verifiable by all. To find the solution of the problem, miners have to find a nonce which can be any number that befits some certain criteria. To find the nonce, brute-force search is used. So, miners cannot predict anything about when they can solve the problem or how close they are to solve the problem [23].

The mining system is very secured against the attacks to alter the blockchain. If a dishonest miner attempts to create an alternative blockchain to breech the security of actual blockchain then, that alternative blockchain needs to be faster than the actual blockchain. However, to do so, the dishonest miner will be in need of a very powerful computational resource. In this way, it makes the older blocks more secured from hacking. A block is considered secured if it is six blocks deep in the chain [23].

It is known as difficulty of Bitcoin [24], a renowned decentralized application of blockchain is adjusted once in every 2016 blocks. That is why, the network needs to maintain that no more than one block can be added to the chain in every ten minutes. This ten minutes of duration is actually a compromise between the confirmation time of the first block and the work wasted because of forking.

A. Mathematical Puzzle

A puzzle needs to be solved in order to complete the mining process. A puzzle can be many things including:

- Finding a given hash or finding which input to use based on a known output

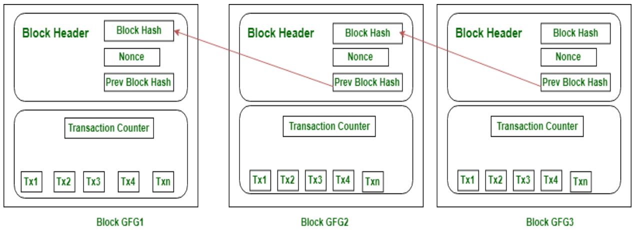


Fig. 1: A Blockchain Network [25]

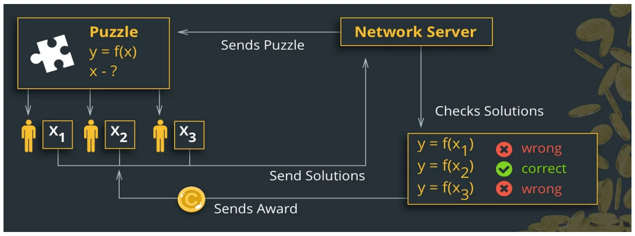


Fig. 2: Proof-of-Work Consensus Mechanism [26]

- Integer factorization or the presentation of number as a multiplication of other two numbers

The appropriate puzzles to be used is determined considering their difficulty levels.

B. Implementation

After solving the puzzle, new block is added to the chain and transactions are confirmed. The difficulty depends on users, current power, and load of the network. Every block contains its hash and the hash of the previous block to increase security and to prevent any kind of threat. When a miner is able to solve the puzzle, new block is created and the miner receives the reward.

Fig. 1 shows the basic blockchain network in which every block is interconnected using its own hash and the previous hash. Fig. 2 shows how the Proof-of-Work mechanism works in a very convenient way to understand.

IV. FPoW: A Filtered Proof-of-Work

In this section, we present our proposed consensus mechanism FPoW explaining its algorithm and distinction with PoW to understand how FPoW can be ASIC resistive. Recall that PoW refers to a system or mechanism which is time and energy consuming but easily verifiable and satisfies some given requirements. It is known as the original consensus mechanism for several blockchain network. Filtered Proof-of-Work modifies the consensus mechanism to make it more ASIC-resistant. It will apply a round system and at the start of each round there will be a dummy mathematical puzzle of certain difficulty level to calculate the computing power of the mining devices. This will give the system the ability to find out ASIC-based mining nodes as it is known that they are specially produced to solve this kind of problems. So, all the ASIC-based mining devices will be on top of the list which will be generated according to their computing power. Based on the list, the system will remove a number of mining nodes from the network which have greater computing power than other nodes. After performing all the filtering, the original Proof-of-Work mechanism will run among the remaining mining nodes with certain difficulty. The mining node which will be able to solve that first, will create a new block and receive the reward. After that a new round will begin and the same procedure will be repeated. After every round, the network will allow new nodes to be connected or older nodes to be removed.

A. Notations Summery

The notations used in the algorithm are described as below:
N: Number of round
n: Nonce
t_s: Timestamp of that time
i: Mining node number
t_i: Time taken to solve the puzzle
x: Number of nodes to be removed from high computing devices
y: Number of nodes to be removed from low computing devices
R_{high} and R_{low}: Percentage of nodes to be removed from high and low end

B. FPoW Algorithm

The whole process follows the algorithm as given below:

```
1. Initialize round $N$
2. $n = 0$, $t_s =$ timestamp, data = given data
3. Find a hash using sha256 which contains four zeros at the start. Use $n$, $t_s$, and data
4. $n++$
5. Repeat step 3 & 4 until condition fulfills
6. Get time $t_i$ for all $i$ nodes upon fulfilling the condition
7. Arrange all $i$ nodes in ascending order
8. Remove $R_{high}$ of $i$ from the top
9. Arrange all remaining $(i - x)$ nodes in descending order
10. Remove $R_{low}$ of $i$ from the top
11. Apply standard PoW mechanism to the remaining $(i - x - y)$ mining nodes
12. $N++$
13. Start new round and repeat step 1-10
```

The entire algorithm depends on a dummy puzzle which tells the mining nodes to find a hash that starts with four zeros as an example. This puzzle can be any puzzle but it needs to be there for sorting all the mining nodes according to the time they take to solve it. The node which takes least time to solve this puzzle has undoubtedly the best computation power. So, removal of R_{high} of the nodes which take the least times means removing the ASIC-based mining devices in a real world scenario. Also, by removing R_{low} of the least computing power devices will make sure that nodes that have no chance of mining will also be eliminated to save energy and resources.

The difficulty of both the dummy puzzle and original standard one will be increasing with time as it is done in decentralized applications. The proposal of removing R_{high} from the top of the list would be based on the number of ASIC-based mining devices, which are costly compared to general purpose devices. For example, R_{high} can be set to 10%. On the other hand, the removal of lowest R_{low} computational power devices ensures reduction of power and resource waste. For example, R_{low} can be set to 20%. Certainly, this percentage can be varied and adjusted with the changing number of mining nodes and other factors.

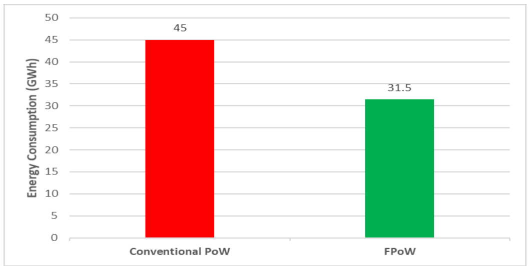


Fig. 3: Comparison of energy consumption PoW and FPoW

V. Performance Evaluation

A. Testbed Setup

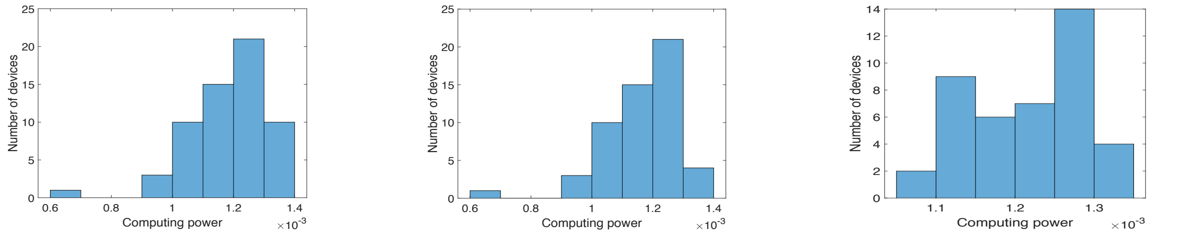
In our experimental setup, we created a decentralized blockchain network of 60 PCs. This way we mimicked a real world blockchain network scenario. 60 PCs were used to represent 60 mining nodes.

B. Result Analysis

According to the Algorithm 1, a dummy puzzle was set to sort the nodes according to their computing power. Fig. 4a shows the mining nodes in ascending order of computing power. In this case, the time t of every node (localhost) to solve the puzzle was recorded. Then from the result, $1/t$ was found for every node. The node which solved the dummy problem first was considered to have the best computing power, or we can say that the node whose solving time t was the least had the higher $1/t$, i.e., computing power. Then from the list, 10% which means 6 nodes which took the least times to solve the puzzle were removed. After that, 20% which means 12 nodes which took the most times to solve it were removed.

A mining node may take random time to solve a puzzle and it is not uniform but our goal was to test the model and show that the nodes which took the least and most times were removed. In Fig. 4a, all 60 nodes are put in a histogram according to their computing power. Again, the computing power is nothing but $1/t$. Fig. 4b shows that 6 nodes have been removed which was on the rightmost side. In other word, 6 mining nodes which had the best computing power were filtered out by the new system.

After filtering out the devices which had the best computing power, the system filtered out some of the devices which had the least computing power. From step 10 of the Algorithm 1, it was done to remove the mining devices which had little no chance of mining. Fig. 4c shows the scenario after filtering out all devices which had the least computing power as well as the best computing power. By doing this, it can



(a) Without Filtering any node

(b) Filtering high computing nodes

(c) Filtering both high and low nodes

Fig. 4: Mining nodes with respect to computing power and after filtering high and low computing nodes

ensure that potentially ASIC-based mining devices as well as devices which have no chance of mining will not participate in creating new blocks for blockchain network. A comparison between conventional PoW with our proposed FPoW is shown in Fig. 3. According to our result, FPoW is 30% more energy efficient than PoW which makes it better suitable for blockchain applications. Unlike PoW, FPoW prevents potential ASIC-based mining nodes from adding new blocks to the blockchain network. That is why, the very core idea of ASIC-based mining fails to dominate general purpose miners. So, it will be beneficial to implement FPoW in real world blockchain networks where ASIC-based miners monopolize over the whole network.

VI. Conclusion and Future Work

In our work, we presented a new consensus mechanism which is ASIC-resistant and flexible for different blockchain applications. We used PCs as mining nodes to measure the performance of our consensus mechanism. Our proposed method is more energy efficient than other consensus mechanisms. Usage of the dummy puzzle ensures to sort all the mining nodes according to their computing power to filter out ASIC-based mining devices. Furthermore, the decentralized nature of blockchain will not be violated by filtering out ASIC-based mining devices as those devices themselves are the true threats for the decentralized nature of blockchain technology. However, the dummy puzzle solving will take place randomly and thereafter, it will not be possible to make the filtering process ineffective by reducing the computing capability of any ASIC-based node for a particular time.

It is true that ASIC-resistivity depends on many factors and it is a hard nut to crack. So, in future, we plan to improve our consensus mechanism FPoW to automatically adjust the percentage of nodes to be removed in each round. We further plan to analyze the performance of FPoW in large scale applications.

References

[1] J Bonneau, A Miller, J Clark, A Narayanan, J A Kroll and E W Felten. "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies." In 2015 IEEE Symposium on Security and Privacy, pp. 104-121. IEEE, 2015.

[2] M Swan, "Blockchain: Blueprint for a new economy " O'Reilly Media, Inc.", 2015.

[3] F Tschorsch and B Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies." IEEE Communications Surveys & Tutorials 18, no. 3 (2016): 2084-2123..

[4] MB Taylor, "The evolution of bitcoin hardware." Computer 50, no. 9 (2017): 58-66.

[5] M. M. S. Maswood, M. M. I. Mamun, D. Huang and D. Medhi, "A Sliding Window Based Monitoring Scheme to Detect and Prevent DDoS Attack in Data Center Networks in a Dynamic Traffic Environment," 2018 IEEE 39th Sarnoff Symposium, Newark, NJ, USA, 2018, pp. 1-6.

[6] E Duffield and D Diaz. "Dash: A payments-focused cryptocurrency." Whitepaper, https://github. com/dashpay/dash/wiki/Whitepaper (2018).

[7] "X14 POW/POS cryptocurrency with Block Explorer, Stats, and IRC chat!" Accessed: Sept. 19, 2018. [Online]. Available: https://github.com/webcoinx14/Webcoin.

[8] "X17 algorithm - list of all X17 coins and miners for NVIDIA & AMD." Accessed: Sept. 19, 2018. [Online]. Available: https://coinguides.org/x17- algorithm-coins.

[9] H Cho, "ASIC-resistance of multi-hash proof-of-work mechanisms for blockchain consensus protocols." IEEE Access 6 (2018): 66210-66222.

[10] L Pighetti, "X16S - sixteen shuffled algorithms designed for small miners." Accessed: Sept. 19, 2018. [Online]. Available: https://github.com/Pigeoncoin/brand/blob/master/X16S-whitepaper.pdf.

[11] T. Black and J. Weight. "X16R - ASIC resistant by design." Accessed: Sept. 19, 2018. [Online]. Available: https://ravencoin.org/wpcontent/uploads/2018/03/X16R-Whitepaper.pdf.

[12] "Quark mining guide." Accessed: Sept. 19, 2018. [Online]. Available: http://www.quarkcoins.com/mining-quarkcoin.html

[13] "Time Travel (TimeTravel10 — Bitcore) algorithm, coins, miners and hashrate." Accessed: Sept. 19, 2018. [Online]. Available: https://coinguides.org/time-travel-coins/

[14] G Wood, "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper 151, no. 2014 (2014): 1-32.

[15] C Percival, "Stronger key derivation via sequential memory-hard functions." (2009).

[16] N Van Saberhagen,"CryptoNote v 2.0." Technical Report. White Paper (2013).

[17] Revolver coin resources. Accessed: Sept. 19, 2018. [Online]. Available: http://revolvercoin.org/resources.

[18] A Kiayias, A Russell, B David and R Oliynykov. "Ouroboros: A provably secure proof-of-stake blockchain protocol." In Annual International Cryptology Conference, pp. 357-388. Springer, Cham, 2017.

[19] G BitFury "Proof of stake versus proof of work." White paper, Sep (2015).

[20] "Delegated proof-of-stake consensus." Accessed: Sept. 19, 2018. [Online]. Available: https://bitshares.org/technology/delegated-proof-of-stake-consensus.

[21] M Castro and B Liskov. "Practical Byzantine fault tolerance." In OSDI, vol. 99, no. 1999, pp. 173-186. 1999.

[22] M Ball, et al. "Proofs of Useful Work." IACR Cryptology ePrint Archive 2017 (2017): 203.

[23] S Sharkey and H Tewari. "Alt-PoW: an alternative proof-of-work mechanism." In 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), pp. 11-18. IEEE, 2019.

[24] S Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", Manubot, 2019.

[25] Proof of Work (PoW) Consensus. [Online]. Available: https://www.geeksforgeeks.org/proof-of-work-pow-consensus

[26] Dawn of indisputable trust, does Blockchain guarantee security? [Online]. Available: https://medium.com/digina-x-plorers/dawn-of-indisputable-trust-does-blockchain-guarantee-security-75576eb71eac