Research Article

Energy Efficient Multiprocessing Solo Mining Algorithms for Public Blockchain Systems

Zeeshan Raza, Irfan ul Haq, Muhammad Muneeb, and Omair Shafiq

1Department of Computer and Information Sciences (DCIS), Pakistan Institute of Engineering and Applied Sciences (PIEAS), Islamabad 45650, Pakistan
2School of Information Technology, Carleton University, Ottawa, ON, Canada

Correspondence should be addressed to Zeeshan Raza; zeeshan.raza@yahoo.com

Received 30 March 2021; Revised 29 June 2021; Accepted 30 August 2021; Published 31 October 2021

Academic Editor: Jiwei Huang

Copyright © 2021 Zeeshan Raza et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Blockchain as a decentralized distributed ledger is revolutionizing the world with a secure design data storage mechanism. In the case of Bitcoin, mining involves a process of packing transactions in a block by calculating a random number termed as a nonce. The nonce calculation is done by special nodes called miners, and all the miners follow the Proof of Work (PoW) mining mechanism to perform the mining task. The transaction verification time in PoW-based blockchain systems, i.e., Bitcoin, is much slower than other digital transaction systems such as PayPal. It needs to be quicker if a system adapts PoW-based blockchain solutions, where there are thousands of transactions being computed at a time. Besides this, PoW mining also consumes a lot of energy to calculate the nonce of a block. Mining pools resulting into aggregated hashpower have been a popular solution to speed up the PoW mining, but they can be attacked by using different types of attacks. Parallel computing can be used to speed up the solo mining methods by utilizing the multiple processes of the contributing processors. In this research, we analyze various consensus mechanisms and see that the PoW-based blockchain systems have the limitations of low transaction confirmation time and high energy consumption. We also analyze various types of consensus layer attacks and their effects on miners and mining pools. To tackle these issues, we propose parallel PoW nonce calculation methods to accelerate the transaction verification process especially in solo mining. We have tested our techniques on different difficulty levels, and our proposed techniques yield better results than the traditional nonce computation mechanisms.

1. Introduction

Blockchain has introduced a new transaction/data storage mechanism that provides better transparency, is more secure, enables business between untrusted parties, and helps in reducing fraud [1]. The use of blockchain technology is not limited to the cryptocurrencies now but is also being used in other industries like transportation, automotive industry, supply chain management [2], healthcare [3, 4], and agriculture sector [5, 6]. Blockchain offers advantages like transparency and immutability, but it also has some limitations specially when the PoW is used in solo mining. Proof of Work (PoW) [7, 8] is one of the first blockchain mining algorithms popularized by Bitcoin, and now many blockchain technologies use it for transactions confirmation.

The principle behind PoW is to solve a mathematical puzzle, and a reward is given to the miners who solve this complex problem. In PoW mining, miners need to pack transactions in a block and use a brute-force mechanism to find a nonce, which satisfies a given difficulty level. All the miners are given equal opportunity to find the nonce, and in case of success, they are given mining rewards as well as transaction fees.

As mentioned in the literature, such as [9], the mining process works approximately as shown in equation (1). Symbol + is used to denote the concatenation of strings. The cryptographic problem of computing a double SHA256 hash has to be solved by a miner denoted by $M$.

$$s = SHA256(SHA256(n + h + s' + x)).$$  \hspace{1cm} (1)
Here, \( s < x \), where \( n \) is a nonce value, \( h \) is a double SHA256 hash over the transactions that miner \( M \) intends to incorporate into its next block \( B \) (in the case of Bitcoin, \( h \) is the Merkle root), \( s \) is the solution for the block at the head of the blockchain at miner \( M \), and \( x \) is the current level of difficulty (leading zeros). If \( s \geq x \), then \( n \) is incremented, and \( s \) is recomputed up to the point that a solution is found with \( s < x \). If miner \( M \) finds a valid solution \( s \), miner \( M \) appends block \( B \) to the blockchain at miner \( M \) and broadcasts \((B, n, h, x)\) to the blockchain peer-to-peer network.

Nonce values are numeric values that are concatenated with block data before performing the mining task. The block data is then given to a hashing function SHA256 to get a hash of a targeted difficulty level. If the targeted difficulty level is not achieved, then the nonce value is incremented and again concatenated with block data before applying SHA256. The whole process continues until a hash that satisfies the given difficulty level is achieved. Once nonce is found, the block is broadcast to the blockchain network.

The nonce finding process in typical PoW is described in Figure 1.

PoW is a complex task that takes much more time and consumes a huge amount of energy [10, 11]. First blockchain application based on PoW is Bitcoin, and according to Bitcoinist “the average cost to mine a bitcoin in Serbia is about 3,100 US Dollars” [11]. It is also mentioned that “mining of a single bitcoin block consumes energy, which is enough to power more than 28 homes in the United States for one day” [11].

A popular method to increase the chances of success is to make a pool of mining resources by collaborating with other miners and dividing the reward consequently. The consolidated pool of resources builds more hashpower and increases their chance to succeed, but it decreases the chances of success if a miner wants to perform solo mining. Besides, these attackers can attack miners and mining pools as mentioned in Table 2 to influence the public blockchain systems.

In this paper, we propose algorithms to parallelize nonce computation of the PoW solo mining by assigning different ranges of nonce values to multiple processes. The proposed algorithms not only speed up the PoW mining process but also reduce energy consumption. Rather than applying pure brute force through aggregated hashpower, our proposed algorithms based on parallel computing [29] follows the principle of divide and conquers and subdivides a complex task into subtasks, which are then processed in parallel on a single machine. All the processes try to solve the subtasks of nonce computation in parallel at the same time, and once a processor finds a solution, it is communicated to all other processes. The proposed parallel PoW is much faster than the sequential version and saves energy, thus reducing the carbon footprint. Scientific contributions of this paper include the following:

- Interleaved algorithm: multiple processes try to find the suitable nonce from different nonce intervals/ranges.
- Progressive algorithm: multiple processes are assigned consecutive nonce values, and in case of failure in an iteration, jump to the next nonce value (a jump of 8 values in case of 8 processes) in next iteration and test the proposed parallel algorithms on different difficulty levels.

The rest of the paper is organized as follows: The literature review is discussed in Section 2, and the proposed solo mining algorithms are given in Section 3. Section 4 presents the performance analysis of proposed techniques, and the paper is concluded in Section 5.

2. Literature Review

Scalability is the main issue in PoW-based public blockchain systems, and researchers are working on different solutions based on hashing algorithms and consensus mechanisms to tackle this issue. Some related work typically related to the scalability issue of PoW is discussed in this section.

The work in [30] introduced a new protocol to improve blockchain performance by changing the chain data structure to Graph Chain. Their parallel mining mechanism is focused on the selection of leaders among \( M \) miners. By solving a puzzle, miners can become leaders, and leaders are assigned duty for a period. The authors suggested that transaction confirmation speed can be increased by allowing more leaders to do PoW mining tasks in parallel. They only focused on the miners’ selection process and did not work on the improvement of nonce computation.

In [31], the authors proposed an accelerated process of PoW mining. They built a process that carries out selection of a manager, work distribution, and a reward system. In their method, miners can use the same transaction data (same transaction hash) but cannot use the same nonce values; thus, no multiple miners can carry out the same mining task. Same as the study in [30], the focus of [31] is on miners selection.

The work in [32] also proposed a parallel mining protocol. In their protocol, each transaction is connected to at least two transactions that are verified, and all miners need to verify any new transactions. Their focus was also on miners but not on the actual mining process.

2.1. Blockchain Consensus Algorithms

Consensus algorithms [33, 34] are decision-making processes for a group, where participants of a group support the decision that is best for everyone. To overcome the scalability issue of PoW, other consensus mechanisms are also introduced, which are discussed with the help of the comparative analysis provided in Table 1.

Each consensus mechanism shown in Table 1 has its strengths and weaknesses and could be used in different types of blockchain systems. But the most common consensus algorithm in public blockchains is PoW, which has time and energy consumption issues associated with it. In this research, our focus is on scalability of such blockchain systems, which intend to use PoW specially in solo mining.
2.2. Attacks on the Blockchain Consensus Layer. Security is an essential feature in a variety of systems and is very important issue in blockchain-based systems. There are a variety of attacks, which are used by the attacker to attack the blockchain data, blockchain networks, and their communication, consensus mechanism, miner/mining pools, and smart contracts [56, 57], i.e., Malleability Attack [58], Quantum Attack [59], Distributed Denial of Service (DDoS) Attack [60], Eclipse Attack [61], Sybil Attack [62], Border Gateway Protocol (BGP) Attack [63], Phishing Attack [64], Selfish Mining Attack [65], Consensus Delay Attack, Double Spending Attack [15], Integer Overflow Attack [66], and Short Address Attack [67].

As our research work is based on consensus mechanism and mining, we focus on the consensus layer attacks and highlight the research work done to mitigate them. In selfish mining attack [65], a selfish miner in a mining pool uses selfish strategies to get more rewards than the honest miners. The selfish miner tries to withhold a validated block and stops its broadcasting to mining pool network but continues to mine the next block. In this way, a selfish miner demonstrates more PoW than other miners of the mining pool. Doubles pending [15] is a digital cash scheme flaw, in which the attacker spends a digital token more than once, as a digital token is associated with a digital file that can be duplicated. In bribery attack, some miners act rationally and accept bribes from attackers to increase their reward. Refund attack is a Payment Protocol attack that could affect the BIP70 protocol merchants [22]. In block withholding attack, a miner who has mined a block does submit it but abandons it and causes a mining pool and loses all bitcoin rewards. In balance attack [26], attackers select miners that have the same mining capabilities, and rather than entering into mining competition with other miners, they defer the messages between the selected miners. Consensus Delay is the time between the block propagation to block storage after the consensus [68]. In a supply chain system, attackers can use consensus delay attack to interrupt the information propagation and, hence, can easily create a double-spent transaction by refuting the vote of an authorized user [13].
In Table 2, we did a comparative analysis of different attacks, which could eventually influence the working of consensus mechanism and mining process. Our research work could be beneficial in blockchain systems, which avoids the mining pools but rather wants fast solo mining protocols. If a system adopts solo mining, then definitely it will have to bear the consequences of more time and energy consumption. We proposed two parallel commuting based techniques to make the solo mining faster and cheaper in terms of energy consumption.

3. Proposed Parallel Algorithms for Nonce Calculation

Two main performance indicators of PoW include transaction verification time and energy consumption and both are tackled in our proposed parallel processing-based algorithms. In our proposed techniques, we did not alter the core working of PoW, but building upon the existing research, we proposed different nonce value selection methods before performing the PoW mining on multiple processes.

First of all, the performance of PoW mining as described in Algorithm 1 is tested. Algorithm 1 is tested on different difficulty levels, and the time taken to compute the nonce value on each difficulty level is computed as shown in 3; then, we compared it with our proposed parallel PoW techniques. For experimental purposes, the string "Parallel Computing" is used in place of Merkle Tree (in case of bitcoin), as even a simple string is enough to validate performance of proposed solution. We did not change the string in the whole process but varied the difficulty levels to calculate the mining time at each difficulty level for PoW and parallel PoW techniques.

The pseudocode of the PoW is given in Algorithm 1.

In our naive implementation, a block of blockchain contains the following fields:

- nonce: int
- index: int
- blockData: string
- timeStamp: dateTime
- hash: string
- previousHash: string

We have computed the results on 8 difficulty levels on available Intel(R) Core(TM) i7-3770 CPU @ 3.40 GHz CPU machine as well as on a machine with built-in NVIDIA GeForce RTX 2060 GPU.

Table 3 is generated by implementing Algorithm 1 on the CPU; it contains difficulty levels, nonce values, and time taken in seconds to perform the mining task on constant block data.

As shown in Table 3, there is a significant amount of change in the nonce values and time taken in seconds as we increase the difficulty levels from 1 to 8. Time is almost constant from difficulty levels 1 to 4 but rapidly changes from difficulty levels 5 to 8, which shows that PoW mining becomes difficult on higher levels of difficulty.

To address the time consumption issue as shown in Table 3, we have introduced two parallel processing-based PoW mining algorithms and done multithreading and multiprocessing in both methods as shown in Figure 2.

3.1. Interval/Interleaved Algorithm. In the proposed interleaved algorithm, the nonce values are divided into multiple ranges/chunks, and the multiple processes/threads perform mining on different nonce ranges in a parallel fashion. The workflow and proposed mechanism of the interleaved approach are shown in Figure 3.

The pseudocode of the interleaved approach is given in Algorithm 2.

3.2. Multiprocessing Interleaved Approach. In this approach, we make 8 nonce value ranges as given in Figure 4. These ranges are given to multiple CPU processes to compute the nonce value. Once a process finds a nonce that satisfies the difficulty level, other processes stop working. The nonce value is then propagated to the blockchain network, and in case of acceptance, the reward is given to the miner. The results of the multiprocessing interleaved approach are given in Table 4.

3.3. Multithreading Interleaved Approach. We performed the mining task by giving subarrays to multiple threads to calculate the hash of a given difficulty level. Once a thread is successful in getting the resultant nonce, the whole process stops. Results computed by the multithreading interleaved approach are given in Table 5.

3.4. Progressive Approach. In this proposed approach, the PoW mining process is divided into 8 processes, and each process is assigned nonce values from 1 to 8. If a nonce value does not satisfy the desired difficulty level, it is updated by adding 8 in the previous value, and the mining process is repeated until one of the processes gets the desired nonce value. Once the solution is found, all other processes stop working, and the nonce value is propagated to the whole network. The workflow and proposed mechanism of parallel proof of work progressive approach are given in Figure 5.

The pseudocode of a progressive approach is given in Algorithm 3.

3.5. Multiprocessing Progressive Approach. In the multiprocessing progressive approach, the PoW mining process is assigned to 8 different processes. Each process initially assigned the nonce values from 1 to 8, and in the iteration, it updates the nonce value by adding 8 into it. If a process finds a nonce value that satisfies the given difficulty level, all other processes stop working, and the nonce value is propagated to the blockchain network. Table 6 contains the results of a multiprocessing progressive approach.

3.6. Multithreading Progressive Approach. In the multithreading progressive approach, 8 different threads perform the mining. Table 7 contains the results computed by the multithreading progressive approach.
3.7. GPU-Based Interleaved Approach. For GPU-based results and analysis, we picked the available laptop machine with built-in NVIDIA GeForce RTX 2060 GPU and calculated the time consumption and energy consumption of both PoW and our best performing multiprocessing interleaved algorithm. The selection of nonce value ranges and increment in nonce values is done on CPU, while GPU is used for parallel implementation of the SHA256 algorithm. Figure 6 elaborates the process.
Initialization

Block Data = Block Index + Merkle Tree + Previous Hash + Timestamp + …
NonceRangeSet = Range1, Range2, …, RangeN.

BlockHashes

BlockHash1 = SHA256 (Block Data + First Nonce Value in Range1)
BlockHash2 = SHA256 (Block Data + First Nonce Value in Range2)
;
;
BlockHashN = SHA256 (Block Data + First Value in RangeN).

Process1
while BlockHash1 does not satisfy the difficulty level do.
    BlockHash1 = SHA256 (Block + (Nonce Value + 1)).
Process2
while BlockHash2 does not satisfy the difficulty level do.
    BlockHash2 = SHA256 (Block + (Nonce Value + 1)).
;
;
ProcessN while BlockHashN does not satisfy the difficulty level do.
    BlockHashN = SHA256 (Block + (Nonce Value + 1)).

Solution
Broadcast the solution to the Blockchain network (Nonce value, the Merkle root and the Mined Block).

**Algorithm 2: Interleaved approach.**

**Figure 3: Interleaved approach workflow and mechanism.**

**Table 4: Multiprocessing interleaved approach results (CPU).**

| Difficulty level | Nonce value | Time in seconds |
|------------------|-------------|-----------------|
| 1                | 5200000003  | 0.009993791582000195 |
| 2                | 6500000027  | 0.009989261627917266 |
| 3                | 5200000299  | 0.0029981136322021484 |
| 4                | 5200000299  | 0.003997564315785984 |
| 5                | 5200000299  | 0.003997802734375 |
| 6                | 5200000299  | 0.003997802734375 |
| 7                | 260538310   | 2.223620414733867 |
| 8                | 1015800503  | 462.1195707321167 |

**Figure 4: Nonce value ranges.**

**Table 5: Multithreading interleaved approach results (CPU).**

| Difficulty level | Nonce value | Time in seconds |
|------------------|-------------|-----------------|
| 1                | 5200000003  | 0.0059969425201416016 |
| 2                | 6500000027  | 0.005996227264404297 |
| 3                | 5200000299  | 0.03896665573120117 |
| 4                | 5200000299  | 0.08294916152954102 |
| 5                | 5200000299  | 0.04797053337097168 |
| 6                | 5200000299  | 0.07795357704162598 |
| 7                | 260538310   | 7.604280948638916 |
| 8                | 1015800503  | 2235.2516202926636 |
4. Performance Analysis of Proposed Techniques

The code of the proposed interleaved and progressive techniques is done in Python programming language on both CPU and GPU machines.

4.1. Data Used for Evaluation. We generated data set by implementing the PoW and proposed parallel PoW algorithms on different difficulty level and evaluated the proposed algorithms. Table 3 for PoW and Tables 4–7 consist of the nonce values and time consumption at different difficulty levels from 1 to 8.
4.2. CPU-Based Results. On CPU, we performed the proposed parallel techniques and compared them with PoW.

4.2.1. Time Consumption. From our findings of Tables 3–5, multiprocessing interleaved approach is the best one. It performs way better than other proposed multithreading and multiprocessing approaches. It takes just 2.22 seconds as compared to 7.60 seconds in the multithreading interleaved approach and 556.78 in the traditional PoW [69] approach (with serial execution) for difficulty level 7. In the case of difficulty level 8, results are even better: 462.11 in multiprocessing interleaved approach, 536.25 in the case of multiprocessing progressive approach, and 2209.52 seconds in the case of Algorithm 1-based PoW mining.

The multithreading interleaved approach performs better than the multithreading progressive approach, but its performance is not up to the mark as compared to Algorithm 1-based PoW and multiprocessing progressive approach. Mining is a complex task, so any multithreading approach will not work better, but if we have a simple problem of finding a solution in any domain, we can improve performance through a multithreading interleaved approach. The multiprocessing progressive approach performs better than Algorithm 1-based PoW and multithreading progressive approach; this is because processes can perform better on complex tasks. It can be seen in Table 6 that as the difficulty levels increase the performance of the multiprocessing progressive approach, it becomes better as it takes 536.28 seconds to mine a block of 8 difficulty level as

| Difficulty level | Nonce value | Time in seconds |
|------------------|-------------|-----------------|
| 1                | 9           | 0.0019996166229248047 |
| 2                | 29          | 0.015625476837158203 |
| 3                | 1985        | 0.003113746430664062 |
| 4                | 9433        | 0.008895532989501953 |
| 5                | 166408      | 0.08794569969177246 |
| 6                | 27688014    | 14.330108404159546 |
| 7                | 260538310   | 132.9916124343872 |
| 8                | 1015800503  | 536.2866580486298 |

| Difficulty level | Nonce value | Time in seconds |
|------------------|-------------|-----------------|
| 1                | 9           | 0.00000000000000000000 |
| 2                | 29          | 0.015624523162841797 |
| 3                | 1985        | 0.03897666931152344 |
| 4                | 9433        | 0.0529682362609863 |
| 5                | 166408      | 0.8890793323516846 |
| 6                | 27688014    | 38.5037682056427 |
| 7                | 260538310   | 838.6467852592468 |
| 8                | 1015800503  | 2861.722503242493 |

Figure 6: GPU-based process of interleaved approach.
compared to 2861.72 seconds in the multithreading progressive approach and 2209.52 seconds in traditional PoW.

In the multithreading progressive approach, the time taken for mining is almost similar to Algorithm 1-based PoW for 1–4 difficulty levels, but the performance of the multithreading progressive approach is not better for higher difficulty levels; this is because the threads work better on simple tasks and in case complex problems performance of multithreading decreases.

We can conclude from CPU processing that the multiprocessing interleaved approach is the best one and reduces the time consumption of the PoW mining process. Comparative analysis of all mentioned techniques is given in Figures 7–9.

4.2.2. Energy Consumption. Intel(R) Core(TM) i7-3770 CP consumes the power of 146.4 W wattage [70], and if we multiply 0.1464 by the time consumed in hours in the mining process, we can get the energy consumption in kWh.

We did the energy consumption comparison of Algorithm 1-based PoW, multiprocessing progressive, and multiprocessing interleaved approach. For difficulty levels
from 1 to 6, the energy consumption of all three is almost equal, but if we go to higher difficulty levels of 7 and 8, then there is a significant decrease in energy consumption in the proposed techniques. The performance of the multiprocessing progressive approach is 4 times better than PoW for 7 and 8 difficulty levels, and multiprocessing interleaved performed almost 5 times better than traditional PoW in case of energy consumption. Figure 10 elaborates the energy consumption in the CPU.

4.3. GPU-Based Results. Time consumption and energy consumption results show that the proposed multiprocessing interleaved approach is the best performing technique on both CPU and GPU.

4.3.1. Time Consumption. Similar to CPU, GPU produced the best results in the interleaved approach. We performed interleaved technique by varying the number of processes and analyzed that GPU produced better results with 32 parallel processes. Figure 11 shows the PoW and interleaved results, while Figure 12 shows the change in results with the change of the number of processes. We did the experiment with 8, 16, 24, 32, and 40 processes but obtained optimal results with 32 processes. This is because the CPU GPU synchronization in task completion for 32 processes is a perfect match, while in 8, 16, 24, and 40, one of them has to wait for the other to start its assigned tasks.

4.3.2. Energy Consumption. NVIDIA GeForce RTX 2060 GPU consumes the energy of 480 wattage [71], and by multiplying 0.480 with the time consumed (in hours) in the mining process, we can get the energy consumption in kWh.

We picked some high values for nonces to calculate energy consumption at it was almost zero for smaller nonce values. Figure 13 shows the results of the experiment of energy consumption in kWh and the same as CPU, GPU also performing 4 times better in the multiprocessing interleaved approach.

5. Conclusion

Parallel processing is used to solve numerous complex problems and can also be used in blockchain mining to make it faster. PoW mining is a famous blockchain mining protocol and is being used in many blockchain-based systems; however, due to its complex nature, it has time and energy consumption issues. To improve these issues, we built two parallel processing-based PoW solo mining algorithms, in which multiple processes solve a complex mathematical puzzle on different nonce values. Pool mining can be affected by different types of attacks; hence, in our proposed algorithms, we encourage fast solo mining instead of pool
mining. The results indicate that the proposed solo mining algorithms perform much better than sequential PoW mining. We conclude that if a public blockchain system chooses to adopt solo mining with better performance, our proposed multiprocessing interleaved algorithm could prove to be beneficial.

**Data Availability**

There is no data provided for publication in this paper.

**Conflicts of Interest**

The authors declare that they have no conflicts of interest.

**References**

[1] J. Golosova and A. Romanovs, “The advantages and disadvantages of the blockchain technology,” in Proceedings of the 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), pp. 1–6, IEEE, Vilnius, Lithuania, November 2018.

[2] F. Longo, L. Nicoletti, A. Padovano, G. d’Attri, and M. Forte, “Blockchain-enabled supply chain: an experimental study,” Computers & Industrial Engineering, vol. 136, pp. 57–69, 2019.

[3] M. Höllbl, M. Kompara, A. Kamisilić, and L. N. Zlatolas, “A systematic review of the use of blockchain in healthcare,” Symmetry, vol. 10, no. 10, 2018.

[4] T. McGhin, K. Choo, C. Z. Liu, and D. He, “Blockchain in healthcare applications: research challenges and opportunities,” Journal of Network and Computer Applications, vol. 135, pp. 62–75, 2019.

[5] O. B. Almeida, M. C. Rodriguez, T. C. Samaniego, E. G. Ferruzola, R. N. Cabezas, and W. V. Bazán, “Blockchain in agriculture: a systematic literature review,” in Proceedings of the International Conference on Technologies and Innovation, pp. 44–56, Springer, Guayaquil, Ecuador, November 2018.

[6] A. Kamilaris, A. Fontis, and F. X. Prenafeta-Boldú, “The rise of blockchain technology in agriculture and food supply chains,” Trends in Food Science & Technology, vol. 91, pp. 640–652, 2019.

[7] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system,” Technical Report, Bitcoin, Manubot, 2019.

[8] A. Baliga, “Understanding blockchain consensus models,” Persistent, vol. 4, pp. 1–14, 2017.

[9] J. Göbel, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor, “Bitcoin blockchain dynamics: the selfish-mine strategy in the presence of propagation delay,” Performance Evaluation, vol. 104, pp. 23–41, 2016.

[10] A. Gervais, G. O. Karaame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, “On the security and performance of proof of work blockchains,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 3–16, Vienna, Austria, October 2016.

[11] L. Kugler, “Why cryptocurrencies use so much energy,” Communications of the ACM, vol. 61, no. 7, pp. 15–17, 2018.

[12] Q. Bai, X. Zhou, X. Wang, Y. Xu, X. Wang, and Q. Kong, “A deep dive into blockchain selfish mining,” in Proceedings of the 2019 IEEE International Conference on Communications (ICC), pp. 1–6, IEEE, Shanghai, China, May 2019.

[13] M. Saad, L. Nijlla, C. Kamhoua, and A. Mohaisen, “Countering selfish mining in blockchains,” in Proceedings of the 2019 International Conference on Computing, Networking and Communications (ICNC), pp. 360–364, IEEE, Honolulu, HI, USA, February 2019.

[14] R. Zhang and B. Preneel, “Publish or perish: a backward-compatible defense against selfish mining in bitcoin,” in Proceedings of the Cryptographers’ Track at the RSA Conference, pp. 277–292, Springer, San Francisco, CA, USA, February 2017.

[15] U. W. Chohan, “The double spending problem and cryptocurrencies,” 2017.

[16] K. Sai and D. Tipper, “Disincentivizing double spend attacks across interoperable blockchains,” in Proceedings of the 2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), pp. 36–45, IEEE, Los Angeles, CA, USA, December 2019.

[17] J. Bae and H. Lim, “Random mining group selection to prevent 51% attacks on bitcoin,” in Proceedings of the 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W), pp. 81–82, IEEE, Luxembourg, Luxembourg, June 2018.

[18] X. Yu, M. T. Shiwen, Y. Li, and R. D. Huijie, “Fair deposits against double-spending for bitcoin transactions,” in Proceedings of the 2017 IEEE Conference on Dependable and Secure Computing, pp. 44–51, IEEE, Taipei, Taiwan, August 2017.

[19] H. Sun, N. Ruan, and C. Su, “How to model the bribery attack: a practical quantification method in blockchain,” in Proceedings of the European Symposium on Research in Computer Security, pp. 569–589, Springer, Guildford, United Kingdom, September 2020.

[20] J. Bonneau, “Why buy when you can rent?” in Proceedings of the International Conference on Financial Cryptography and Data Security, pp. 19–26, Springer, Christ church, Barbados, February 2016.

[21] T. Guggenberger, V. Schlatt, J. Schmid, and N. Urbach, “A structured overview of attacks on blockchain systems,” in Proceedings of the Pacific Asia Conference on Information Systems (PACIS), Dubai, UAE, July 2021.

[22] P. McCorry, S. F. Shahandashti, and F. Hao, “Refund attacks on bitcoin’s payment protocol,” in Proceedings of the International Conference on Financial Cryptography and Data Security, pp. 581–599, Springer, Christ church, Barbados, February 2016.

[23] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Nijlla, “Security implications of blockchain cloud with analysis of block withholding attack,” in Proceedings of the 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), pp. 458–467, IEEE, Madrid, Spain, May 2017.

[24] S. Solat and M. Potop-Butucaru, “Zeroblock: preventing selfish mining in bitcoin,” 2016, https://arxiv.org/abs/1605.02435.

[25] C. Natoli and V. Gramoli, "The balance attack or why forkable blockchains are ill-suited for consortium," in Proceedings of the 2019 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 579–590, IEEE, Denver, CO, USA, June 2017.

[26] C. Natoli and V. Gramoli, “the balance attack against proof-of-work blockchains: The r3 testbed as an example,” 2016, https://arxiv.org/abs/1612.09426.

[27] V. Gramoli, The Red Belly Blockchain. personal Communication, Facebook, USA, 2017.

[28] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: generalizing selfish mining and combining with an eclipse attack," in Proceedings of the 2016 IEEE European Symposium
on Security and Privacy (EuroSéP), pp. 305–320, IEEE, Saarbruecken, Germany, March 2016.

[29] A. Grama, V. Kumar, A. Gupta, and G. Karypis, Introduction to Parallel Computing, Pearson Education, London, United Kingdom, 2003.

[30] J. Kan, S. Chen, and X. Huang, “Improve blockchain performance using graph data structure and parallel mining,” in Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), pp. 173–178, IEEE, Shenzhen, China, August 2018.

[31] S. S. Hazari and Q. H. Mahmoud, “A parallel proof of work to improve transaction speed and scalability in blockchain systems,” in Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0916–0921, IEEE, Las Vegas, NV, USA, January 2019.

[32] X. Boyen, C. Carr, and T. Haines, “Blockchain-free cryptocurrencies: a rational framework for truly decentralised fast transactions,” IACR Cryptology ePrint Archive, vol. 2016, 2016.

[33] G. T. Nguyen and K. Kim, “A survey about consensus algorithms used in blockchain,” Journal of Information processing systems, vol. 14, 2018.

[34] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, “Survey of consensus protocols on blockchain applications,” in Proceedings of the 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1–5, IEEE, Coimbatore, India, January 2017.

[35] Litecoin, “Litecoin - open source p2p digital currency,” 2020, https://litecoin.org/.

[36] Medium, “The fastest cryptocurrency transaction speeds for 2018 by crypto account builders medium,” 2021, https://medium.com/@johnhinkle_80891/the-fastest-cryptocurrency-transaction-speeds-for-2018-498c1ba87cf.

[37] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen, and E. Dutkiewicz, “Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities,” IEEE Access, vol. 7, Article ID 85727, 2019.

[38] Navcoin, “Navcoin - an easy to use decentralized cryptocurrency,” 2021, https://navcoin.org/en.

[39] Stratis, “Stratis blockchain development platform,” 2021, https://www.stratisplatform.com/.

[40] A. Wahab and W. Mehmood, “Survey of consensus protocols,” 2018, https://arxiv.org/abs/1810.03357.

[41] Waves, “Waves.tech,” 2021, https://waves.tech/.

[42] S. M. S. Saad and R. Z. R. M. Radzi, “Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos),” International Journal of Integrated Care, vol. 10, 2020.

[43] Lisk, “Lisk blockchain application platform lisk,” 2021, https://lisk.io/.

[44] ARK, “The simplest way to blockchain,” 2021, https://ark.io/.

[45] EOSIO, “Eosio blockchain software & services,” 2021, https://eos.io/.

[46] A. Andrey and C. Petr, “Review of existing consensus algorithms blockchain,” in Proceedings of the 2019 International Conference “Quality Management, Transport and Information Security, Information Technologies”(IT&QM&IS), pp. 124–127, IEEE, Sochi, Russia, September 2019.

[47] Q. He, N. Guan, M. Lv, and W. Yi, “On the consensus mechanisms of blockchain/dlt for internet of things,” in Proceedings of the 2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES), pp. 1–10, IEEE, Graz, Austria, June 2018.

[48] NEM, “Nem ecosystem blockchain - because together, everything is possible,” 2021.

[49] D. Wang, C. Jin, H. Li, and M. Perkowski, “Proof of activity consensus algorithm based on credit reward mechanism,” in Proceedings of the International Conference on Web Information Systems and Applications, pp. 618–628, Springer, Guangzhou, China, September 2020.

[50] Decred, “Decred - secure. adaptable. sustainable,” 2021, https://decred.org/.

[51] Espers, “Espers - web3 fractal engine,” 2021, https://espers.io/.

[52] A. and Y. Lu, “On security analysis of proof-of-elapsed-time (poet),” in Proceedings of the International Symposium on Stabilization, Safety, and Security of Distributed Systems, pp. 282–297, Springer, Boston, MA, USA, November 2017.

[53] B. Hyperledger, “Hyperledger sawtooth – hyperledger,” 2021, https://www.hyperledger.org/use/sawtooth.

[54] Z. Zhang, D. Zhu, and W. Fan, “Qpbft: practical byzantine fault tolerance consensus algorithm based on quantified-role,” in Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 991–997, IEEE, Guangzhou, China, December 2020.

[55] A. Hyperledger, “Hyperledger fabric – hyperledger,” 2021, https://www.hyperledger.org/use/fabric.

[56] Y. Meng, F. Lu, Y. Liu, and X. Huang, “Attacks and countermeasures on blockchains: a survey from layering perspective,” Computer Networks, vol. 191, Article ID 107978, 2021.

[57] M. Saad, J. Spaulding, L. Njilla et al., “Exploring the attack surface of blockchain: a comprehensive survey,” IEEE Communications Surveys & Tutorials, vol. 22, pp. 1977–2008, 2020.

[58] C. Decker and R. Wattenhofer, “Bitcoin transaction malleability and mtgox,” in Proceedings of the European Symposium on Research in Computer Security, pp. 313–326, Springer, Wrocław, Poland, September 2014.

[59] A. M. Khalifa, A. M. E. Bahaa, and M. A. Sobh, “Quantum attacks and defenses for proof-of-stake,” in Proceedings of the 2019 14th International Conference on Computer Engineering and Systems (ICCES), pp. 112–117, IEEE, Cairo, Egypt, December 2019.

[60] U. Javaid, A. K. Siang, M. N. Aman, and B. Sikdar, “Mitigating bot device based ddos attacks using blockchain,” in Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, pp. 71–76, Munich, Germany, June 2018.

[61] E. Heilmann, A. Kendler, A. Zohar, and S. Goldberg, “Eclipse attacks on bitcoin’s peer-to-peer network,” in Proceedings of the 24th USENIX Security Symposium (USENIX Security 15), pp. 129–144, Washington D.C., USA, August 2015.

[62] J. R. Douceur, “The sybil attack,” in Proceedings of the International Workshop on Peer-To-Peer Systems, pp. 251–260, Springer, Cambridge, MA, USA, March 2002.

[63] M. Apostolaki, A. Zohar, and B. Sikdar, “Hijacking bitcoin: routing attacks on cryptocurrencies,” in Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), pp. 375–392, IEEE, San Jose, CA, USA, May 2017.

[64] A. Andreyukhin, “Phishing attacks and preventions in blockchain based projects,” in Proceedings of the 2019 International Conference on Engineering Technologies and Computer Science (EnT), pp. 15–19, IEEE, Moscow, Russia, March 2019.

[65] I. Eyal and E. G. Sirer, “Majority is not enough: bitcoin mining is vulnerable,” Financial Cryptography and Data Security,
Springer, in Proceedings of the International Conference on Financial Cryptography and Data Security, pp. 436–454, March 2014.

[66] J. Gao, H. Liu, C. Liu, Q. Li, Z. Guan, and Z. Chen, “Easyflow: keep ethereum away from overflow,” in Proceedings of the 2019 IEEE/ACM 41st International Conference on Software Engineering: Companion Proceedings (ICSE-Companion), pp. 23–26, IEEE, Montreal, QC, Canada, May 2019.

[67] Y. Feng, E. Torlak, and R. Bodik, "Precise attack synthesis for smart contracts," 2019, https://arxiv.org/abs/1902.06067.

[68] T. Kim, J. Noh, and S. Cho, "Scc: storage compression consensus for blockchain in lightweight iot network," in Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), pp. 1–4, IEEE, Las Vegas, NV, USA, January 2019.

[69] D. V. Flymen, “Proof of work,” in Learn Blockchain by Building One, pp. 39–53, Springer, 2020.

[70] Anandtech, "Power consumption - the intel ivy bridge (core i7 3770k) review,” 2021, https://www.anandtech.com/show/5771/the-intel-ivy-bridge-core-i7-3770k-review/20.

[71] Realhardtechx, "Psu requirements - realhardtechx," 2020, https://www.realhardtechx.com/.