Journal of
Sensor and Actuator Networks

MDPI

Article

Scaling Up Security and Efficiency in Financial Transactions and Blockchain Systems

Nazar Abbas Saqib [1,*] and Shahad Talla AL-Talla [2,*]

[1] SAUDI ARAMCO Cybersecurity Chair, Department of Networks and Communications, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia
[2] Department of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia
* Correspondence: nasaqib@iau.edu.sa (N.A.S.); 2210500149@iau.edu.sa (S.T.A.-T.)

Abstract: Blockchain, the underlying technology powering the Bitcoin cryptocurrency, is a distributed ledger that creates a distributed consensus on a history of transactions. Cryptocurrency transaction verification takes substantially longer than it does for conventional digital payment systems. Despite blockchain's appealing benefits, one of its main drawbacks is scalability. Designing a solution that delivers a quicker proof of work is one method for increasing scalability or the rate at which transactions are processed. In this paper, we suggest a solution based on parallel mining rather than solo mining to prevent more than two miners from contributing an equal amount of effort to solving a single block. Moreover, we propose the idea of automatically selecting the optimal manager over all miners by using the particle swarm optimization (PSO) algorithm. This process solves many problems of blockchain scalability and makes the system more scalable by decreasing the waiting time if the manager fails to respond. Additionally, the proposed model includes the process of a reward system and the distribution of work. In this work, we propose the particle swarm optimization proof of work (PSO-POW) model. Three scenarios have been tested including solo mining, parallel mining without using the PSO process, and parallel mining using the PSO process (PSO-POW model) to ensure the power and robustness of the proposed model. This model has been tested using a range of case situations by adjusting the difficulty level and the number of peers. It has been implemented in a test environment that has all the qualities required to perform proof of work for Bitcoin. A comparison between three different scenarios has been constructed against difficulty levels and the number of peers. Local experimental assessments were carried out, and the findings show that the suggested strategy is workable, solves the scalability problems, and enhances the overall performance of the blockchain network.

Keywords: blockchain; particle swarm optimization; PSO-POW; efficiency in financial transactions; parallel mining

Citation: Saqib, N.A.; AL-Talla, S.T. Scaling Up Security and Efficiency in Financial Transactions and Blockchain Systems. *J. Sens. Actuator Netw.* **2023**, *12*, 31. https://doi.org/10.3390/jsan12020031

Academic Editor: Mohamed Amine Ferrag

Received: 5 March 2023
Revised: 18 March 2023
Accepted: 28 March 2023
Published: 3 April 2023

1. Introduction

The banking business has been serving as a middleman for financial transactions since its inception. They have offered the trust necessary for the flow of money. The banking system has always been impacted by technology. Banks have continuously changed how they operate to keep up with information and technological innovation. For information flow, banks are now linked to technology networks like Society for Worldwide Interbank Financial Telecommunications (SWIFT). Therefore, the banking sector depends entirely on technology to carry out daily tasks.

Banks are frequently criticized for being wasteful, expensive, and opaque. Neobanks and fintech companies such as PayPal, Revolut, and N26 are upending traditional banks with their creative solutions. Blockchain offers an answer to these complaints as well as

a competitive edge over the fintech sector. The interest in blockchain has expanded significantly over time, and recently, central banks and governments have also been investigating its potential applications. The potential of blockchain is being explored by numerous banks globally, so the future is undoubtedly bright.

Financial industry cybersecurity experts need to stay up to date on the risks, industry rules, and technology needed to stop assaults. The following are a few advantages of blockchain for cybersecurity:

- Preventing the spread of malware. The blockchain can be used to validate software upgrades and downloads;
- Securing the transfer of data. Transactions are protected by encryption;
- The cloud. Attacks on physical servers are prevented by decentralized storage;
- Defending against distributed denial of service (DDoS) assaults. DDoS assaults cannot target a single point of access because of the distributed blockchain design.

A financial service is an automated system for telecommunication that helps the customers to perform financial transactions in a public space without needing human intervention. Scalability is a very important factor in financial transactions for achieving the acceptable throughput of secured transactions. In addition, generating high performance transactions is also very important to be handled without the disturbance of unauthorized access. Thus, scalability can be defined in the finance world as the ability to improve the performance in terms of throughput [1]. Unfortunately, financial services also have a number of limitations such as the following: security, stability, integrity and goods' tampering.

Consequently, there is a need to secure financial transactions which depend on modern technologies that try to prevent any unauthorized access. Science and technology are in rapid development. In addition, computer networks are widely used in different fields. Blockchain technology is one of the most efficient network technologies [1] which is used about all industry sections including artificial intelligence [2], the healthcare sector [3–6], financial transactions [7], the Internet of things [8,9], the government sector [10,11], and others [12]. Each one of these fields profits from blockchain's advantages, which are the following: transparent, decentralized, and immutable and fully distributed peer-to-peer architecture.

Blockchain may be a key driver for the banking industry. The use of blockchain is a good solution to deal with these problems. However, despite the attractive advantages of the blockchain, scalability is one of its major limitations. Simply put, scalability is the transaction number that is processed per second. In blockchain, scalability is small and insufficient (up to seven for Bitcoin [13] and fifteen for Ethereum [5]). This is unsatisfactory for most centralized payment systems that need 1000 s of transactions per second (tx/s). There is a problem called scalability trilemma which is a well-known problem on the blockchain. This problem was first described by Vitalik Buterin, who is the cofounder of Ethereum [14]. Vitalik points out that there are trade-offs between three important factors: decentralization, scalability, and security.

The peer-to-peer network performance paradigm for blockchain technology needs to be widely used and reliable proven. This thesis aims to scale blockchain transactions while preserving its decentralized structure.

The main contributions of this work are proposing a solution based on parallel mining rather than solo mining to prevent more than two miners from contributing an equal amount of effort to solving a single block. Moreover, we propose the idea of automatically selecting the optimal manager over all miners by using the particle swarm optimization (PSO) algorithm. This process solves many problems of blockchain scalability problems and makes the system more scalable by decreasing the waiting time if the manager fails to respond. Additionally, the proposed model includes the process of a reward system and the distribution of work. In this work, we propose the particle swarm optimization proof of work (PSO-POW) model. Three scenarios have been tested which are solo mining, parallel mining without using the PSO process, and parallel mining using the PSO process (PSO-POW model) to ensure the power and robustness of the proposed model. This model

has been tested using a range of case situations by adjusting the difficulty level and the number of peers.

2. Literature Review

Many studies have attempted to address the issues with financial transactions. Numerous technologies are employed to address this issue. The major technology to be discussed here is blockchain.

The expansion of business calls for more reliable ways to share papers quickly and without human interaction. The communication of business-related data across applications, based on a structured machinereadable format, is known as electronic data interchange (EDI) [15]. The information necessary from each trading partner is obtained from the corresponding ERP system and translated into an EDI message standard that both parties have agreed upon if two company partners use EDI for document exchange to process a trade. Subsequently, automatically connecting to one another and exchanging their standard EDI documents for handling transactions is possible. A somewhat complex information technology infrastructure supports EDI. Data processing, data management, and networking capabilities are just a few of the many operations needed to efficiently convert data into an electronic format. Furthermore, dependable data transmission between distant parties and regulated access to data is needed [16]. A worldwide standard identified as UN/ED-IFACT is utilized amongst the communicating parties to guarantee compatibility with EDI communication [17].

Communication with people must be effective and efficient for a business to succeed. In electronic communication, EDI offers a standardized and regulated type of communication. However, EDI use was expanding quickly, and stakeholders anticipated that it would eventually overtake other forms of corporate communication in a number of sectors [18]; despite this, this technology is still lagging in terms of adoption [19]. The adoption of EDI is significantly influenced by interorganizational trust, outside pressure, expenses, and the size of adopting companies [20]. A robust method for the routine automated exchange of data between parties who maintain a long-term commercial relationship is EDI. On the other hand, the documentation chain is broken if many more parties—especially those without EDI—are involved in the process. The information that had to be transmitted is no longer a requirement. The significance of blockchain is shown here.

According to a recent projection [21], blockchain will increase company value by over 175$ billion annually by 2025 and by over 3$ trillion by 2030. By 2030, 10–20 percent of the world's economic infrastructure, according to another study [22], will be conducted utilizing blockchain technology. Blockchain, according to researchers [23], will revolutionize the exchange of electronic data. These upbeat and similar works have helped to significantly enhance business interest in blockchain over the past few years.

Through a blockchain-based transaction system, the authors of [24] suggest a ban on corruption and money laundering in non-governmental groups (NGOs) and government fundraising organizations. They created a blockchain-based framework for the financial transaction and tested it on the Rinkeby test network. The outcomes of the framework test show that computing is significantly safer and devoid of any fraud. When compared to the conventional client–server financial transaction system, the framework performs better.

The authors of [25] suggested a platform that enables several authorized users to own and manage the network's nodes. It does away with the third party's involvement in controlling the numerous transactions and financial data. Additionally, it encourages user–user transactions before storing data about bank transactions in the blockchain. With the help of this blockchain platform, customers may conduct private and secure transactions for less money and without being subject to a foreign exchange cap.

In [26], the researchers suggest a blockchain-based encrypted messaging solution. They put forth a blockchain-based messaging architecture that preserves the effectiveness and security of the data stored on the blockchain. The users' certificates were validated by

the model using a smart contract, which checked the users' public keys and identities. Users are able to send encrypted messages thanks to the system's complete decentralization.

The authors of [27] research paper presented a mechanism to protect mobile device transactions using a blockchain-based server system through a mobile SIM serial-based verification system. The user's account is linked to the serial number of the subscriber identity module (SIM). Thus, if an intruder attempts to make a transaction using a different SIM, the model alerts mismatch of the login credentials. Based on that, the system notifies the bank of the intruder's location, and the bank sends an email containing the intruder's details to the registered user. Since the mobile serial number is specific to the SIM, the intrusive party has no prospect of conducting any transactions from another handset. Overcoming OTP-related issues may be the problem. Through the Ethereum blockchain technology, which offers server-side database security, the bank may validate the digital signatures used during the transaction and the consensus mechanism for transaction confirmation. Therefore, utilizing blockchain-based security, it is possible to establish mathematically that banking transactions are secure.

According to the researchers in [28], the Internet of things is moving in a way that will increase the security, anonymity, and data integrity of Bitcoin. Although smart cards look to be leading in technology and are very profitable, their high price prevents them from being sold in all industries. Blockchain is a non-centralized data and transaction system created specifically for cryptocurrencies. As a result, the primary characteristics of Bitcoins that cause this problem are their provision of security, anonymity, and data integrity without interfering with transactions.

A financial technologies (fintech) start-up was suggested by the researchers in [29] to conduct financial transactions using blockchain technology and cryptocurrency in users' digital marketing. Fintech is a useful invention that may energize established financial markets. This study demonstrated how information technology supports innovation in financial transactions, demonstrating how fintech presents a new paradigm.

The authors of [30] worked on cross-border transactions to make sure that they were implemented. They suggested asymmetric consortium blockchain, a novel type of consortium blockchain (ACB). The super node is supported by the new blockchain technology to control all transactions across time. The researchers created a new smart contract to lessen opportunity loss for each node and make the profits allocation scheme more equitable. They used numerical experiments based on Shenzhen and Hong Kong transaction data to demonstrate their theories. The results showed that the suggested ACB system is effective and intelligent for the new cross-border transaction system.

In [31], the authors put forth a blockchain-based application for a decentralized network-based transaction mechanism for financial data backup. Using a decentralized distributed blockchain ledger, each node has a copy of the transactional information. Therefore, a failure in a single node does not result in a complete loss of transaction data. The account ledger component, which includes credit and debit transactions completed using timestamps and transaction IDs, is what the system depends on. Each block also includes a hash of the previous and current blocks, which are used to safeguard the information in the chain in addition to the account ledger data.

The authors of [32] presented an IoT model-based system that uses a variety of approaches to secure the blockchain system. The suggested approach includes a Radio Frequency Identification (RFID)-based system for financial transactions. Only authorized customers with access to the system may access the data it collects. As a result, the first degree of security is implemented by employing M2M authentication to provide authentication to the legitimate client. The transaction system can be accessed if the user has been authenticated. The model system uses hashing to secure the transaction data that is saved and makes use of blockchain technology. Results from experiments used to validate the model show that it satisfies data security standards by implementing several security techniques that enhance the generated hash's privacy.

By introducing the associated MapReduce financial transaction exploitation, the authors of [33] evaluated the MapReduce characteristics and technology of financial transaction. Through examination and comparison of MapReduce and financial transaction technologies, the work explores the MapReduce technology's method for financial data transaction. The work offered insightful opinions and recommendations for utilizing MapReduce technology in financial transaction processes and for sustainable development.

By utilizing proof-of-work consensus techniques, they proposed a permissionless blockchain networks method in [34] to increase scalability. The method's introduction of parallel proof of work enables all miners to participate equally in the competition and assure that speed and power are rising. As the level of difficulty and the number of miners rise, the results indicated tremendous promise for parallel proof of work.

The goal of the blockchain distribution network (BDN), which the authors utilized as a trust model in [35] to overcome the scalability issue, is to secure peer-to-peer trust and allow blockchain systems to grow to thousands of transactions per second. Additionally, they claimed that employing a global infrastructure to enable distributed blockchain systems in a provably neutral manner will scale blockchain and cryptocurrencies at the same time.

In [36], the researcher employed two techniques, attribute-driven design (ADD) and quality attribute workshop (QAW), to meet the needs of their system, which aims to ensure security and availability through the application of three system-designed tactics: active redundancy to fault recovery, identify actors to authenticate the access and encrypt data to manage privacy.

To ensure a high pace of transactions in a permissioned block chain, a transaction model was developed in [37]. Dual-channel parallel broadcast (DCPB) uses three techniques to increase network performance and transaction rate: dual-channel model (DCM), parallel pipeline technology (PPT), and block generation and broadcast backup (BGBB). The experiment demonstrated an improvement in speed of 4–5 times when compared to (PPT), and performance was better when compared to conventional resolution. The final option, (BGBB), can accelerate processing by 25%.

The [38] writers proposed a PolyShard architecture that combines security, throughput efficiency, and storage linear scaling. Instead of storing and processing a single uncoded shard as is performed traditionally, the notion is that each node stores and computes on a coded shard of the same size that is formed by linearly mixing uncoded shards. The security against false results from malicious nodes is demonstrated by this coding, which is made possible using noisy polynomial interpolation techniques.

According to this analysis of the literature, these works mostly leverage blockchain, EDI, Internet of things (IoT), artificial intelligence (AI), and cloud computing technologies. The majority of contemporary models employ blockchain to address the issue of transaction security in financial transactions. Table 1 compares between the previously mentioned researchers according to the main blockchain features, illustrating the achieved features for each research. Other efforts have made use of big data, IoT, AI, and machine learning. In our effort, we will concentrate on developing a new blockchain security model that will use blockchain technology to enhance the scalability and the overall performance of financial transactions using AI. Since most of modern technologies are used in such works to handle the problems of financial transactions and most of research works did not touch the performance and scalability of financial transaction using blockchain, in our work, we will focus on using blockchain technology to improve the scalability and performance of financial transaction.

Table 1. Comparative analysis against different features.

	Papers							
Features	[33]	[27]	[35]	[36]	[26]	[32]	[37]	[38]
Scalability	-	-	✓	✓	✓	-	-	✓
Confidentiality	-	✓	-	-	✓	✓	-	-

Table 1. *Cont.*

	Papers							
Integrity	-	✓	-	-	-	✓	✓	-
Availability	-	-	-	-	-	✓	✓	-
Authentication	-	-	-	-	-	-	-	-
Permissioned	-	-	-	-	-	-	-	✓
Permissionless	-	-	✓	-	-	-	-	-
Privacy	✓	-	-	-	-	-	✓	-

Additionally, there is multi-objective particle swarm optimization for feature selection with fuzzy cost, dual-surrogate assisted cooperative particle swarm optimization for expensive multimodal problems. Multi-objective optimization problems are optimization problems with many objectives that clash with one another at the same time (MOPs). Researchers have developed numerous great multi-objective optimization evolutionary algorithms (MOEAs), which fall into three broad categories, to tackle multi-objective optimization problems successfully. It primarily consists of MOEAs with dominance, decomposition, and indicator bases [39].

Two PSO-based multi-objective FS functions have been put forth in [40]. The first way makes advantage of the FS submissive concept. The Pareto front has been searched using the mutation, gathering, and dominance to PSO concepts in the second technique.

3. Basic Methods and Techniques

In this section, the basics of the methods that are used in this thesis are discussed. These methods and techniques are basically performed for the main phases of the scalability model, which are parallel mining and selecting manager.

3.1. Scalability

Scalability is how quickly transactions can be handled on the Bitcoin network. Just like other systems, blockchain has significant drawbacks [41,42], one of which is scalability. The blockchain network is presently used for transactions, mining, and maintaining ledgers by hundreds of cryptocurrencies. Although scaling problems affect all cryptocurrencies, VISA, a conventional transaction provider, has already reached a peak of 10,547 transactions per second [43]. Due to the diverse protocols used by each cryptocurrency, transaction speeds vary. Table 2 derived from [44] displays the transaction and confirmation times for several cryptocurrencies.

Table 2. The speed of various cryptocurrencies' transactions [2].

Cryptocurrency	Transactions per Second	Average Transaction Confirmation Time
Bitcoin	3–7	60 min
Ethereum	15–25	6 min
Ripple	1500	4 s
Bitcoin Cash	61	60 min
Stellar	1000	2–5 s
Litecoin	56	30 min
Monero	4	30 min
IOTA	1500	2 min
Dash	10–28	15 min

Blockchain has certain distinctive elements or features that set it apart from conventional systems. These features must be understood in order to understand blockchain.

3.2. Particle Swarm Optimization (PSO)

Particle swarm optimization (PSO) is one of the most important optimization techniques as it simply implemented and works efficiently; it was proposed by Kennedy and Eberhart [45]. It was compared with genetic algorithm (GA) [46], and it has been shown that PSO performed with better accuracy in a smaller amount of time. Additionally, it has little parameters to be tuned, as PSO does not need to adjust "mutation" or "recombination".

Its inspiration comes from mimicking the attitude of a flock of birds or a school of fish. There are some basic names for the PSO mechanism such as candidate solutions, which are called particles in PSO, and the PSO population of these particles are called swarm. The main idea of the PSO mechanism is that the population particles tour a multi-dimensional problem space to achieve the unique standard goal that is reaching the optimal solution. As the particles travel through the search space, they rely on their computation in three basic experiences:

1. Their experience;
2. Neighborhood local experience (pbest);
3. nd Global best among all particles (gbest).

For PSO implementation, there are some parameters that should be tuned according to the nature of the used application. The particles in the swarm do not tour in the search space as one group, but are portioned into local groups depending on the local best (pbest) of their computation. However, they take care of the global best (gbest) that gives experience about the other particles in the surrounding local groups. Thus, PSO achieves the balance between local and global exploration through caring about both the local and global best computations. Additionally, in each iteration, the particles change their current position by amount and direction of a velocity that is computed based on the local and global computations as described in Figure 1.

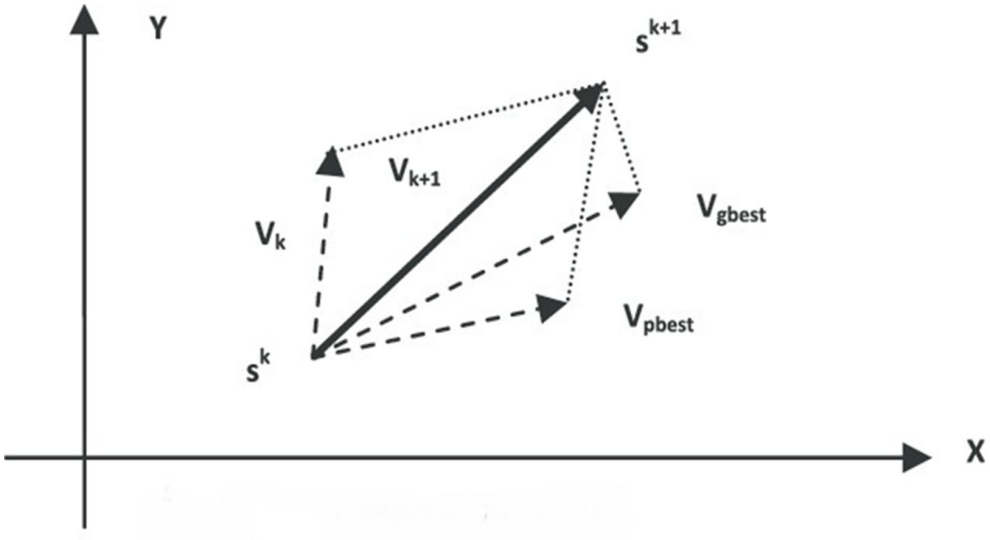

Figure 1. PSO searching point changing mechanism.

Where s^k represents current searching position, v^k represents current velocity, s^{k+1} represents new modified searching position, v^{k+1} represents new modified velocity, V_{pbest} represents velocity with care of pbest, and V_{gbest} represents velocity with care of gbest.

Thus, all particles update their position based on main four parameters: (1) the current position, (2) the current velocity, (3) the distance between the current position and pbest, and (4) the distance between the current position and gbest. The main architecture of PSO is shown in Figure 2.

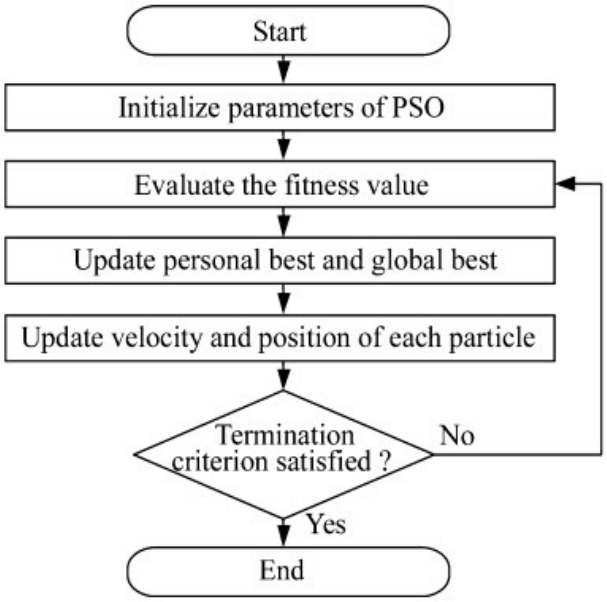

Figure 2. PSO architecture.

4. Proposed PSO-POW Scaling Model

In this section, we perform a strategy that uses parallel mining rather than solo mining to speed up the proof of work procedure. The aim is to prevent more than two miners from contributing an equal amount of effort to solving a single block. Additionally, an optimization method is used to select the best manager for each epoch.

4.1. Proof of Work (POW) Phase

The Bitcoin index, the preceding block's hash value, and the timestamp are three pieces of information that are used by the miners in the proof of work process that are all identical. It is possible that the nonce value selected by the miners and the nature of the transactions could vary. All miners will utilize identical transaction data, but a different nonce, thanks to the way the suggested approach is constructed. As a result, no two miners will ever do the same task. All miners will therefore use identical data, save for the nonce for a specific block.

Management must make sure that no two miners use the same nonce value and that all miners utilize the same transaction data in order to create such an environment. Every era will have a different manager, who will be selected from the miners. An epoch in this context holds the span of time between two blocks. In this scenario, the management, not the miner, will decide which nonce has to be computed. The management can make sure that no two miners utilize the identical nonce value in this way. The manager is also in charge of generating the transaction hash for each block that falls under his or her purview, which will be given to the miners along with the nonce value. The transaction hash should be the same for all miners, unlike nonces. In a conventional system, each node is directly or indirectly connected to every other node. They will still be linked together in the planned system, and they will also have a direct line to the management.

The blockchain should begin with a genesis block that contains no transactions. The management for the following block (Block 1) will be chosen at random; however, for the following blocks, the manager who has an optimum value of the compute average transaction number of a node will be optimally selected, as will be explained in the next sections. The conventional approach will now be used, as all miners compete with one another to solve the genesis block. The epoch for the subsequent block will start when a miner solves the genesis block. At this stage, the suggested solution will be successful.

As shown in Figure 3, the manager will initially produce a transaction hash using the unconfirmed transactions while also producing multiple sets of nonces. No single nonce

value should appear in more than one group; instead, each group will contain a range of nonce values. The manager must first construct and register at least m number of groups if there are m active miners in the network. The manager will then give each active miner a group of nonces and the transaction hash. No two miners will belong to the same group, thanks to the mechanism. The available transaction data and the range of nonce assigned to each miner, with the exception of the manager, will now be used to try to solve the next block.

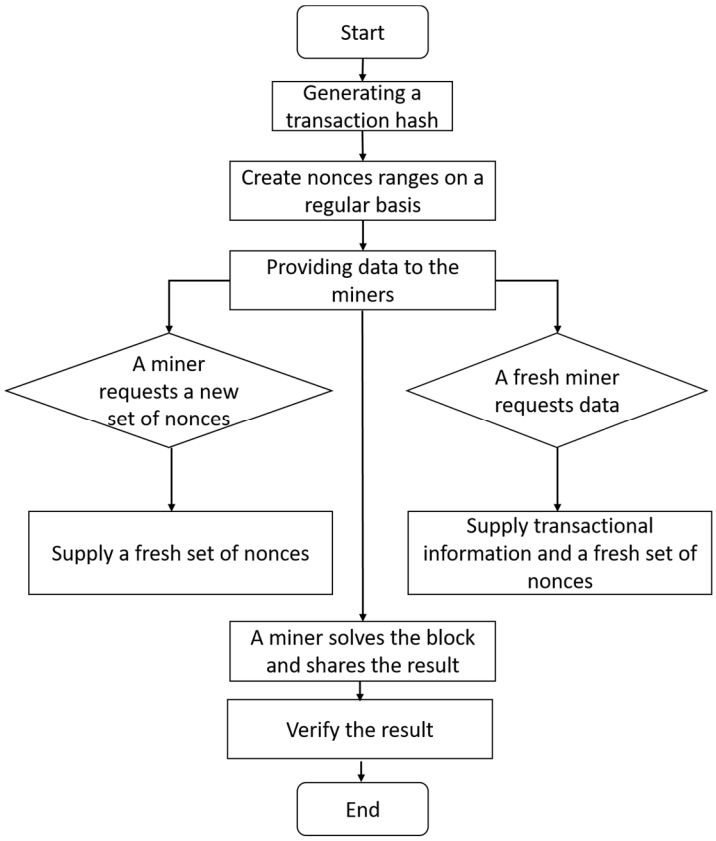

Figure 3. The process of a miner acting as a manager.

More groups of nonces will be generated and registered simultaneously by the manager. A miner will request a fresh nonce range from the manager once all of the nonce values in the allotted range have been used. The manager will then give the miner access to an unoccupied range. Once more, if a new miner joins the network and requests the manager's assistance, the manager will provide the new miner the same transaction data plus a fresh batch of nonces. Because of this, the manager should produce as many groupings of nonces as they can. The procedure will keep going until a predetermined answer to the current nonce is discovered.

4.2. New Manager Selection Phase

Each block's manager will switch under the suggested procedure. A manager's validity is limited to the block for which they are accountable. Only a miner who has an optimal value of an average transaction number of a node (ATN) can be a manager. PSO used to do this, as illustrated in Algorithm 1. In contrast to block 1, whose manager will be selected at random, the genesis block has no manager because it contains no transactions. The manager chosen will be the one who is optimally selected by the PSO algorithm for the remaining blocks.

Calculate a node's average transaction number (ATN): By completing the questionnaires Mi for the aptitude tests, we obtain the state of the i-th node. This questionnaire evaluates each node's average transaction volume based on four factors: node properties

(CRT), network nature (HCL), safety components (DAA), and reward value (RV). The following chart shows the primary and nine subsidiary influencing factors:

$$M = CRT, HCL, DAA \quad (1)$$

$$CRT = calculate - power - ratio, online - time, pay - off \quad (2)$$

$$HCL = hop, connection - number, latency \quad (3)$$

$$DAA = discarded - probability, atracked - probability, 10ttract - probability \quad (4)$$

Alex won the 2012 ImageNet challenge and proposed the AlexNet network structure model for picture categorization. In order to complete a capability assessment system, a modified AlexNet was suggested. The goal is to fit the input characteristic matrix M to the average transaction number ATN. Reward value will be explained in the next subsection.

$$ATN = f(M) = f(CRT, HCL, DAA, RV) \quad (5)$$

Manager selection using PSO algorithm: Equation (5) is the fitness function for PSO algorithm that should be maximized to select the best manager who has the optimal value of ATN, as will be shown in the following PSO algorithm.

Algorithm 1 Manger Selection Algorithm

1: Randomly initialize the swarm particles within the range shown in Table 3.
2: Calculate the fitness function for all particles in the swarm according to Equation (5).
3: Initialize pbest and gbest, with the value of pbest of specific particle assigned from the objective values that are computed, and the value of gbest computed by selecting the best value of all pbest values.
4: For each particle in the swarm, velocity is measured according to Equation (1).
5: All particles position values are recomputed according to Equation (2)
6: Update the value of fitness function for all particles, both pbest and gbest.
7: Check the stopping criteria. If achieved, the threshold values will be the particles posi-tions of gbest. If not, go to step 4.
8: Output: The machine with the best value of ATN

Table 3. Chosen parameters for PSO implementation.

Parameter	Value
Num of iterations	100
Swarm size	20
C1	1.5
C2	1.5
Vmax	2
Vmin	−2
Xmax	255
Xmin	0

As illustrated from Algorithm 1, PSO will select the best machine that has the optimal value of ATN, and it will be the new manager for the next block. In Figure 4, M6 has the best ATN value, so it was selected to be the manager of the next block (block 1). Once M6 acted as manager for block 1, it was unable to compete with other miners as a typical miner would.

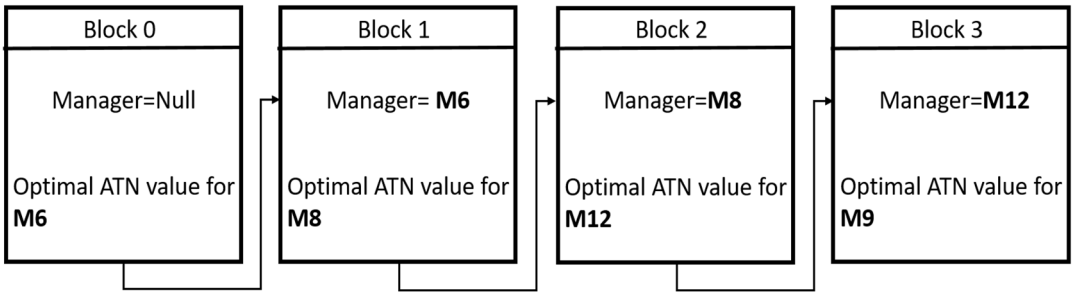

Figure 4. Manager selection process using PSO.

4.3. Reward Value

The amount of money that can currently be mined as a reward for each block in Bitcoin (2018) is 12.5 BTC. Following the creation of a block, the miner will be able to mine a set quantity of cryptocurrency using the suggested technique. However, not all of the transaction fees for all of the transactions will go to the miner. Instead, the transaction fees will be shared between the manager and the miner who solved the block, with the manager receiving 65% of the transaction fee.

An example is provided in Figure 5, where Block 1 is solved by M8 with M6 as the manager of that block. M8 and M6 will receive 35% and 65%, respectively, of the transaction fee. Since the manager generates the transaction data, he or she is rewarded more than the miner who found the block's solution. When a miner has finished fulfilling his or her duty as manager, they will both collect their rewards (mining and transaction fees).

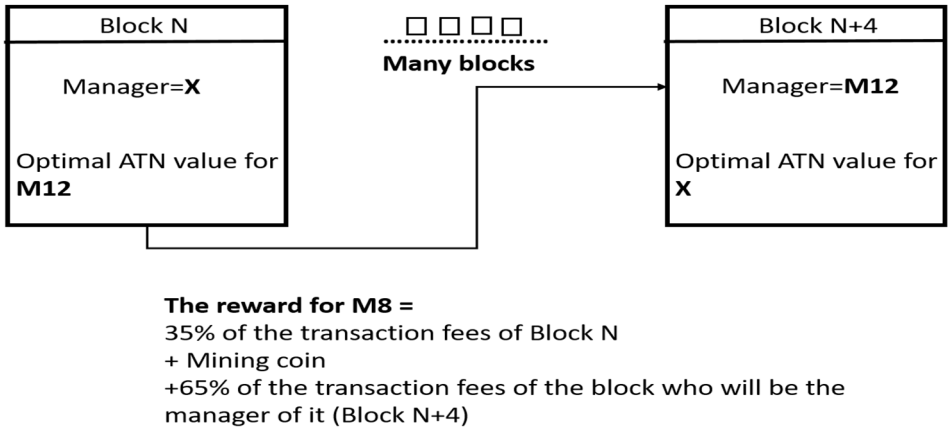

Figure 5. Reward value calculation.

Speed of the transaction, fairness to miners, decentralization, and solving the problem of multi-block selection are the main characteristics of the solutions that have been offered. The subsections that follow go into more depth.

5. Experimental Results and Discussion

In this section, three scenarios were introduced. First, the test has been conducted against solo mining. Then, the parallel mining with the original step of selecting a manger was tested. Finally, the test has been conducted with parallel mining with the process step of optimization with PSO. Each scenario's results are introduced. Additionally, an explanation is performed between the different scenarios' results.

5.1. Evaluation Environment

In this section, a description of the used programming languages and tools is introduced. The code for the proposed model was created using the Go programming language.

In particular, a peer-to-peer network has been created utilizing the Golang GX library [47]. The same program can be distributed to various nodes using this decentralized package manager. The proof of work has been carried out using the cryptographic hash technique SHA-256. The genesis block has been core coded; however, it lacks a transaction history and a previous hash value. By default, the manager for the following block will be the miner that connects to the system first except in the POW-PSO scenario, where it will be randomly selected by the PSO only in the first iteration.

The suggested solution has been put into practice using a peer-to-peer network with a ring structure [48]. A maximum of two nodes can be connected to by each node. A node that is connected to a network can create a new connection for another node to use so as to join the network. Every node address includes a distinct IP and ID. Each node's ID is unique and generated at random. The IP is the node's network address, which a new node can connect to. A node cannot accept new connections once it has established a connection with another node.

Diagrams of the network with different IP addresses and unique IDs are shown in Figures 6 and 7. The network's first peer is indicated here by the blue highlighted peer. The last peer connected to the network, marked in orange, is waiting for an incoming connection. The following figure illustrates how a miner assumes the role of a manager, and a direct connection is made with every other peer. In this instance, the peer with peer ID 104 is managing. Both locally and remotely, the suggested system has been evaluated. The evaluation of the proposed model has been performed with three different scenarios. First, it was performed against solo mining. Then, the parallel mining with the original step of selecting a manger was tested. Finally, the test was conducted with parallel mining with the process step of optimization with PSO.

We employed a Docker container to put this strategy into practice (docker.com). A Linux-based container with its own network interface is offered by Docker. All peers will be connected to a special network that Docker has constructed. The implementation was carried out using a Core i7-8750H CPU clocked at 2.20 GHz and the Ubuntu operating system. There are 8.00 GB of RAM installed.

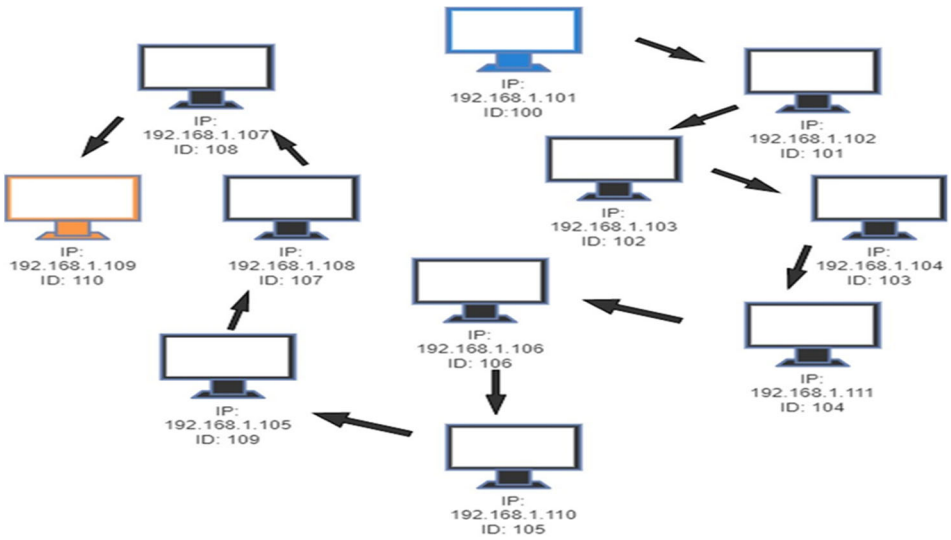

Figure 6. Network structure with different IP and ID.

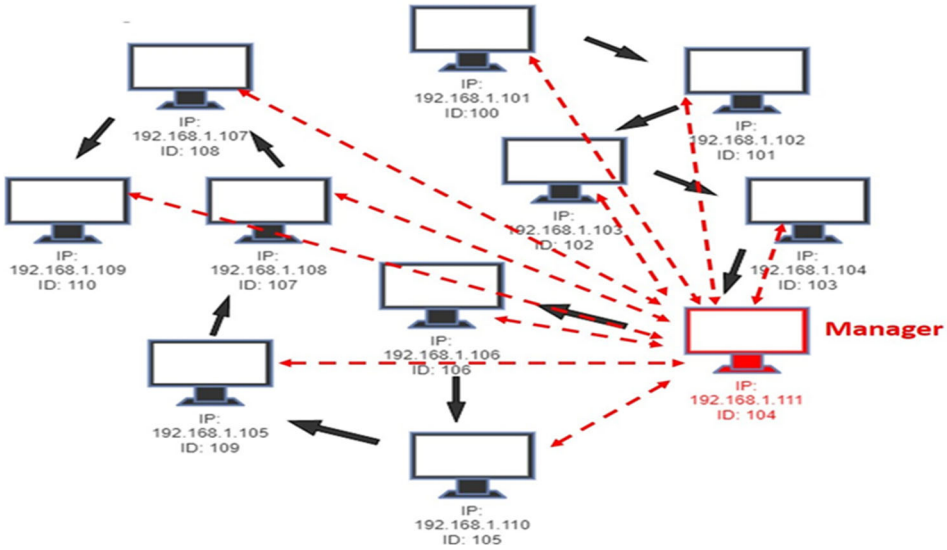

Figure 7. Network structure showing the selected manager.

5.2. Pool Mining Scenario (First Scenario)

In this scenario, to evaluate the solution, it is crucial to divide the resources evenly to each peer. As we mentioned, a Docker container was employed to put this strategy into practice. Each miner has been given a 10% share of the total resource to ensure that they all have an equal amount of computing power. Another identical environment has been created utilizing the same resources and components in order to compare the test results with the current system. The miners are lone workers in this arrangement. As in the current arrangement, they are in competition with one another, and the successful miner obtains the entire payout.

The scenario has been run using various peer counts, with varying degrees of difficulty. Here, the difficulty level designates the smallest string of consecutive zeros that must come before a valid hash. The test results based on solo mining are shown in Figure 8. Here, "average time (s)" refers to the typical amount of time, measured in seconds, needed to solve a block. A total of 20 multiple experiments were tested under identical circumstances, averaging the outcomes. The index, timestamp, transaction hash, prior hash, and nonce are used as input to determine the solution.

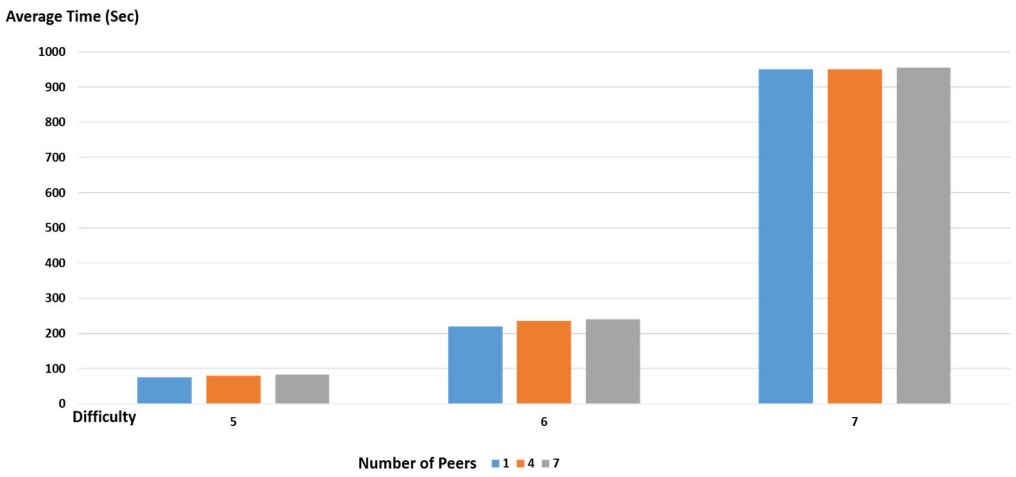

Figure 8. First Scenario Results (Solo Mining).

5.3. Parallel Mining Scenario (Second Scenario)

In this scenario, to evaluate the solution, it is not crucial to divide the resources evenly to each peer, as in real life, this is not logical. So, we use Docker so as to not equally divide the resources among each peer. This step's results will be noted in the following scenario when we use PSO to select the best manager.

Same as the previous scenario, parallel mining has been run using various peer counts, with varying degrees of difficulty. The test results based on parallel mining are shown in Figure 9. Additionally, 20 multiple experiments were tested under identical circumstances, averaging the outcomes.

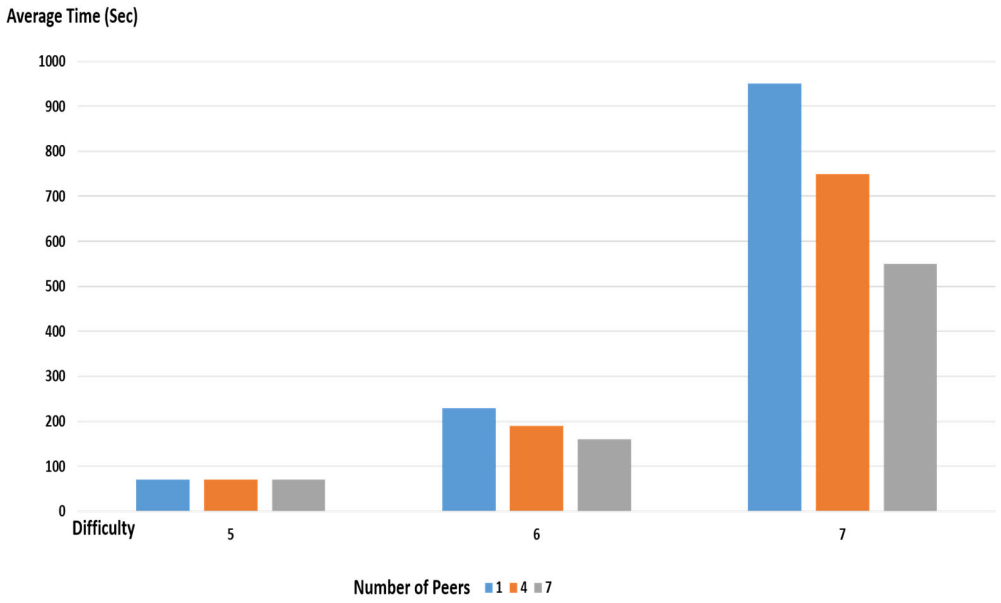

Figure 9. Second scenario results (parallel mining without using PSO step).

There is no discernible difference between solo mining and parallel mining at difficulty levels 1, 2, 3, and 4. Parallel mining has improved for difficulty levels 5, 6, and 7, and as Figures 8 and 9 show, this improvement becomes more noticeable as the difficulty level and the number of miners' rise. In solo mining, the average time is solely influenced by the difficulty, whereas in parallel mining, the average time is influenced by both the difficulty and the quantity of peers. The average amount of time needed grows as difficulty level does.

Once more, when the number of peers rises, the average time falls since fewer miners are performing the same tasks in tandem. Another crucial point to note is that, regardless of the number of peers, the average time required by one peer in parallel mining is almost identical to that of solo mining. This is due to the fact that no parallel work is being performed while there is only one miner participating in parallel mining. Compared to one miner, the improvement increases by 34% for five miners. It should be mentioned that depending on the processing power allotted to the miners, the outcomes could change.

However, there is still a problem in this model: if multiple miners solve the hash at the same time, which miner will be the next selected manager. This is a significant problem with how Bitcoin is now validated. The longest chain is always trusted by Bitcoin clients. The block is therefore accepted by the majority of miners (at least 51%) and is added to the blockchain network if two miners solve the hash simultaneously. The other miners' efforts will be for nothing. For a certain period of time, this condition may occur in a parallel chain in the network. Clients must therefore wait until there are enough confirmed blocks. The typical wait time in Bitcoin is six blocks. So, in the following scenario, this problem will be handled.

5.4. Parallel Mining Scenario with PSO (PSO-POW Scaling Model) (Third Scenario)

Additionally, in this scenario, we use Docker to not equally divide the resources among each peer. Similar to the previous two scenarios, parallel mining with PSO has been implemented using various peer counts, with varying degrees of difficulty. The test results based on PSO-POW model are shown in Figure 10. Furthermore, 20 multiple experiments were tested under identical circumstances and averaging the outcomes.

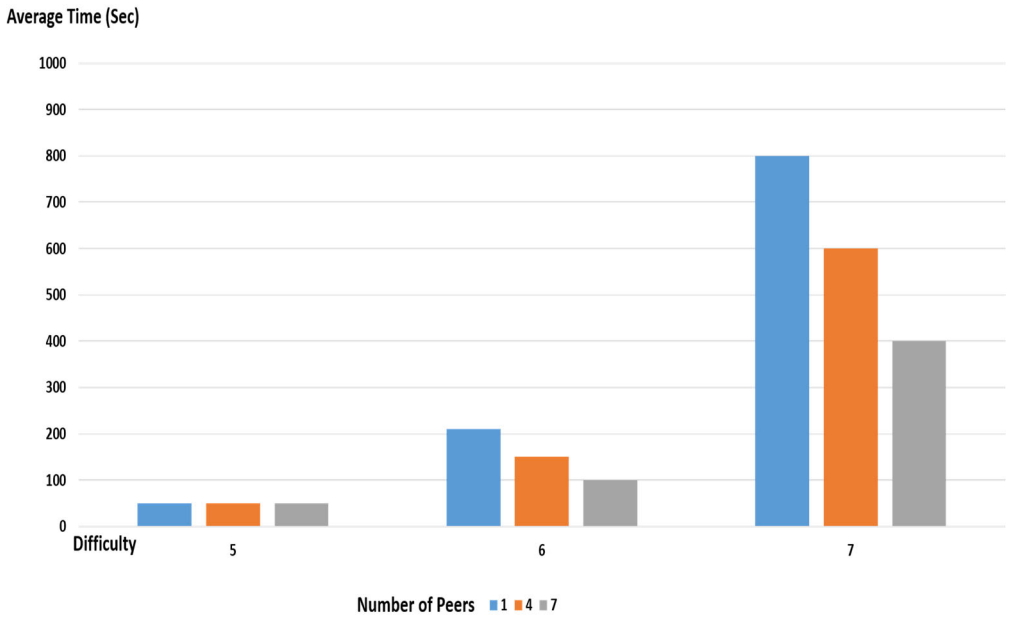

Figure 10. Third scenario results (PSO-POW Model).

As can be noticed from Figure 10, the average time decreases with the increase in peers because the miners are handling the tasks in parallel. Additionally, from Figures 9 and 10, it can be noted that the average time for PSO-POW is less than in parallel mining (second scenario) for the same difficulty level and the number of peers.

Using PSO ensures that there is no suspended time to wait for selecting the best manager, as it automatically selects the miner with the best features. The previous process makes the model more scalable and enhances the overall performance of the model. As in the second scenario (parallel mining without PSO), we face a problem of hanging because of the many miners who end the tasks at the same time. However, PSO solves this problem by fast selecting the best one of them to be a manager, which makes the model faster and more scalable to entering more peers without any effect on model speed or scalability.

All miners in the proposed model must rely on the manager to receive a transaction hash and nonces at the start of each epoch. There may be a single point of failure if the management disconnects or does not reply. However, this is a very unlikely outcome given the suggested PSO process. A selected miner will be rewarded for carrying out their managerial duties.

Table 4 compares our results with most relevant paper for parallel mining [35] against a different difficulty (D) and a different number of peers (P) for 15 blocks, showing the time in minutes. When we compared them against different numbers of peers (7P, 19P, and 25P) we found that POW-PSO outperformed parallel mining with respect to achieved time (POW-PSO achieved little time in minutes, maintaining a minority ratio with an increasing number of peers). This comes from the speed of response in dealing with the single point of failure and the speed of selecting the manager process. So, by increasing the number of peers for POW-PSO, there is a significant decrease in time with robustness of the model (scalability). From another point of view, comparing between two scenarios against a difficulty (block creation time), the minute differences for 7D against 10D when the number of peers is increased from 7P to 25P can be noticed. For the proposed model,

the difference in time from 7P to 25P is the highest for both 7D and 10D as illustrated in Table 4. Thus, we can again ensure that the proposed POW-PSO model was more efficient with increasing difficulty level.

Table 4. Comparison between traditional parallel mining with proposed model (POW-PSO) against achieved results.

Time Required to Solve a Block with	Parallel Mining (Second Scenario) [35]	Parallel Mining with PSO (POW-PSO) Model (Third Scenario)
(15 Blocks/6D/7P)	15.64 min	13.67 min
(15 Blocks/6D/19P)	15.18 min	7.80 min
(15 Blocks/6D/25P)	10.08 min	6.49 min
(15 Blocks/10D/7P)	57.11 min	39.65 min
(15 Blocks/10D/19P)	52.30 min	31.73 min
(15 Blocks/10D/25P)	48.34 min	27.86 min

The single point of failure will only last for the one iteration in which it occurs thanks to the way the proposed model is constructed. The miner can produce the transaction hash and the nonces if a manager does not react. Every miner in blockchain systems without authorization has access to every transaction record. As a result, the miner will use a separate nonce and transaction hash for that block in place of the conventional scheme. Because the miners will work alone rather than in parallel, this sort of period will take longer. However, since the manager was chosen by PSO, the subsequent block will once more adhere to the suggested method.

Another problem which is (many miners solve the hash at the same time) significant is how Bitcoin is now validated. The longest chain is always trusted by Bitcoin clients. The block is therefore accepted by the majority of miners (at least 51%), and is added to the blockchain network if two miners solve the hash simultaneously. The other miners' efforts will be for nothing. For a certain period of time, this condition may occur in a parallel chain in the network. Clients must therefore wait until there are enough confirmed blocks. The typical wait time in Bitcoin is six blocks.

This waiting period is cut down in the suggested PSO-POW model. When two miners complete a hash simultaneously, PSO will automatically choose one of their results to serve as the prior hash for the following block. Along with transaction information and a range of nonces, the manager will disseminate this information to all miners. The manager for the following block will be the miner whose response is chosen by PSO process. Furthermore, the model will prevent more than one miner from serving as a manager for a given block. A parallel chain in the network is therefore less likely than it is in the current setup.

A malicious manager might try to hurt a miner by giving them a used set of nonces. Since the manager must register each nonce range with the system, this is effectively impossible. Multiple users using the same nonce range is not supported by the system. The management is also unaware of miner information until he discovers a solution. Therefore, it is quite improbable that the manager will hurt a particular miner.

A manager cannot be aware of how many peers are working concurrently. As a result, a manager needs to keep creating and registering nonce range to the network. A new peer must request a new nonce range and the transaction data when it first connects. The transaction data and a fresh nonce range that has not yet been used by any miner will then be given to him. This process makes the model more scalable.

Sybil Attack: A malevolent person using numerous fictitious identities attempts a Sybil attack to take over a network or sway its decisions. In effect, this cannot happen because of the manager who controls most of the decisions; additionally, it is changed every iteration to ensure fairness.

Race Condition Attack: An attempt by a bad actor to unfairly advantage themselves by taking advantage of the fact that several nodes frequently run blockchains is known as a race condition attack. This cannot happen in our model, as the manager is the only one that can generate the nonces and control the flood of the blockchain.

6. Conclusions

The suggested model introduces parallel proof of work, in which all miners compete to solve the puzzle simultaneously. The results of our implementation and evaluation of the suggested method in the local environment indicate substantial promise for parallel proof of work as the level of difficulty and the number of miners rise. We propose the automatic manager selection process by using particle swarm optimization algorithm. This process helped in selecting the most appropriate miner to be a manager.

The PSO-POW is for solving the problem of the waiting period. In the event that two miners perform a hash concurrently, PSO will automatically select one of their outputs to act as the prior hash for the subsequent block. The manager will communicate this information to all miners along with transaction information and a variety of nonces. The miner whose response is selected by the PSO process will serve as the manager for the next block. The methodology will also stop multiple miners from acting as managers for the same block. Therefore, the likelihood of a parallel chain in the network is lower than it is in the current configuration.

The appropriate value for parameters is a very important task, as it has an effect on the next steps of the scalable model results. In this thesis, PSO has proved ots efficiency in selecting the appropriate parameters values to obtain the optimal manager for the POW model. In terms of future work, blockchain and transaction processing methods in the field of cryptocurrencies and Bitcoin will be the main focus.

Author Contributions: Data curation, S.T.A.-T.; Formal analysis, S.T.A.-T.; Funding acquisition, N.A.S.; Investigation, N.A.S. and S.T.A.-T.; Project administration, N.A.S.; Resources, N.A.S.; Supervision, N.A.S.; Validation, S.T.A.-T.; Writing—original draft, S.T.A.-T. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to thank SAUDI ARAMCO Cybersecurity Chair, Imam Abdulrahman Bin Faisal University for funding this project.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to express their appreciation to the Journal Editor, an Associate Editor, and the four anonymous reviewers for their insightful comments. We also would like to thank Imam Abdulrahman bin Faisal University for facilitating access to the resources used in this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Antonopoulos, A.M. Cryptocurrency Transaction Speeds: The Complete Review. Available online: https://www.oreilly.com/library/view/mastering-bitcoin/9781491902639/ch01.html (accessed on 25 June 2022).
2. Scribe, G.A. Understanding Cryptocurrency Transaction Speeds. Available online: https://medium.com/coinmonks/understanding-cryptocurrency-transaction-speeds-f9731fd93cb3 (accessed on 25 June 2022).
3. Jaoude, J.A.; Saade, R.G. Blockchain Applications—Usage in Different Domains. *IEEE Access* **2019**, *7*, 45360–45381. [CrossRef]
4. Shahbandi, M. Financial Technologies for Accepting Transactions Using Blockchain Technology and Crypto Currency in Digital Marketing. *Int. Bus. Econ. Stud.* **2021**, *3*, 23. [CrossRef]
5. Bonneau, J.; Miller, A.; Clark, J.; Narayanan, A.; Kroll, J.; Felten, A. SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In Proceedings of the 2015 IEEE Symposium on Security and Privacy, San Jose, CA, USA, 17–21 May 2015.
6. Eberhart, R.; Kennedy, J. A New Optimizer using Particle Swarm Theory. MHS'95. In Proceedings of the Sixth International Symposium on Micro Machine and Human Science, Nagoya, Japan, 4–6 October 1995.

7. Feng, L.; Zhang, H.; Tsai, W.T. System architecture for high-performance permissioned blockchains. *Front. Comput. Sci.* **2019**, *13*, 1151–1165.
8. Amine, M.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet Things J.* **2018**, *6*, 2188–2204.
9. Fu, Z.; Dong, P.; Li, S.; Ju, Y. An intelligent cross-border transaction system based on consortium blockchain: A case study in Shenzhen, China. *PLoS ONE* **2021**, *16*, e0252489. [CrossRef]
10. Gartner. Blockchain Potential and Pitfalls. Available online: https://www.gartner.com/en/webinars/3878710/blockchain-potential-and-pitfalls (accessed on 2 March 2022).
11. Kamal, H.; Moussa, D.; Batrick, S. A Comparative Study of Various Metaheuristic Techniques Applied to The Multilevel Thresholding Problem. *Eng. Appl. Artif. Intell.* **2010**, *23*, 676–688.
12. Huang, K.; Zhang, X.; Mu, I.; Rezaeibagha, F.; Du, X.; Guizani., N. Achieving intelligent trust-layer for internet-of-things via self-redactable blockchain. *IEEE Trans. Ind. Inform.* **2019**, *16*, 2677–2686. [CrossRef]
13. Huemer, C.; Liegl, P.; Zapletal, M. *Handbook of e-Tourism*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 343–371.
14. Khacef, K.; Pujolle, G. *Web, Artificial Intelligence and Network Applications*; Springer International Publishing: Cham, Switzerland, 2019; pp. 662–672.
15. Klapita, V. Implementation of electronic data interchange as a method of communication between customers and transport company. *Transp. Res. Procedia* **2021**, *53*, 174–179. [CrossRef]
16. Kumari, S.; Farheen, S. Blockchain based data security for financial transaction system. In Proceedings of the 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 13–15 May 2020.
17. Kuzmanovic, A. Net neutrality: Unexpected solution to blockchain scaling. *Commun. ACM* **2019**, *62*, 50–55.
18. Lee, S.; Ainin, S.; Dezdar, S.; Mallasi, H. Electronic data interchange adoption from technological, organizational and environmental perspectives. *Int. J. Bus. Inf. Syst.* **2015**, *4*, 299–320.
19. Li, S.; Yu, M.; Yang, C.; Avestimehr, A.; Kannan, S.; Viswanath, P. Polyshard: Coded sharding achieves linearly scaling efficiency and security simultaneously. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 249–261. [CrossRef]
20. Mertz, L. (Block) chain reaction: A blockchain revolution sweeps into health care, offering the possibility for a much-needed data solution. *IEEE Pulse* **2018**, *9*, 4–7. [CrossRef]
21. Miglani, A.; Gupta, H.; Khatri, S. A security model to enhance online transactions using blockchain technology. In Proceedings of the 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 30–31 August 2018.
22. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. *Decentralized Bus. Rev.* **2008**, 21260. Available online: https://assets.pubpub.org/d8wct41f/31611263538139.pdf (accessed on 5 April 2022).
23. Nordrum, A. Govern by blockchain dubai wants one platform to rule them all, while illinois will try anything. *IEEE Spectr.* **2017**, *54*, 54–55. [CrossRef]
24. Novinkina, J.; Davydovitch, A.; Vasiljeva, T.; Haidabrus, B. Industries pioneering blockchain technology for electronic data interchange. *Acta Logist.* **2021**, *8*, 319–327. [CrossRef]
25. PwC. Blockchain Is Here. What's Your Next Move? Available online: https://www.pwc.com/jg/en/publications/blockchain-is-here-next-move.html (accessed on 5 April 2022).
26. Sakho, S.; Jianbiao, Z.; Essaf, F.; Badiss, K. Improving banking transactions using blockchain technology. In Proceedings of the 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 6–9 December 2019.
27. Sangwan, R.; Kassab, M.; Capitolo, C. Architectural considerations for blockchain based systems for financial transactions. *Procedia Comput. Sci.* **2020**, *168*, 265–271. [CrossRef]
28. Scherer, M. Performance and Scalability of Blockchain Networks and Smart Contracts. Master's Thesis, Umeå University, Umeå, Sweden, 2017.
29. Shahnaz, A.; Qamar, U.; Khalid, A. Using blockchain for electronic health records. *IEEE Access* **2019**, *7*, 147782–147795. [CrossRef]
30. Hazari, S.S.; Mahmoud, Q. Improving transaction speed and scalability of blockchain systems via parallel proof of work. *Future Internet* **2020**, *12*, 125. [CrossRef]
31. Shen, C.; Pena-Mora, F. Blockchain for cities—A systematic literature review. *IEEE Access* **2018**, *6*, 76787–76819. [CrossRef]
32. Sundareswaran, N.; Sasirekha, S.; Shanmugapriya, T.; Paul, I.; Sharma, S. Secure banking transaction using blockchain. In Proceedings of the AIP Conference Proceedings, Kozhikode, India, 26 March 2021.
33. Veselá, L. Factors affecting the adoption of electronic data interchange. *Acta Univ. Agric. Silvic. Mendel. Brun.* **2017**, *65*, 2123–2130. [CrossRef]
34. Veselá, P.; Cempírek, V.; Stopková, M.; Bartuš, L. Various electronic data interchange (EDI) usage options and possible substitution. *NAŠE MORE Znan. Časopis Za More I Pomor.* **2018**, *65*, 187–191.
35. Wan, N.; Liu, Y.; Xiao, W. A financial transaction methods based on mapreduce technology and blockchain. In Proceedings of the 2020 3rd International Conference on Smart BlockChain (SmartBlock), Zhengzhou, China, 23–25 October 2020.
36. Wood, G. On Sharding Blockchains. Available online: https://github.com/ethereum/wiki/wiki/Sharding-FAQ (accessed on 10 July 2022).
37. Wood, G. Ethereum: A secure decentralized generalized transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.

38. Xenya, M.C.; Quist-Aphetsi, K. Decentralized distributed blockchain ledger for financial transaction backup data. In Proceedings of the 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), Accra, Ghana, 29–31 May 2019.
39. Yao, H.; Mai, T.; Wang, J.; Ji, Z.; Jiang, C.; Qian, Y. Resource trading in blockchain-based industrial internet of things. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3602–3609. [CrossRef]
40. Yao, Q.H.; Xiao, X. White paper on the development of insurance science and technology in china. *China Insur. Sci. Technol. Lab. Fudan Univ.* **2017**, *14*, 87–99.
41. Yunitarini, R.; Santoso, P. A literature review of electronic data interchange as electronic business communication for manufacturing. *Manag. Prod. Eng. Rev.* **2018**, *9*, 117–128.
42. Zhao, B.; Wang, R.; Cai, Y.; Zhao, E. Block chain financial transaction using artificial neural network deep learning. In Proceedings of the IOP Conference Series: Materials Science and Engineering, Xi'an, China, 25–27 October 2019.
43. Jain, M.; Kaswan, S.; Pandey, D.; Bajal, E.; Katara, V.; Bhatia, M.; Hooda, M. A blockchain-based fund management scheme for financial transactions in NGOS. *Recent Pat. Eng.* **2021**, *16*, 3–16.
44. Xue, B.; Zhang, M.; Browne, W.N. particle swarm optimization for feature selection in classification. A multi-objective approach. *IEEE Trans. Cybern.* **2013**, *43*, 1656–1671.
45. Namrata, K.; Pawanesh, A. Wrapper-based optimized feature selection using nature-inspired algorithms. *Neural Comput. Appl.* 2023, *in press*.
46. Hill, A. The Pioneer's Guide to GX—Decentralized Dependency Management on IPFS, Hacker Noon. Available online: https://hackernoon.com/the-pioneers-guide-to-gx-decentralized-dependencymanagement-on-ipfs-90064858f4c2 (accessed on 10 October 2022).
47. Shaker, A.; Douglas, S. Self-stabilizing structured ring topology p2p systems. In Proceedings of the Fifth IEEE International Conference on Peer-to-Peer Computing (P2P'05), Konstanz, Germany, 31 August 2005–2 September 2005.
48. Salah, K.; Habib, M.; Nizamuddin, N.; Al-Fuqaha, A. Blockchain for ai: Review and open research challenges. *IEEE Access.* **2019**, *7*, 10127–10149. [CrossRef]