Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2022) 30: 406 – 419

doi:10.3906/elk-2105-217

Block size optimization for PoW consensus algorithm based blockchain applications by using whale optimization algorithm

Betül AYGÜN[1*], **Hilal ARSLAN**[2]

[1]Management Information System, İİBF, İzmir Demokrasi University, İzmir, Turkey
[2]Department of Software Engineering,Faculty of Engineering and Natural Science,
Ankara Yıldırım Beyazıt University, Ankara, Turkey

Received: 21.05.2021 • **Accepted/Published Online:** 25.12.2021 • **Final Version:** 04.02.2022

Abstract: Blockchain-based applications come up with cryptocurrencies, especially Bitcoin, introducing a distributed ledger technologies for peer-to-peer networks and essentially records the transactions in blocks containing hash value of the previous blocks. Block generation constitutes the basis of this technology, and the optimization of such systems is among the most crucial concerns. Determining either the block size or the number of transactions in the block brings out a remarkable problem that has been solved by the miners in recent years. First, higher block size results in higher transaction time, on the other hand, smaller block size has many disadvantages such as security, lower transaction fees, lower transaction numbers in a given time interval, which makes it unable to compete with other currency systems due to this bulky structure and higher block generation time. In this study, multiobjective optimization problem (OP) is proposed by minimizing block generation and transmission time. This multiobjective OP is transformed into a single OP by applying weighted sum method. To determine the optimal block size, particle swarm optimization (PSO) algorithm and whale optimization evolutionary algorithm (WOA) are employed. Although both algorithms have capability to reach optimum block size and corresponding time, WOA achieves better performance than PSO in terms of the convergence speed and output fluctuation. Moreover, analysis of the prediction of optimum block size is carried out under different weights which creates many optimization functions. Experimental results indicate that if higher weight is assigned to the transmission time, then block size decreases sharply. Furthermore, the experimental results reveal that design of the blockchain network and number of nodes in network profoundly affect the block size selection due to the time constraints.

Key words: Blockchain, block size, whale optimization algorithms, particle swarm optimization

1. Introduction

The blockchain technology, which is conspicuoused with popular cryptocurrencies principally Bitcoin, has begun to be used widely in several areas only for financial sectors but also for health industries as well as supply chain management sectors. It is a kind of a distributed ledger technology which holds identical copy of the transactions across participants in a network. The immutability, security, transparency, and decentralization are the primarily advantages persuading volunteer organizations for adopting this innovation technology. However, it has not found a wider application area right now as a result of its lower performance [1]. Cryptocurrency transaction requires a lot of time for being transferred across addresses when compared to online payment systems such as VISA processing almost 2000 transactions per second. For the time being, as Reddy et al. stated that Bitcoin roughly suffers from lower transaction rates (3-7 transaction per second), which makes it difficult to be adopted in any financial service [2].

*Correspondence: betul.aygun@idu.edu.tr

In brief, blockchain is the integration of chains of each block and blocks are linked together by holding the hash value of the previous block. Each block contains certain information: size, number of transactions, transactions itself and block header [3]. To generate new blocks on the chain, all parties on the chain network come to a common agreement to write transactions on to the ledger. There are many protocols for the consensus of the participants called as consensus algorithms. To generate an efficient blockchain, consensus algorithms take the essential part of it [4].

Proof of Work (PoW) and Proof of Stake (PoS) protocols are widely adopted in many blockchain networks such as Bitcoin, Ethereum, and Litecoin. However, PoW based consensus algorithms suffers from lower transaction per second (tps), which causes the blockchain scalability bottleneck problem. [5, 6]. To overcome this problem, increasing block size seems to be a logical step for maximizing the number of transactions in blockchain based networks. The block size as well as block creation time are focused on achieving the scalability of the Bitcoin as the key parameters [7]. As claimed by the studies of Khan et al. and Scherer, block size has a crucial role in determining the overall performance of the proposed system [1, 8]. Furthermore, Jiang and Wu claimed that higher block size increases the transaction fee, but it reduces the probability representing successfully mined blocks [9].

While the blocks with large size improve transaction fees as well as the overall performance, they decreases time for the block generation. This may result in less decentralization due to the fact that nodes having lower bandwidth cannot compete with other ones having higher computing sources. This low competition weakens blockchain security [10]. Moreover, the blocks with large size increase the number of blocks that are not included in the chain called as stale blocks. In PoW network, once the block is created, it is distributed through the node network. Hence, increasing block size requires more time for transferring the blocks. As Gemeliarana claimed that smaller block size results in less propagation time [10]. Furthermore, it decreases the security and increases the centralization [11].

Dimitri [12] stated that block size optimization solves the trade off between maximization of the revenue and becoming as an alternative payment system. Moreover, there is a trade off in selecting block size between security and speed in building an encryption of cryptographic hash function. If block size is smaller, then security becomes an important issue (Birthday paradox; if the block size is bigger, then speed of hashing and transmission of it becomes an issue. From the point of miners, using large block size results in higher transaction fees. However, block transmission is a critical issue, thus, determining an optimal block size becomes an important debate in cryptocurrencies and even blockchain based networks. As claimed so far, both large and small block sizes introduce several problems.

As it is clearly stated, transmission time, block generation time, Merkle tree construction time and transaction fees are the blockchain parameters that depend on block size. In this study, we focus on determining optimum block size and aim to improve time for generating the block(s) in PoW blockchain systems. For this reason, delay and block generation time is considered as an objective function. We note that the transaction fee and security is out of the scope of this approach. Considering the delay objective function, higher block size results in higher transmission time, however, for block generation time, higher block size causes lower time. To solve this trade off, we determine two objective functions to achieve an optimum block size while minimizing the time value.

For the solution of the optimization problems, particle swarm optimization (PSO), ant colony optimization (ACO), and genetic algorithm of bio-inspired heuristic algorithms have been preferred mainly in the literature over the last decade. Furthermore, the Whale Optimization Algorithm (WOA), a bio-inspired metaheuristic

algorithm, is proposed, and its various variants are quickly adopted in the literature. When the literature is dogged deeper, a slew of different WOA applications, including feature selection, optimization, clustering algorithms, and unit commitment, are found to overcome various types of optimization problems. When comparing the other metaheuristics, WOA has some advantages. First, it requires few parameters to be tuned. Second, It balances between exploitation and exploration. Finally, it has clear frameworks [13]. Considering these advantages over other metaheuristics, WOA is used to reach the optimum solution in this study. Furthermore, we apply PSO algorithm to demonstrate the efficiency of the proposed method. We apply the weighted sum method to solve multi objective optimization problem. Since it is difficult to obtain weight vectors, several different weights for the problem is analyzed in the Results and Discussion section.

In our study, the size of the blocks across network, remarkably prominent topic on blockchain networks, is determined. To achieve this, the mathematical optimization problem of the time estimation for both blocks generation and transmission time is proposed. For the construction of the model, block size, mempool transaction size, Merkle tree construction time, overhead of block time, performances of the miners are granted as parameters. Furthermore, WOA is employed to minimize the time required to generate blocks containing transactions in memory pool. The results are compared with the results of PSO algorithm. The main contributions stated in this study are given below:

- Proposing a mathematical optimization problem minimizing both transmission time and block generation time,
- Solving this multi-objective optimization problem with a fairly new heuristic technique, WOA, and comparing it with the well-know PSO technique.

The remainder of the paper is organised as follows: Section 2 describes the related works about block size optimization and evolutionary algorithms in the literature. In Section 3, multiobjective mathematical optimization problem is represented, and whale optimization evolutionary algorithm used for solving this problem is detailed. In Section 4, the results of the proposed method is given and compared to the results of PSO algorithm. Eventually, Section 5 summarises the study with suggesting several studies for future work.

2. Literature review

Although block size makes the problem sophisticated in cryptocurrency Bitcoin mining process, there are few studies optimizing the block size in blockchain based systems in the literature. Singh et al. [14] defined a multi objective problem, which minimizes the transaction time and block generation time. They used the multiobjective particle swarm optimization technique to solve the problem [14]. They claimed that Pareto front solution, one of the approaches for the solution of multiobjective optimization problems, is suitable for the block size optimization problem, and they used it to solve the problems stated in the study.

Khan et al. [8] discussed the performance of the blockchain based secure e-voting system. They focused on the performance and scalability constraints under the population size, block size, block generation rate as well as transaction speed. They claimed that block size has a profound role in determining the overall performance and scalability of the blockchain based solutions. In conjunction with block size, number of transactions in the block and block generation rate has important effects on the blockchain based systems. However, there is a trade-off between the block size, block generation rate, and transaction processing speed. In the study of Cao, different consensus algorithms such as PoW, PoS, and DAG (Direct Acyclic Graph) were analyzed technically in terms of the block generation average time, the confirmation delay and the transaction per second [15]. The

blockchain technology, which is conspicuoused with popular cryptocurrencies principally Bitcoin, Reddy [2] and Sharma [16] modelled the block propagation time in the Bitcoin networks. Their model is used as one of the objectives that are minimized to reach an optimum block size during our study. Croman et al. [17] propose one of the leading works in the scalability of blockchain based systems. This study gives several practical limitations such as latency, throughput, bootstrap time and cost per transactions. These parameters and their effects on networks are defined practically and generally. It is a good guide to realise the scalability issues. Nonetheless, in their study, latency and throughput was not optimized in a mathematical manner theoretically. On the other side, Kim et al. [18] considered scalability issue of Bitcoin under three categories; throughput, cost as well as capacity and categorized solutions into classes as on-chain, off-chain, child-chain and inter-chain. Gervais et al. [19] also discussed the block size effects on block propagation time, stale block rate, block generation interval and an adversary. By simulation experiments, it was claimed that bock size has a great effect on propagation time.

In this study, we focus on increasing the performance of the blockchain networks having PoW consensus by optimizing the block size and minimizing the delay. Although there are various studies on block propagation and transmission time, they are not considered from the point of the optimum value for block size. Moreover, they have not also considered the block creation time, which consists of the Merkle tree generation time and overhead for each block, which are the factors that are considered in our study. Expected mining time depending on target difficulty and computational power of miners is out of this study due to the fact that they are not depended on the block size. On the other hand, block size restriction determines the TPS, which is considered as one of the parameter that are optimized during this study. In this study, multiobjective problem is defined for optimizing the block size. The aim of the optimization problem is to improve the performance of the blockchain based networks having PoW consensus.

3. Methodology

3.1. Problem Formulation

In this section, a mathematical model for the optimization problem is defined. The aim of the optimization problem is to increase the block size while reducing transmission and the time to generate blocks. Generally, each block contains certain information regarding to block size, block header, transactions, and total number of transactions. Block header contains hash value of the previous block, timestamp, Merkle root, difficulty target and nonce value [3]. Among these criteria, size (number of transactions) with Merkle tree generation, which depends on the block size, is required to be optimized to generate block in blockchain-based networks in a shorter time with a higher security. Moreover, in PoW consensus networks, the header of the block is only hashed instead of the transactions in the block. For this reason, hashing time does not depend on the size of the blocks. On the other hand, for the creating of Merkle tree, full transactions in the block, which mainly depends on the block size, have to be hashed.

In brief, there are two critical metrics for the maximization of the block size, which are block transmission time and block generation time. Furthermore, for the blockchain networks, propagation delay is another issue that have been optimized in several studies [20]. In this study, the propagation and transmission time is called as delay. If the block size is high, the propagation and transmission time will increase, while the block generation time will decrease. Otherwise, while small block sizes reduce the transmission time, total block generation time will increase, as too many blocks will exist to cover all transaction in the memory pool. As a result, the balance between these delay times, which will be discussed in detail in this study, requires optimization of block sizes.

The problem is transformed to multiobjective optimization problem. The block building time is computed as in Equation 1 [21]. Memory pool is the number of total transactions achieved in Bitcoin transactions waiting to be confirmed. In Equation 1, S_{mem} represents the total size of memory pool. If the size of each block is S_b, then S_{mem}/S_b is number of blocks generated. Assume that each block overhead timing is unique and contains $S_{overhead}$ size of data. Thus, total building time for block at that memory pool transactions is mainly equal to the multiplication of the summation of overhead time and Merkle tree construction with number of blocks. Merkle tree is a crucial part of the blockchain technology.

$$T_b = \frac{S_{mem}}{S_b}.(T_{overhead} + (\frac{Tot_t}{MerkTree_t} \times T_{merkle}) \tag{1}$$

Merkle tree construction time is computed by using the number of transactions in the block. Thus, the block size should be converted to number of transactions included in that block. Assume that the size of each transaction is represented as S_t. Then, transaction number is equal to $Tot_t = \frac{S_b}{S_t}$. $MerkTree_t$ is the number of transactions in the Merkle tree. In this study, the number of transaction is fixed to 10. $Tot_t/MerkTree_t$ represents the number of merkle tree that would be constructed. The time for creating Merkle tree with 10 transactions is stated as T_{merkle} and its value is expected to 0.02 seconds.

Furthermore, block size is another crucial parameter for the network propagation and transmission delay. The delay that depends on block size is formulated in Equation 2 [2, 16, 22, 23] where h is depth of the tree of the blockchain network and R is the bandwidth of the node. In this study, we assume that R is equal for each node in the blockchain. N_T is the number of miners connected to that node, and the formula to evaluate it is Formula 3. The depth of the tree is obtained by using the Formula 4.

$$T_d = h(T_p + \frac{S_b}{R}.N_T) \tag{2}$$

$$N_T = (n-1).P_e \tag{3}$$

$$h = log_\mu(n.(N_T - 1) + 1) \tag{4}$$

On account of the fact that we have two objective functions that are minimized, weighted sum method is used to transform multiobjective optimization problem into a single objective optimisation function. The objective function, O, is formulated as below. The aim of this study is to find optimum block size by minimizing the objective function O.

$$O = \vec{w}.T_d + (1 - \vec{w}).T_b \tag{5}$$

All the notations used in the previous formulas are stated in Table 1.

3.2. Whale optimization algorithm

To solve the multiobjective optimization problem, weighted sum method that transforms multiobjective problem into single objective by choosing different weights in proportion to the relative importance of the objective functions is applied. The problem is solved by using the newly proposed optimization algorithm, WOA. Moreover, PSO algorithm is used and compared with WOA algorithm with respect to convergence speed. One reason for choosing these algorithms is that they are robust, simple, and powerful [24]. Furthermore, WOA

Table 1. Notation definitions.

Symbol	Definition
T_b	Block generation time
S_{mem}	Mempool size
S_b	Block size
$T_{overhead}$	Total time for overheading
Tot_t	Total number of transaction in block
$MerkTree_t$	Number of transactions in Merkle Tree
T_{merkle}	Merkle Tree construction time
S_t	Size of transaction
T_d	Delay for block creation
h	Depth of the tree
T_p	Processing time
N_T	Number of connected nodes
n	Total number of nodes

for solving the objective problem requires few parameters to be tuned and balances between exploitation and exploration without being trapped in local optima [25].

WOA is a bio-inspired heuristic algorithm that first proposed in the study of [26]. It mimics the hunting behaviour of humpback whales. The position of agents is updated according to the leader position in each iteration. The leader among the humpback whales is a whale closest to the prey, i.e. the one having the best fitness value in the optimization problem.

There are two phases: exploitation and exploration. According to the value of $|A|$, computed using Equation 7, the phase is decided if it is smaller than 1, then exploration phase is begun; otherwise, exploitation phase is started. $|A|$ value is calculated according to a value given in Equation 6 which is linearly reducing vector in each iteration and $\vec{r}$ value, uniformly distributed random number.

$$\vec{a} = 2(1 - i/MaxIter) \tag{6}$$

$$\vec{A} = 2.\vec{a}.\vec{r} - \vec{a} \tag{7}$$

In the exploitation phase, whales can update their position in two different ways: shrinking encircling position update and spiral position update according to the randomly created number N_r. The formulas for the exploitation phase for the WOA algorithm are given in equation 8. $\vec{X}$ is used as the position of the whale agent. Star is used to represent the position of the leader having closest distance to the prey. $\vec{C}$ value is computed according to the $\vec{r}$ value constructed to evaluate $\vec{A}$ vector and given in Equation 8. $\vec{D}$ and $\vec{D'}$ are distance vectors between the positions of agent and leader. The equations for $\vec{D}$ and $\vec{D'}$ are given in Equation 10 and 11, respectively.

$$\vec{X}(i+1) = \begin{cases} \vec{X}^*(i) - \vec{A}.\vec{D} & if N_r < 0.5 \\ \vec{D'}.e^{bl}.cos(2.pi.l) + \vec{X}^*(i) & if N_r >= 0.5 \end{cases} \tag{8}$$

$$\vec{C} = 2.\vec{r} \tag{9}$$

$$\vec{D} = |\vec{C}.\vec{X}^*(i) - \vec{X}(i)| \tag{10}$$

$$\vec{D}' = |\vec{X}^*(i) - \vec{X}(i)| \tag{11}$$

In the exploration phase, shrinking encircling position update of exploitation phase is used. The formula is given in Equation 12. However, in this update, leader position is not used. Instead, randomly selected whale position is used to prevent stuck in local optima. This random value is used for the evaluation of distance vector value. The formula for distance vector is given in Equation 13. Rand is used to represent the randomly selected agents in the algorithm.

$$\vec{X}(i+1) = \vec{X}^{rand}(i) - \vec{A}.\vec{D} \tag{12}$$

$$\vec{D} = |\vec{C}.\vec{X}^{rand}(i) - \vec{X}(i)| \tag{13}$$

4. Results and discussion

In this section, the results of the optimization algorithms are presented detail. First of all, simulation parameters are described. Secondly, the results of the multiobjective optimization problem solved by both WOA and PSO heuristic algorithms with different weights are detailed. Finally, convergence and accuracy performance of the algorithms are compared. For the implementation of the heuristic algorithms, Python 3.6.4 is used.

4.1. Parameter selection

Firstly, the parameter for the blockchain network is decided. Besides, parameters of WOA and PSO are given below. The network is assumed to be unstructured directed P2P network. When a node enters the blockchain, it connects to a set of peers, and this connection are used for transaction and block propagation. We assume that 10.000 nodes (miners) exist on the network. Bandwidth of the nodes is assumed to be same and equal to 10 Mbps. Number of nodes connected to a given node is equal to 8. Furthermore, depth of the tree is evaluated according to the Formula 4 [2]. In Table 2, the blockchain network parameters are given. We used the same parameters for the blockchain system with Reddy et al.[2] and Singh et al.[21]. For the optimization algorithms, especially for PSO, parameter selection plays a crucial role in the performance of the algorithm. Moreover, the value of a in WOA also highly effects the performance of the algorithm [27]. For the PSO and WOA algorithms, parameters were selected with trial and error approach. Since the parameter selection affects the performance of the evolutionary algorithms, large number of trials are performed to get the most appropriate parameters.

4.2. Experimental results and discussion

Firstly, the delay function, T_d, and block creation time T_b is evaluated with respect to the different block size ranges between 12 Kb and 6000 Kb (almost 10 transactions to 500 transactions). The graph of both function is represented in Figure 1. As expected, when the block size increases, delay function increases linearly according to the Equation 5 created in the methodology section. On the other hand, with the increasing block sizes, since the total number of blocks covering all transactions in memory pool will decrease, it will cause decreasing

Table 2. Input values for the blockchain network and algorithmic based parameter values.

Blockchain network		Particle Swarm Optimization		Whale optimization algorithm.	
n	10.000	c_1 acceleration coef.	1.49445	a linear component	2
N_t	8	c_2 acceleration coef.	1.49445	spiral parameter	0.5
$T_{overhead}$	5 sec	weight	0.74	hunting population size	100
$MerkTree_t$	10	population size	100		
T_{merkle}	0.02 sec				
S_{mem}	96.000 Kb				
$RangeofS_b$	$[12, 600]$ Kb				
S_t	1.2 Kb				
T_p	30 msec				
R	10 Mbps				
μ	100 msec				
P_e	$8/(n-1)$				
R	1 MB				

the total block creation time and so forth; there is a trade-off between these two functions. This situation is presented with respect to different block sizes in Figure 1.

On this occasion, these two delay times are transformed into a single objective problem by weighted sum method. In the scope of this study, several optimization problems are constructed according to the different weights ranging from 0.01 to 0.99. With different weights for the objective function, transmission delay and block generation time is evaluated. While the weight (w) increases for the delay, the weight value for the block generation time (1-w) decreases. Hence, higher weight brings less delay time with higher block generation time. It emphasizes that block size should be minimized, which is the situation that affects the blockchain performance negatively. Figure 2 indicates this situation apparently.

In the first part of the Figure 2, it is obviously caught that when the weight is 0.6, delay starts to decrease, and, in the second part, block generation time starts to increase at that value. Because, according to optimum solutions, up to weight 0.6, block size is always equal to 600 Kb (maximum block size that can be achieved). When the weight increases, since keeping block size at maximum does not give the minimum cost, then optimum block size starts to decrease as demonstrated in Table 3.

The time for the transmission is reasonably long, which dominates the time for block generation. Thus, for the higher weight values in the optimization problem, which makes the transmission delay more prominent, the total time increases and block size decreases. In Table 3, when the weight increases to 1, then block size converges to 70.46 (approximately 59 transactions), which is the unintended consequence. For instance, when the delay function has a weight of 0.7, then the block size becomes 350.54 Kb.

To take an overall view, the optimum block size and corresponding total time value is shown in Figure 3. Both the results of PSO and WOA algorithm are given. In terms of achieving the optimum solution, there is no difference between these two algorithms. Up to weight value of 0.6, maximum block size is the optimum value. However, for higher weight values than 0.6, since the delay function overshadow the block generation time, the optimum time is obtained with lower block size. When the weight for the optimization problem is 0.7, the optimum value for the block size is 458,96 Kb; on the other hand, when the weight is 0.8, then optimum

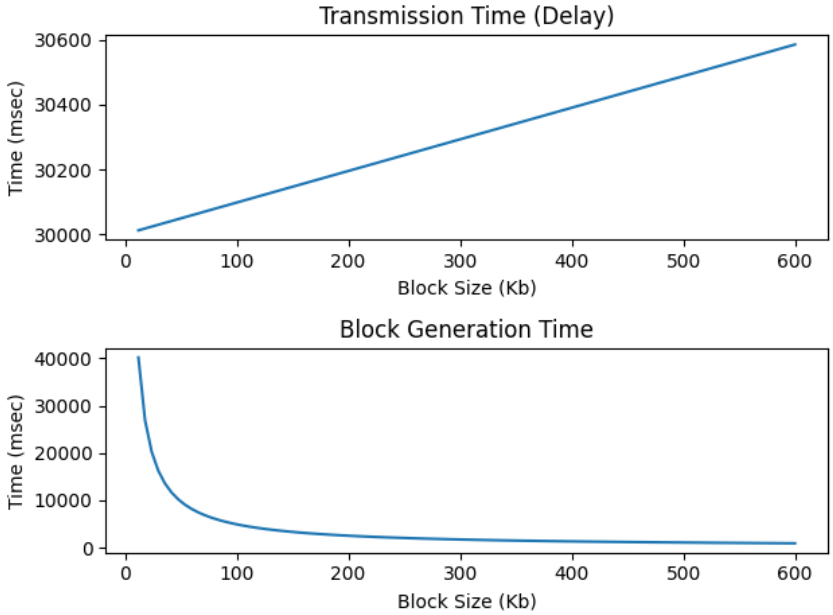

Figure 1. The relationship between the block size and delay and block generation time.

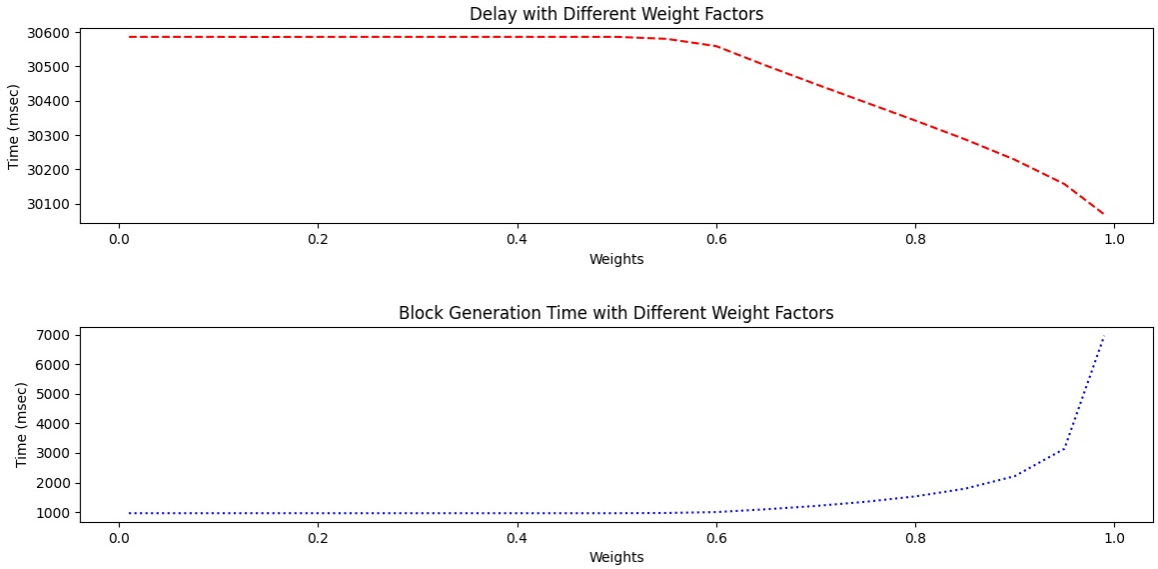

Figure 2. The relationship between the various weight values of the objective function with respect to the delay and block generation time, respectively

block size becomes 350.54 Kb. In other words, approximately, each block should contain 291 transactions to keep the total time for the block generation minimum. Even though the block size is decreased to minimize the total time, it still has higher total time as stated apparently in the second part of the Figure 3.

Concisely, delay function plays a decisive role in the block size optimization [28]. In the cases of higher weight values, which implies that delay is important, the block size reduces significantly. In the assumptions for the model, the number of nodes in blockchain network is set to 10.000, and the network is assumed to be P2P

Table 3. Optimum block size values achieved by whale optimization algorithm.

Weight	Block Size (Kb)	Total Time
0.50	600	15772.97
0.60	572.43	18734.82
0.70	458.96	21675.5
0.80	350.54	24579.72
0.90	233.69	24426.79
0.99	70.46	29837.84

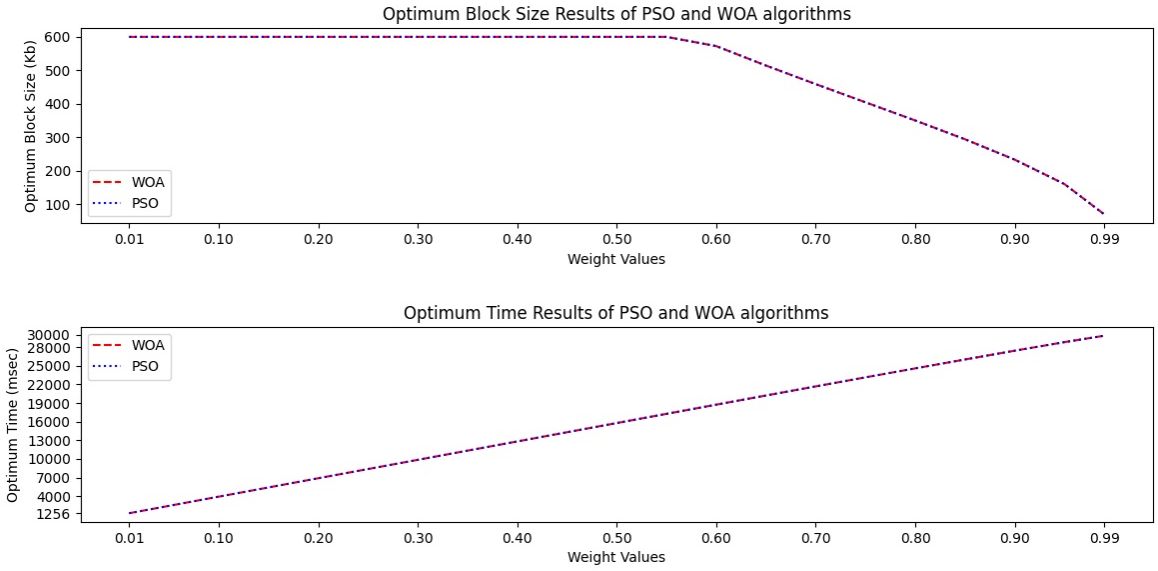

Figure 3. The relationship between the various weight values of the objective function with corresponding to the block size and total time, respectively.

network. This assumption makes the delay value higher. The blockchain network plays a vital role in delay and could be designed as decreasing the number of connection to share same amount of information to overcome this delay [29].

4.3. Comparison of the performance of the algorithms

Within the scope of this study, two optimization algorithms are applied, widely used algorithm, PSO, and the one emerged recently are used for the solution of several prominent problems in the literature, WOA. These algorithms are compared according to the performance of 100 trials with 10 population size. The analysis are figured out for two cases. In the first case, the aim is to reach optimum block size; in the second, the aim is to find optimum time estimation.

Furthermore, the accuracy performance of PSO and WOA are compared. In the scope of this study, accuracy is to obtain optimum block size while achieving the minimum delay and block generation time. These trials are carried out under different objective functions created by different weights. Figure 3 presents that

Both PSO and WOA algorithms have same efficiency in producing optimum block size and delay and block generation time under 100 iterations for different optimization functions.

Secondly, algorithms are compared according to the convergence speed, number of trials that the optimum solution is achieved. As it is seen in Figure 3, although both algorithms result in best optimum solution under long iterations, when the algorithms are executed under different iterations, the convergence to the optimum values is heavily different.

In the Figure 4, the results of the fitness value (in this case, the optimum time value) under different iteration number are shown. In the first one, PSO results under different iteration are given; in the next, the results of the WOA are represented, and the last sub figure represents the results of the both algorithms under different iterations. These sub figures prominently revealed that even under low iteration numbers, WOA yields more promising results than PSO. In spite of the fact that PSO starts with closer values to optimum solution, it has lower convergence value than the WOA algorithm. At the iteration 10, WOA obtains the optimum solution. When it is compared with PSO reaching the optimum solution at the 22^{th} iteration, it is obviously realized that it reaches best solution earlier.

From the point of optimum block size, represented in Figure 5, it is more obviously stated that WOA converges to the optimum solution faster than the PSO. WOA reaches to the optimum block size at 8^{th} iteration, however PSO reaches to the solution at 32^{th} iteration which proves that WOA has higher convergence speed than PSO.

Additionally, in the block size estimation, PSO has larger fluctuations in the optimization process in contrast to WOA having more stable process. In the Figure 5, the optimum value achieved by PSO algorithm changes sharply around 25 iteration. As stated in the paper of Li et al. [30], PSO is easily fluctuated and has a large time-varying error. As in our case too, this also makes the WOA more efficient than PSO algorithm.

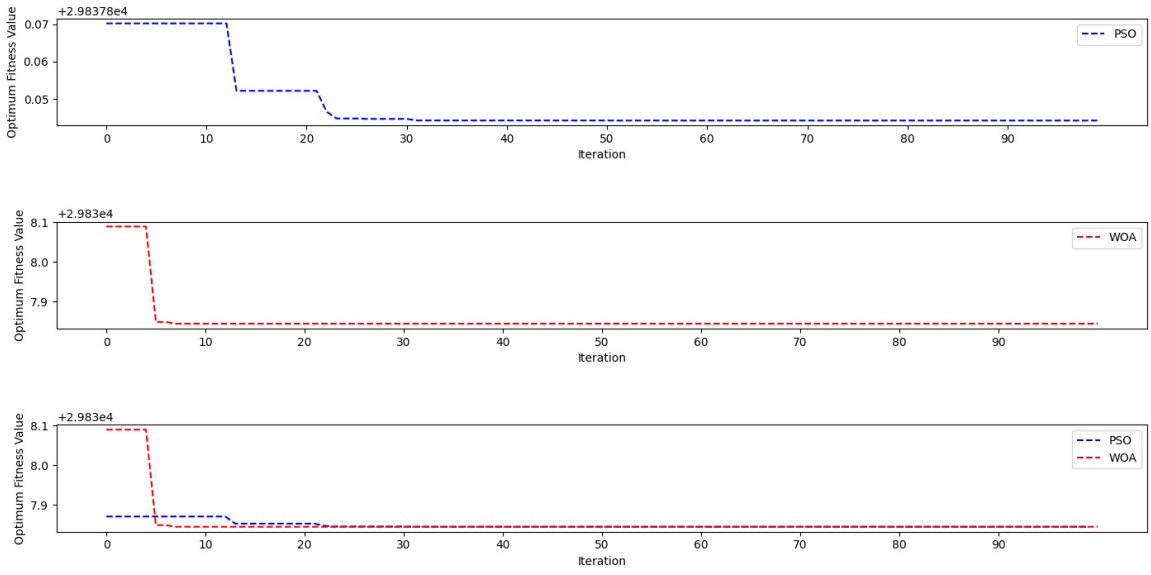

Figure 4. The block size convergence of the PSO and WOA algorithms according to the number of iterations.

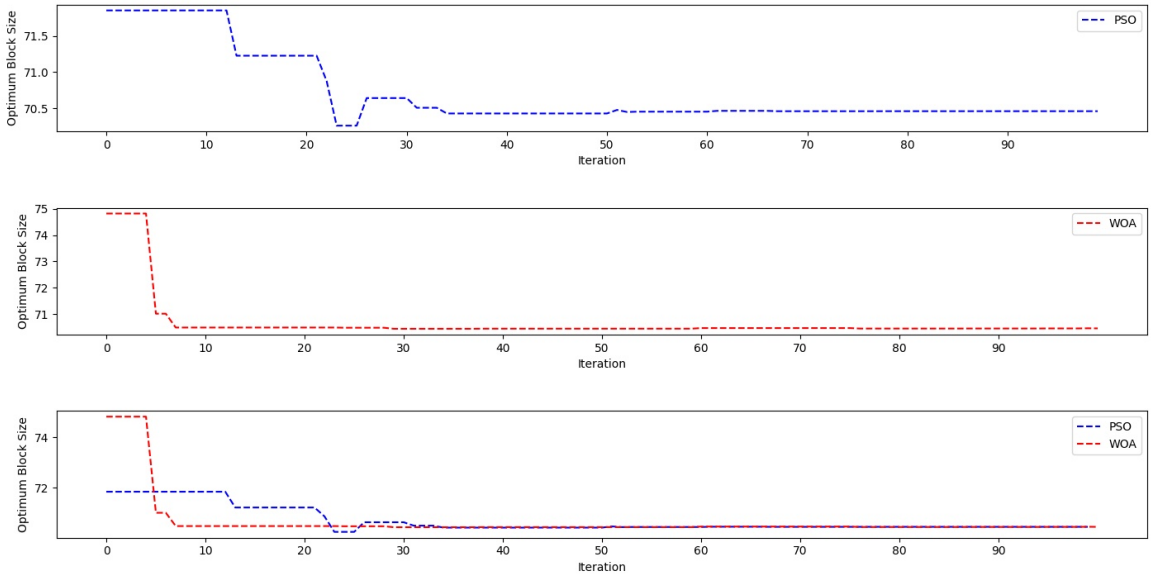

Figure 5. The fitness function convergence of the PSO and WOA algorithms according to the number of iterations.

5. Conclusion

In this study, multidimensional optimization problem minimizing the delay and block generation time is proposed. These two time functions depend on the block size, and the aim is to find an optimum block size value that results in minimum time. Weighted sum method is used to transform multiobjective problem into single objective optimization problem with weight factors. This minimization problem is solved by using two well-known evolutionary algorithms: PSO and WOA. This research is concentrated on two objectives. First subject is to evaluate the optimum block size. When the block size increases, the delay increases on the contrary block generation as time decreases. The block size changes in consonance with the different weights assigned to functions. When the weight factor for delay function is 0.7, then optimum block size is 458.96 Kb (almost equal to 382 transactions under assumption made in Methodology section). We can conclude that delay is much more dominant without considering security and network fairness, and efficient network design in blockchain network provides mine with a higher number of transaction in a constrained time. This makes blockchain based systems much more preferable and implementable. Furthermore, in blockchain based financial currencies such as Bitcoin, Ethereum, it will be easier to compete with other classical finance services in terms of the performance. The second objective is to compare the performance of the algorithms. Both algorithms obtain the same solution in terms of the target value. Butin terms of the performance, WOA converges faster and more steadily than PSO. The results demonstrate the well-deserved notoriety of the WOA heuristic algorithm.

Meanwhile, in this work, only blockchain systems for the PoW consensus algorithms are investigated in a mathematical manner. As a feature work, block size optimization will be further analyzed for other consensus algorithms especially for DAG. Last but not at least, this study depends on only mathematical analysis; the formula can also be implemented into the real scenario. Heretofore, for the optimization of block size, only time parameters were considered. As a feature work, throughput can be optimized by compromising the network fairness. Besides, security becomes another crucial concern while increasing the block size, and large block size results in increased centralization. For further studies, security and decentralization should be examined.

References

[1] Scherer M. Performance and scalability of blockchain networks and smart contracts. 2017.

[2] Reddy BS, Sharma GV. Optimal transaction throughput in proof-of-work based blockchain networks. In Multidisciplinary Digital Publishing Institute Proceedings 2019; 28 (1):6

[3] Ghimire S. Analysis of bitcoin cryptocurrency and its mining techniques. PhD, University of Nevada, Las Vegas, 2019.

[4] Mingxiao D, Xiaofeng M, Zhe Z, Xiangwei W, Qijun C. A review on consensus algorithm of blockchain. In: IEEE 2017 international conference on systems, man, and cybernetics (SMC); 2017. pp. 2567-2572.

[5] Bach LM, Mihaljevic B, Zagar M. Comparative analysis of blockchain consensus algorithms. In: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO); 2018. pp. 1545-1550

[6] Yang D, Long C, Xu H, Peng S. A review on scalability of blockchain. In: The 2nd International Conference on Blockchain Technology; 2020. pp. 1-6.

[7] Vukolić M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In: International workshop on open problems in network security. Springer, Cham, 2015. pp. 112-125.

[8] Khan KM, Arshad J, Khan MM. Investigating performance constraints for blockchain based secure e-voting system. Future Generation Computer Systems 2020; 105: 13-26.

[9] Jiang S, Wu J. Bitcoin mining with transaction fees: a game on the block size. In: 2019 IEEE International Conference on Blockchain (Blockchain); 2019. pp. 107-115.

[10] Gemeliarana IG, Sari RF. Evaluation of proof of work (POW) blockchains security network on selfish mining. In: 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI); 2018. pp. 126-130.

[11] Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: Architecture, consensus, and future trends. In: 2017 IEEE international congress on big data; 2017. pp. 557-564.

[12] Dimitri N. Transaction fees, block size limit, and auctions in Bitcoin. Ledger. 2019.

[13] Chao IM, Hsiung SC, Liu JL. Improved Whale Optimization Algorithm Based on Inertia Weights for Solving Global Optimization Problems. Advances in Technology Innovation 2020; 5 (3): 147.

[14] Singh N, Vardhan M. Multi-objective optimization of block size based on CPU power and network bandwidth for blockchain applications. In: Proceedings of the Fourth International Conference on Microelectronics, Computing and Communication Systems; Springer, Singapore; 2021. pp. 69-78.

[15] Cao B, Zhang Z, Feng D, Zhang S, Zhang L et al. Performance analysis and comparison of PoW, PoS and DAG based blockchains. Digital Communications and Networks 2020; 6 (4): 480-485.

[16] Erdos P, Rényi A. On the evolution of random graphs. Publications of the Mathematical Institute of the Hungarian Academy of Sciences. 1960;5 (1):17-60.

[17] Croman K, Decker C, Eyal I, Gencer AE, Juels A et al. On scaling decentralized blockchains. In: International conference on financial cryptography and data security; Springer, Berlin, Heidelberg; 2016. pp. 106-125.

[18] Kim S, Kwon Y, Cho S. A survey of scalability solutions on blockchain. In: IEEE 2018 International Conference on Information and Communication Technology Convergence (ICTC); 2018. pp. 1204-1207.

[19] Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H et al. On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security; 2016. pp. 3-16.

[20] Zhang L, Wang T, Liew SC. Speeding up Block Propagation in Blockchain Network: Uncoded and Coded Designs. arXiv preprint arXiv:2101.00378. 2021.

[21] Singh N, Vardhan M. Computing optimal block size for blockchain based applications with contradictory objectives. Procedia Computer Science 2020; 171: 1389-1398.

[22] Sompolinsky Y, Zohar A. Secure high-rate transaction processing in bitcoin. In: International Conference on Financial Cryptography and Data Security; Springer, Berlin, Heidelberg; 2015. pp. 507-527.

[23] Noh J, Baccichet P, Hartung F, Mavlankar A, Girod B. Stanford peer-to-peer multicast (SPPM)-overview and recent extensions. In: IEEE 2009 Picture Coding Symposium; 2009. pp. 1-4.

[24] Kalantari KR, Ebrahimnejad A, Motameni H. Dynamic software rejuvenation in web services: a whale optimization algorithm-based approach. Turkish Journal of Electrical Engineering & Computer Sciences 2020; 28 (2): 890-903.

[25] Hu H, Bai Y, Xu T. Improved whale optimization algorithms based on inertia weights and theirs applications. International journal of circuits, systems and signal processing 2017; 11:12-26.

[26] Mirjalili S, Lewis A. The whale optimization algorithm. Advances in engineering software 2016; 95:51-67.

[27] Mohammed HM, Umar SU, Rashid TA. A systematic and meta-analysis survey of whale optimization algorithm. Computational intelligence and neuroscience 2019.

[28] Decker C, Wattenhofer R. Information propagation in the bitcoin network. In: IEEE P2P 2013 Proceedings; 2013. pp. 1-10.

[29] Göbel J, Keeler HP, Krzesinski AE, Taylor PG. Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. Performance Evaluation 2016; 104: 23-41.

[30] Li Z, Chen D, Chen Y, Lei H, Zhu H. PMSM parameter identification based on improved PSO. In: Journal of Physics: Conference Series 2021; 1754 (1): p. 012235.