

Enhancement of security and handling the inconspicuousness in IoT using a simple size extensible blockchain

Saravana Balaji, B.; Vishnu Raja, P.; Nayyar, Anand; Sanjeevikumar, P.; Pandiyan, Sanjeevi

Published in:
Energies

DOI (link to publication from Publisher):
[10.3390/en13071795](https://doi.org/10.3390/en13071795)

Creative Commons License
CC BY 4.0

Publication date:
2020

Document Version
Publisher's PDF, also known as Version of record

[Link to publication from Aalborg University](#)

Citation for published version (APA):

Saravana Balaji, B., Vishnu Raja, P., Nayyar, A., Sanjeevikumar, P., & Pandiyan, S. (2020). Enhancement of security and handling the inconspicuousness in IoT using a simple size extensible blockchain. *Energies*, 13(7), Article 1795. <https://doi.org/10.3390/en13071795>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.




- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal -

Take down policy

If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

Article

Enhancement of Security and Handling the Inconspicuousness in IoT Using a Simple Size Extensible Blockchain

B. Saravana Balaji ¹, P. Vishnu Raja ², Anand Nayyar ^{3,*} , P. Sanjeevikumar ⁴ 
and Sanjeevi Pandiyan ⁵ 

¹ Department of Information Technology, Lebanese French University, Erbil 44001, KR, Iraq; saravanabalaji.b@gmail.com

² Department of Computer Science and Engineering, Kongu Engineering College, Erode 638 060, Tamilnadu, India; pvishnu@kongu.ac.in

³ Graduate School, Duy Tan University, Da Nang 550000, Vietnam

⁴ Department of Energy Technology, Aalborg University, Esbjerg 6700, Denmark; san@et.aau.dk

⁵ Key Laboratory of Advanced Process Control for Light Industry, Ministry of Education, Jiangnan University, Wuxi 214122, China; gpsanjeevi@jiangnan.edu.cn

* Correspondence: anandnayyar@duytan.edu.vn

Received: 3 February 2020; Accepted: 27 March 2020; Published: 8 April 2020



Abstract: Blockchain technology is increasingly used worldwide to enhance the performance and profit of any environment through its defining characteristics, such as security, auditability, immutability, and inconspicuousness. Owing to these characteristics, the blockchain can be used in various non-financial operations of some domains, such as the Internet of Things (IoT) and distributed computing. However, implementing blockchain technology in IoT is not always a feasible solution because blockchain deployment is costly, it has limited extensibility and provides irregular bandwidth and latency. In this regard, a simple size extensible (SSE) blockchain has been proposed to provide an optimal solution for IoT environments by satisfying the needs of the IoT environment as well as ensuring end-to-end security. The implementation of the proposed blockchain develops an overlay network to obtain a distributed environment where the blockchain is handled by the resources present therein. Two novel algorithms were introduced into the proposed system to minimize the irregularity and latency on one hand, and to maximize the throughput of the system on the other. The shared-time depending agreement algorithm (STD) minimizes the irregularity in the extraction operation and latency. The other, the shared throughput administration algorithm (STA) justifies the overall collection of the transmission load in the network and maintains the performance of the blockchain. The proposed system was applied to smart home IoT appliances to test the performance of the proposed system. The experimental results show that the proposed blockchain system minimizes nearly 70% of the data irregularity, latency, and furthermore, 30% of the blockchain extensibility is maximized as compared to the existing systems.

Keywords: blockchain; Internet of Things; simple size extensible; security; inconspicuousness; shared-time depending agreement algorithm (STD); shared throughput administration algorithm (STA)

1. Introduction

In today's world, the use of blockchain technology is popular in various fields such as healthcare, big data, finance, law, cyber security, and supply chain management, for example, Blochie, a blockchain-based platform for healthcare information exchange and TSAR, a fully-distributed trustless

data sharing platform. Blockchain is popular because of several characteristics such as its decentralized network style, auditability, security, immutability, and inconspicuousness [1]. In this paper, the word “activities” refers to “transactions”. Shared digital notes of activities are managed by the blockchain, which is distributed among all the working nodes in the environment. Most of the auditability process can be done through the activities stored in the digital notes. The process is decentralized in the blockchain, where all transactions are evaluated and checked by all other processing nodes in the environment. A group of distinctive nodes, called miners, are used to append activities to the collection of activities waiting for transmission, in which the appended activities are produced as new ones. The appended activities are merged with the waiting activities in the block through the miner, whereby the size of the merged activities touches the limit of the size of the block. When the new block is included in the blockchain environment, an agreement algorithm is used in the blockchain environment to ensure that it is secure against malevolent miners and inappropriate transactions.

Traditionally, deployment of the blockchain uses proof-of-work or proof-of-stake protocols [2]. In order to extract the next block, the proof-of-work strategy requires maximum computing resources to defeat the agreement algorithm. Similarly, the proof-of-stake strategy requires the miners to latch their stake or property into the blockchain network to extract the next block. A public key is used as an identification card for every user when they generate activities, which results in the maximum level of inconspicuousness in the blockchain network [3].

Blockchain, owing to its characteristics, has been integrated into the IoT to enhance security, auditability, reliability, and inconspicuousness. Traditional IoT architectures have several disadvantages or restrictions, such as the utilization of resources and its centralized structure [4–13]. The merits of the blockchain technology solve some of these issues. IBM developed a new blockchain strategy called Hyperledger fabric, whereby only legitimate nodes can access the blockchain network [14]. Even though the blockchain has many merits, it also has some disadvantages and challenges such as extensibility and irregular transmission of data, complicated agreement algorithms, delay, and throughput. The primary objective of this research work is to provide solutions to the above-mentioned issues.

In this regard, the proposed approach introduces the simple size extensible (SSE) blockchain for the IoT. In order to maintain the blockchain and to provide extensibility, the chiefs of the clusters (CC) will take charge. The cluster contains components of the IoT, storage from the cloud, and service providers. The cluster is formed to represent these things as an overlay network. The administration of the blockchain contains valuation and checking and storage of every single activity or block of activities. An activity is said to be the fundamental interaction for networking the authority data among the nodes. A block is developed through the collection of activities where these blocks are added to the blockchain to generate the shared digital notes. In SSE blockchain, the information regarding the IoT components is stored in the cloud storage and not in the chain. This is done to minimize the amount of memory and irregularity of the packet in the blockchain. The exchange of information among the IoT components is not included in the activity flow.

After the information about the packets is updated at the receiver's ends, the activities based on these packets are transmitted through the overlay nodes to the receiving block of the blockchain environment. The process of individuality in the exchange of information among the IoT components results in the best one-to-one scheduling of information packets. Finally, the latency and irregularity of packets are minimized while the information is exchanged. The shared time depending agreement algorithm (STD) has been proposed to minimize any irregularity in the extraction operation in the blockchain. Here, every CC has to wait for a non-interval time before extracting the new block. The STD restricts the CC's ability to produce new blocks within a stipulated time in order to provide security against malevolent CCs. The SSE blockchain appoints a shared faith algorithm to minimize the processing irregularity along with evaluating and checking new blocks that are to be included in the blockchain. Each CC collects proof about the other CCs, depending on the lifetime of the produced new blocks. No verification process has not been done for the activities that have gained the trust of the chiefs of clusters.

Lastly, the shared throughput administration (STA) algorithm was proposed to improve the throughput of the blockchain. The STA ensures maximization of the throughput by adopting extensibility in the blockchain by adding new blocks in the network.

The objectives of this paper are as follows:

- To reduce the gap between the IoT and the blockchain
- To generate a flexible extensible for obtaining more activities in the blockchain
- To perform secure activities and disseminate the blockchain technology in the outside world through the IoT.

The rest of the paper is organized in five sections. Section 2 examines and analyses the literature. The proposed model is outlined in Section 3 and the results are given and discussed in Section 4. Section 5 concludes the paper and considers the implications for the future.

2. Literature Review

A detailed literature review based on the security and inconspicuousness of the IoT and blockchain systems was carried out to examine previous research with the clear objective of finding the optimal solution.

According to Saberi et al. [15], there are still several barriers that prevent the development of a definitive blockchain technology (e.g., inter-organizational barriers, external barriers, and intra-organizational barriers). They refer to supply chain management, but many of the barriers they identify can also be applied in other contexts. Blockchain is not the solution to everything because many limitations and challenges still exist. Astarita et al. [16] states that blockchain technology is promising, but much effort is still necessary for it to reach the maturation stage. The main reason for this is that many models have been theorized in recent years, but only a few have been practically implemented in the area of supply chain and logistics, road traffic management, and smart cities. It is essential to note that the regulatory framework linked to the blockchain is complex, and many questions remain unanswered in this area.

Yeoh [3] analyzed how key regulatory challenges are impacting blockchains in the European Union and the USA. Khan et al. [1] and Panarello et al. [17] highlighted the research problems and challenges regarding blockchains, security, and IoT. Cachin [18] proposed a novel Hyperledger blockchain fabric architecture in which the network overhead was minimized by removing unwanted header fields. This resulted in minimizing the size of the header of the 6LoWPAN and host identity protocol to 25 bytes [18]. To protect the network against illegal users and processes, a novel access control and authentication mechanism was proposed to ensure the security and extensibility of the IoT environment by Liu et al. [19]. In SSE blockchain, one blockchain infrastructure has been proposed and it is maintained through the network of overlay nodes. The components evaluate and authenticate various overlay nodes in the network by refreshing the list of keys in the overlay block administrator. The proposed system performs well by providing better extensibility and optimal security against a more extensive boundary of attacks.

The concept of bitcoin introduced the methodology of blockchain [20]. The objective of the bitcoin was to eliminate the concept of centralization and to promote the decentralization of money transfers by providing maximum security to the users. Ethereum, a novel blockchain methodology was proposed whereby users can develop and utilize intelligent working agreements with a minimum amount of network performance but with maximum security [4]. It had been used in many blockchain applications such as agriculture, to provide grant information, and mini blogging [21,22]. A new technique for energy trading was proposed in which energy developers could negotiate the market price with their consumers by generating an intelligent work agreement to perform the vending. A shared process manager was included in the system to provide security in the energy trading on both sides for the customer and the energy developers [23]. A three-tier mechanism for blockchain was proposed to distribute information among the components of the IoT, companies, and users.

The mechanism develops a separate blockchain to store the information in a secure manner [24]. The proposed system does not depend on separate blockchains for storing the information. Here, the information is stored in the form of the hash in the cloud storage in the blockchain.

Internet of Things Application (IOTA) is a digital note, which depends on cryptocurrency that removes the concept of blocks. It also extracts the details to the environment, which helps to minimize the time required to verify the activities [25]. IOTA is a distributed ledger designed to record and execute transactions between machines and devices in the IoT ecosystem. The ledger uses a cryptocurrency called mIOTA to account for transactions in its network. IOTA's key innovation is Tangle, a system of nodes used to confirm transactions. There is some similarity between the SSE blockchain and the IOTA. Both techniques do not charge for the activities, and both adopt an extensible network. Due to this, the proposed SSE blockchain has the advantage of proper auditability through the immutability of digital notes.

A standard blockchain technique was proposed to provide faith in the vehicular networks [8]. An efficient resource clustering model was proposed to develop an efficient wireless cloud that will help future blockchain environments [26]. The system utilizes the shared faith of all the processing nodes in the environment. The proposed SSE blockchain utilizes the same type of shared faith but minimizes the operational irregularity for checking the new blocks in the blockchain. The GraphCoin technique [27] was proposed to provide the solution for the extensibility in the digital money transactions. The technique aims to validate the security and individuality of the users. Further, a technique called catena was proposed to minimize the irregularity in blockchain auditability and to maximize the throughput of the network. It also enables the establishment of the interactions among the various authors out of the blockchain to minimize the audit and storage of the network [28].

The Memory Optimized and Flexible Blockchain (MOF-BC) method was proposed to facilitate the elimination of activities in the blockchain database, optimize the memory and provide reliable blockchain. Blockchain does not allow for the elimination of activities. The MOF-BC method manages the stability in the blockchain [29]. An agreement algorithm based on proof-of-authority can be related to the proof-of-stake, in which the extracting strength of every extractor depends on its address in the environment instead of the number of latches it owns [30]. Intel developed an agreement algorithm known as the proof-of-elapsed-time to work in the blockchain, in which it is merged with the Hyperledger. The proof-of-elapsed-time algorithm is a chief voting algorithm that was designed to run in a faith deployment network [31]. Another agreement algorithm named AlgoRand is proposed, which depends on Byzantine understanding in which the extractors shall have an understanding in a single meeting of execution [7]. The shared version of Byzantine understanding called federated Byzantine understanding was proposed to facilitate the nodes in the environment to select the evaluators [14]. Restricted or minimum throughput are the major disadvantages of the traditional agreement algorithms. When it comes to the security of the blockchain, the traditional systems restrict the number of blocks that can be included in the blockchain, thus, the throughput of the blockchain is minimized. The proposed STD manages the required blocks through the feedback of the proposed STA to maintain an optimal or to maximize the throughput of the blockchain network. This results in the extensibility of blockchain for the IoT through the proposed STA algorithm and also reduces the gap between the IoT and blockchain.

3. Proposed Simple Size Extensible (SSE) Blockchain

An overlay network is developed by the processing and operating components in the blockchain, such as components of the IoT, users of the IoT, and service providers. The overlay network is depicted in Figure 1. The public key is assigned to every node in the overlay network. In order to ensure inconspicuousness, the new public key is used by the nodes to develop every new activity. Due to some of the restrictions on the IoT, such as limited resources, it is very difficult for it to check every activity of every new block. In order to improve the extensibility and to minimize the operation and irregularity in the packet on the IoT components, one of the inner parts of the overlay nodes maintains the blockchain. Clustering algorithms will be used to form the clusters among the nodes [32,33].

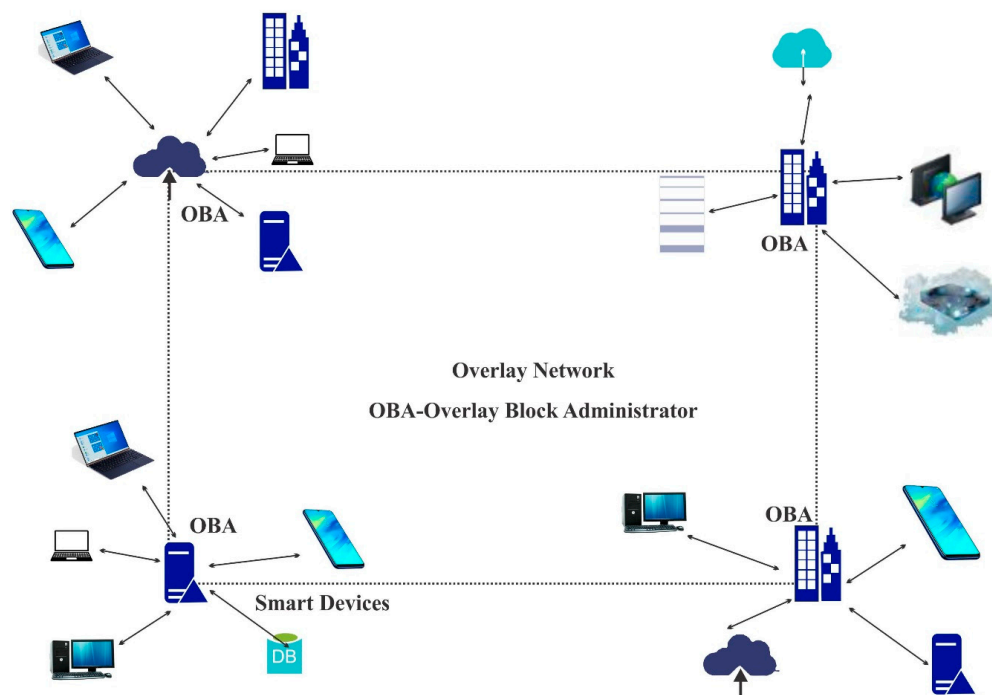


Figure 1. Structure of the overlay network and overlay block administrator.

A cluster head is then selected based on the protocol stated by the clustering algorithm [16]. The overlay block administrators (OBA), acting as the chiefs of the clusters, take charge of maintaining the blockchain. The maintenance of the blockchain includes production, checking, and storage of every activity and block. The participants of the clusters verify the work of the OBA. If any doubt or irregularity regarding the OBA is identified by the participants of the cluster, it will not be transferred to the other OBAs. Instead, a new OBA will be created and selected for transferring the activity.

In the current scenario, Tablet requires interaction with the service provider server. The activities of Tablet are stored in the blockchain. Tablet exchanges the needed information with the server of the service provider, which is required to be done in the blockchain. It is already stated that the information exchange of the SSE is different from the activities. One-to-one communication has been maintained for all of the widely spread activities in the environment. The optimal routing has been performed for these activities by the overlay network. The proposed algorithm supports any scheduling algorithm because it is designed in a flexible manner.

The overlay network uses some scheduling algorithms to perform this scheduling. Here, a scheduling algorithm based on ant colony optimization is used. In order to transmit the information packets, the receiver's overlay block administrator identification should be shared informally in the activities that facilitate the overlay block manager to schedule the packet. As a result, this minimizes the irregularity in the packet during transmission or information interaction. The activity producer authorizes the activity interaction among the overlay nodes through the hash of the information to produce the data integrity. In SSE, all the activities are loaded in the blockchain. The information regarding the IoT components is loaded outside of the blockchain to minimize the irregularity of the packet and utilization of memory in the blockchain. Together, a faith Table record, the faith rate of the other overlay block administrators, and the timeclock specify the creation time of the blocks produced by various overlay block administrators of the blockchain environment. At least " y " verifications (y is checked) should be done out of " x " verifications (x is checked) where x and y are some constant variables. This process is performed to check whether the activity generated by the user is valid or not.

Cryptographic techniques such as digital signatures, hash functions, and asymmetric encryption are used to secure the activities produced by the overlay node. Activities in the blockchain are divided into one-sign activities, and multi-sign activities. One-sign activities constitute only the sign of the

activity producer. Multi-sign activities constitute the need for many signs for the actual activities. A multi-sign activity needs y out of x signs, in which y and x are the number of signs and $x \geq y$. For instance, the structure of the activity is given as

$$A_RC||P_A_RC||OS||Veri||Result||data\ about\ data$$

A_RC represents the activity identifier that constitutes the hash of the activity subject. P_A_RC represents the pointer of the predecessor activity of the overlay node. The overlay node develops one or more sign activity and one-sign activity, which is to merge within the same blockchain and audit in the future. These things can be done through the OS outside security and the verification sign of the activity producer. The verified A_RC will be utilized for the verification of the activity. In the situation of one or more sign activity, the outside security OS , and the verification sign of the various processing, the node will operate the result section. In order to perform a valid activity, y signs are needed out of the x signs. As a cumulative x will be the overall activity, in that the y activity which is appended by the user should be verified to ensure that the activity is valid. The result section includes the outside security OS hash function, which the activity producer will utilize for its successor activity. It is mandatory to check the following activity developed by the node of the same overlay network where the OS outside security is changed by the overlay nodes in which it is used to produce each new activity.

The data about the data section generates the added data about the processing nodes in the activity, which could be present in the future. For instance, the activity is produced to obtain the required information from the components of the IoT at a particular time. The time is mentioned in the data about the data section. The above sections are needed for an activity that is stated as valid. Meanwhile, the other sections can be specified according to the application. The original activity is developed as the initial operation of the overlay node that acts as the source end for the digital notes in the blockchain by utilizing any of the given techniques mentioned below. One of these techniques is guarantee authorization [34]. Here the node depends on the broadly implemented outside security infrastructure of the global web. The nodes in the overlay network communicate a faith guarantee authorization that approves the node in outside security by connecting a verified guarantee. The node adds the guarantee in the initial activity. An overlay block administrator checks the guarantee to check the activity. The overlay block administrator has the right to process the collection of faith-oriented guarantee authorization to do the checking.

Another technique is removing the coin in bitcoin. Some of the nodes will not depend on the outside security infrastructure; in such cases, the node internally develops an initial activity by removing bitcoins [35]. The node develops a non-temporary activity in the bitcoin blockchain by eliminating a needed quantity of coins, known as burning coins. The location of the removed activity is taken as the information for the initial activity. Each cluster has some number of overlay networks in the blockchain-embedded IoT network. The nodes in the overlay network develop an initial activity with outside security as the removed activity and transfer it to the overlay block administrator and depend on its cluster. In some cases, the overlay block administrator acts as an initial activity producer at that time and communicates the activity to other overlay block administrators. In order to check the arrived initial activity, the overlay block administrator compares the outside security of the initial activity with the outside security of the removed activity in the bitcoin blockchain. After that, the overlay block administrators check the sign in the initial activity.

After checking, the abovementioned techniques utilize overlay block administrators to transfer the initial activity to various overlay block administrators, so as to be loaded in the blockchain. In the SSE blockchain, the flow of information is maintained ideally from the flow of activity. Like the bitcoin, more than one activity is combined and then operated as a single block. The maximum number of activities stored at a single block is represented as A_high activities. The capacity of the A_high creates changes in the throughput of the blockchain, so that many activities can be loaded in the one block

with a maximum A_{high} . Every block includes two major components, such as activities and a block chief. The block chief is represented as given below,

$$B_RC || L_B_RC || B_Producer || B_Checkers$$

The hash function reveals information about the block, and it is represented as B_RC . The hash function of the last block is represented by L_B_RC and ensures immutability in the blockchain environment. Consider a scenario: an intruder tries to alter the last loaded activity, then the hash function of that particular block loaded in the consecutive block will not work and it will announce the involvement of the intruder. To obtain extensibility, activities and blocks are shared with the overlay block administrators. In the situation of multi-sign activity, the activities will not be considered as actual until y out of x processing nodes in the activities have included their sign.

The resolution of this issue lies in managing a security collection by the overlay block administrator. Security collection includes the collection of outside securities that can process and communicate with the cluster members. The flowchart of the SSE blockchain is shown in Figure 2. The activities are shared in the cluster to secure the characteristics of the members in the cluster against malevolent overlay block administrators. There is a possibility that the malevolent overlay block administrators will follow the activities accepted by the corresponding member of the cluster to connect various activities, and it will misguide the node. Therefore, from the receiving activities, one of the outside security B is compared with the arrival in the security collection. Then, the overlay block manager transfers the activities to the members of the cluster in which it has stored the security during the security collection. In either case, the activity will be shared with all other overlay block administrators. All unresolved activities are loaded into the activity pool at each overlay block manager. If A_{high} equals the capacity of the execution collection, the overlay block administrator develops the new block using a shared time depending agreement algorithm (STD).

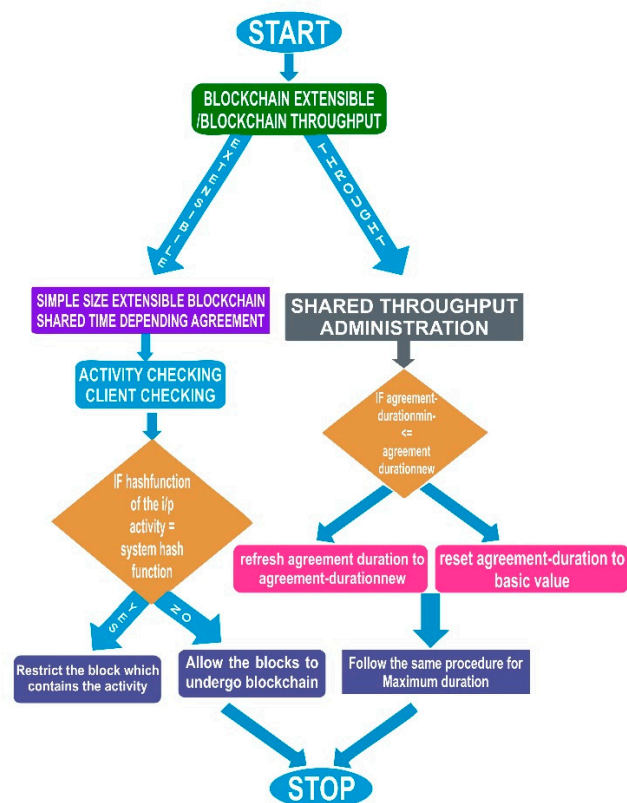


Figure 2. Flowchart of the proposed simple size extensible (SSE) blockchain.

3.1. Shared-Time Depending Agreement Algorithm (STD)

The proposed simple size extensible blockchain introduced an agreement algorithm based on the time duration called the shared-time depending agreement algorithm. The primary objective of any agreement algorithm is to make sure that a block produced is based on random picking, and the fact that there will be limitations in the number of blocks produced. As a result, it secures the blocks against the malevolent blocks. Each and every overlay block administrator will have some latency time before producing a new block. This is done to ensure randomness is achieved in producing the block by the block producers. Some of the overlay block administrators request more short latency time than their quota. At that time, other overlay block administrators check the duration of the new block production from the particular overlay block administrator. By doing this, it limits the overlay block administrators from requesting the short latency time. In such situations, if any overlay block administrator exceeds its count on block production, the extra blocks, as well as their activities will be eliminated. Thus, the standard latency time will minimize fake block production, which is a continuous process if there is no standard latency time. More importance is given to the new block production because these new blocks are shared further in the overlay network and included in the blockchain.

The proposed system limits the number of new blocks generated by the OBAs. A malevolent overlay block administrator may occur, which acts as described above. In order to restrict the malevolent overlay block administrator, a technique called durability utilization is proposed. The objective is to ensure that the overlay block administrator can produce the new block only during that particular duration.

The shared throughput administrator (STA) algorithm is used to maintain durability. The verification process for the activity is described through an algorithm called activity checking, as shown in Algorithm 1.

Algorithm 1: Activity Checking

1. Input: Overlay Activity (O)
 2. Output: True or False
 3. Client Checking:
 4. if (hash function (O.OS) \neq O_1.result) then
 5. return False;
 6. else
 7. if (O.OS rescue O.verification Sign) then
 8. return True;
 9. end if
 10. end if
-

3.2. Shared Throughput Administrator (STA)

The existing blockchain algorithms that are -based on agreement minimize the throughput of the environment. The amount of activity processed in the blockchain per second is minimized. However, when some agreement algorithms are used for the components of IoT, these types of restrictions will not be accepted because the nodes in the IoT environment communicate with all other nodes in various ways. These issues can be resolved by, the proposed simple size extensibility blockchain, which introduces an algorithm called the shared throughput administrator strategy, to ensure the proper usage of the blockchain and also to provide valuable duration. In this algorithm, the overlay block administrator calculates the usage β as the ratio of the sum of new activities produced to the sum of activities included in the blockchain. The objective of the shared throughput administrator is to make sure the value range is set by the β as $(\beta_{min}, \beta_{max})$. The mathematical formula for processing the β is as follows

$$\beta = \frac{E \times V \times Durability}{A_{max} \times P} \quad (1)$$

Here, E represents the endpoint devices of the environment, P represents the overlay block administrators, and V represents the mean value of the new activity the node produces per second. When performing calculations, the counts, or values should be specified. The usage of the duration can be altered based on this specification in two ways: first, by altering the duration time, which represents the repetitions of the blocks included in the blockchain; second, by altering the P -value in which every overlay block administrator can produce one block within the duration time. These two ways are represented in the algorithm shared throughput administrator, as depicted in Algorithm 2.

Algorithm 2: Shared Throughput Administration

```

1. Input:  $\beta$ 
2. while True do
3.   if ( $\beta > \beta_{max}$ ) then
4.     Calculate agreement-durationnew with the formula  $\beta = \frac{\beta_{min} + \beta_{max}}{2}$ 
5.     if (agreement-durationmin  $\leq$  agreement-durationnew) then
6.       refresh agreement-duration to agreement-durationnew
7.     else
8.       reset agreement-duration to basic value
9.     Calculate Z from the formula  $\beta = \frac{\beta_{min} + \beta_{max}}{2}$ 
10.    Cluster again overlay
11.    end if
12.  end if
13.  if ( $\beta < \beta_{min}$ ) then
14.    Calculate agreement-durationnew with the formula  $\beta = \frac{\beta_{min} + \beta_{max}}{2}$ 
15.    if (agreement-durationnew  $\leq$  agreement-durationmax) then
16.      refresh agreement-duration to agreement-durationnew
17.    else
18.      reset agreement-duration to basic value
19.    Calculate Z from the formula  $\beta = \frac{\beta_{min} + \beta_{max}}{2}$ 
20.    Cluster again overlay
21.    end if
22.  end if
23. end while

```

A maximum level field of vision for all algorithms running through the overlay block administrator to maintain the proposed simple size extensible blockchain, is described through the algorithm given below. An overlay block administrator may either obtain an activity A or a Block C through the various overlay block administrators. As in the previous case, the overlay block administrator initially checks the activity, and if it is acceptable, it is included in the collection of waiting activities. In a situation such as $A_Collection \geq \text{block capacity } A_max$, these activities are combined to develop a block. Non acceptable transactions are eliminated. In some situations, the overlay block administrator checks the block initially by checking the related activities. The overlay block administrator uninterruptedly runs the shared throughput administrator through the same collection of threads to maintain the throughput of the simple size extensible blockchain in relation to the job of the environment as shown in Algorithm 3.

Algorithm 3: A maximum level field of vision of algorithms implemented by an overlay block administrator

```

1. Input: A, C
2. while True do
3.   Obtaining from Blockchain
4.   if attain an A then
5.     if (A is acceptable) then
6.       A_collection += A
7.       if (capacity.A_collection ≥ A_max) then
8.         Execute Shared Throughput Administrator Algorithm
9.       end if
10.    else
11.      Discard A
12.    end if
13.  end if
14.  if Attained a C then
15.    Check block
16.  end if
17.  Execute Shared Throughput Administrator Algorithm
18. end while

```

4. Results and Discussion

This section details the results and discusses the research work. The results have been obtained and verified using the following parameters: irregularity of packets (in kilobytes), the number of overlay block administrators used, operating time (in milliseconds), and the percentage of activities checked for the blockchain environment. Tables 1–3, and Figures 3–5 show the comparative results for the existing systems such as the lightweight, scalable blockchain and baseline overhead, and the proposed system, i.e., the simple size extensible blockchain based on the packet irregularity and operating time. Tables 4–6 and Figures 5–8 show the comparative results for the existing systems such as lightweight, scalable blockchain and baseline overhead, and the proposed simple size extensible blockchain based on the percentage of activity checked and operating time.

Table 1 and Figure 3 depict the performance of an existing system, the baseline packet overhead. Here, the operating time and packet irregularity is highlighted. The operating time is measured in milliseconds, and packet irregularity is measured in kilobytes. Table 1 gives the actual number of overlay block (OB) administrators whereas the graph depicts this as a whole. The OB administrators from 1 to 2 have an operating time of 1.0×10^{12} ms and the packet irregularity is 239.141 KB. Moreover, the procedure followed is the same for the remaining OB administrators.

Table 1. Existing system baseline packet overhead operating time and packet irregularity.

Basic Attack Identifier		
Number of OB Administrators	Operating Time in Milliseconds	Packet Irregularity in KB
0.87902	1.0×10^{-4}	239.141
3.93113	2.7×10^{-4}	614.905
6.79819	6.6×10^{-4}	1597.62
9.78487	0.001	2512.62
12.6566	0.00127	3225.67
15.823	0.00153	3871.1
18.8064	0.00195	4988.35

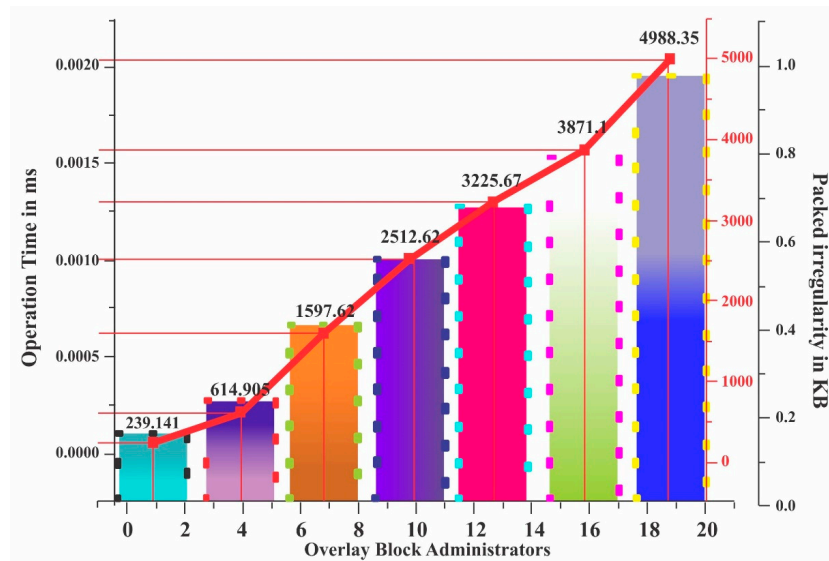


Figure 3. Existing system basic attack identifier timespan and transaction irregularity.

Table 2 and Figure 4 depict the performance of another existing system called the light weight scalable blockchain. Here, the operating time and packet irregularity is examined. The operating time is measured in milliseconds, and packet irregularity is measured in kilobytes. Table 2 gives the actual number of overlay block administrators, whereas the graph depicts this as a whole. The OB administrators from 1 to 2, have an operating time of 1.0×10^{12} ms and the packet irregularity is 170.133 KB. Moreover, the procedure followed is the same for the remaining OB administrators.

Table 2. Existing system sympathy attack identifier timespan and transactions irregularity.

Sympathy Attack Identifier		
Number of OB Administrators	Operating Time in Milliseconds	Packet Irregularity in KB
0.87902	1.0×10^{-4}	170.133
3.93113	2.7×10^{-4}	546.196
6.79819	6.6×10^{-4}	1259.14
9.78487	0.001	1971.69
12.6566	0.00127	2550.01
15.823	0.00153	3027.1
18.8064	0.00195	3874.68

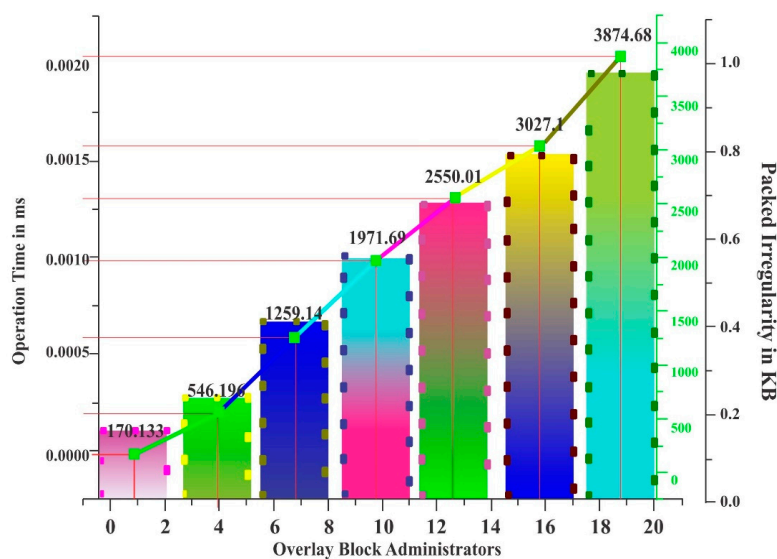


Figure 4. Existing system lightweight scalable blockchain operating time and packet irregularity.

From the above results, it can be seen that the proposed system, the simple size extensible blockchain performs well when compared to existing systems such as the baseline overhead and lightweight scalable blockchain in terms of packet irregularity and operating time. The proposed system minimizes the packet overhead as well as the operating time of the blockchain environment. It produces packet irregularity in the range of 101.124 kilobytes to 3337.08 kilobytes, which is shown in Table 3 and Figure 5. Meanwhile, the existing baseline overhead system produces packet irregularity in the range of 239.141 kilobytes to 4988.35 kilobytes, which is shown in Table 1. The existing system, the lightweight, scalable blockchain, produces packet irregularity in the range of 170.133 kilobytes to 3874.68 kilobytes, which is shown in Table 2.

Table 3. Proposed system simple size extensible blockchain operating time and packet irregularity.

Simple Size Extensible Blockchain		
Number of OB Administrators	Operation Time in Milliseconds	Packet Irregularity in KB
0.99707	6.7×10^{-5}	101.124
3.92962	1.8×10^{-4}	337.079
6.86217	4.5×10^{-4}	943.82
9.85337	7.0×10^{-4}	1685.39
12.9619	9.2×10^{-4}	2089.89
15.8944	12.1×10^{-4}	2595.51
18.827	16.7×10^{-4}	3337.08

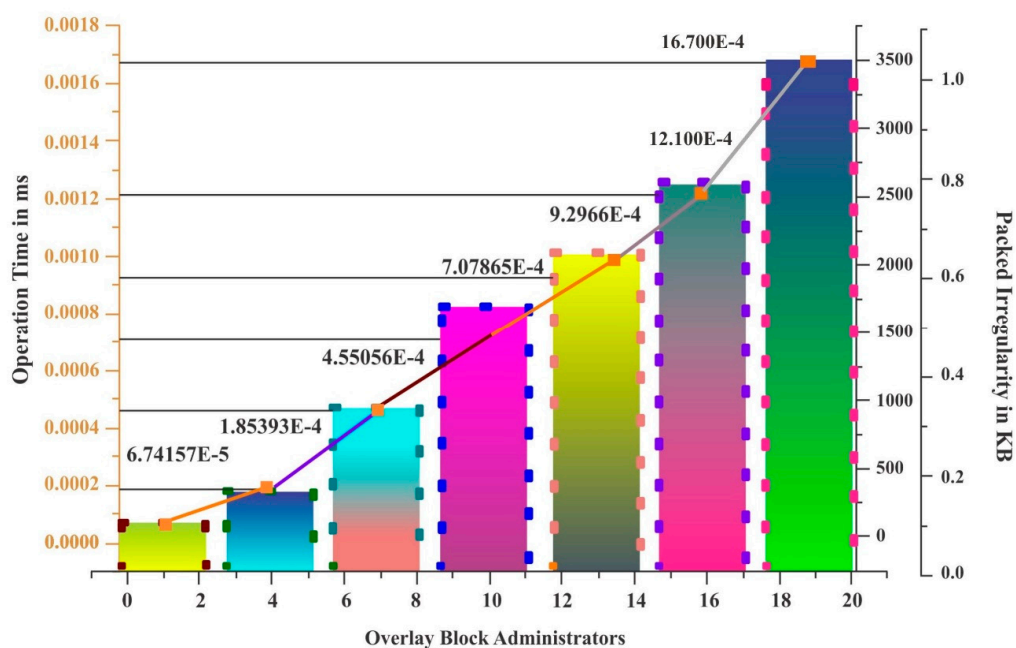


Figure 5. Proposed system simple size extensible blockchain operating time and packet irregularity.

Table 4 and Figure 6 depict the performance of one of the existing systems called baseline packet overhead. Here, the operating time and % of activities checked are given. The operating time is measured in milliseconds, and the activities checked are given as a percentage. Table 4 gives the actual number of overlay block administrators, whereas the graph depicts this as a whole. The OB administrators from 1 to 5, have an operating time of 9.5×10^{-4} ms, and the % of activities checked is -0.0375% . Moreover, the procedure followed is the same for the remaining OB administrators.

Table 4. Existing system baseline packet overhead operating time and % of activities checked.

Baseline Packet Overhead		
Number of OB Administrators	Operation Time in Milliseconds	% of Activities Checked
5.23585	9.5×10^{-4}	−0.0375
14.2925	0.02892	10.7791
23.3491	0.0673	26.1953
32.4057	0.10256	40.7776
41.4623	0.13053	52.0107
50.5189	0.17829	71.1946
59.5755	0.21563	86.1933

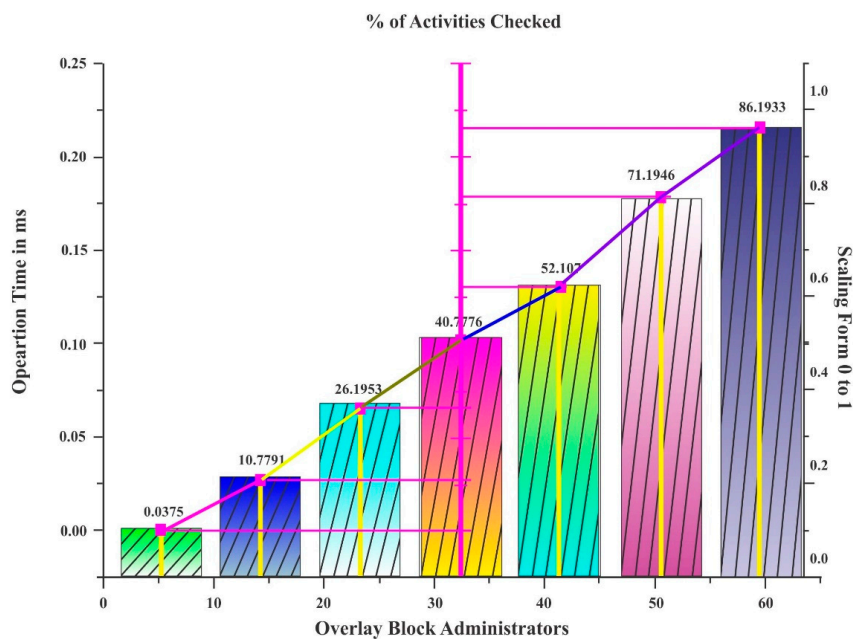
**Figure 6.** Existing system baseline packet overhead blockchain operating time and % of activities checked.

Table 5 and Figure 7 depict the performance of the existing light weight scalable blockchain system. Here, the operating time and % of activities checked are given. The operating time is measured in milliseconds, and the activities checked are given as a percentage. Table 5 gives the actual number of overlay block administrators, whereas the graph depicts this as a whole. The OB administrators from 1 to 5, have an operating time of 90.00102 ms, and the % of activities checked is −0.00987%. Moreover, the procedure followed is the same for the remaining OB administrators.

Table 5. Existing system lightweight scalable blockchain operating time and % of activities checked.

Lightweight Scalable Blockchain		
Number of OB Administrators	Operation Time in Milliseconds	% of Activities Checked
1.27358	0.00102	−0.00987
10.3302	0.01753	6.62061
19.2453	0.03717	14.9267
28.4434	0.06721	26.5782
37.5	0.07122	28.1877
46.6981	0.08356	33.5639
55.7547	0.08757	34.757

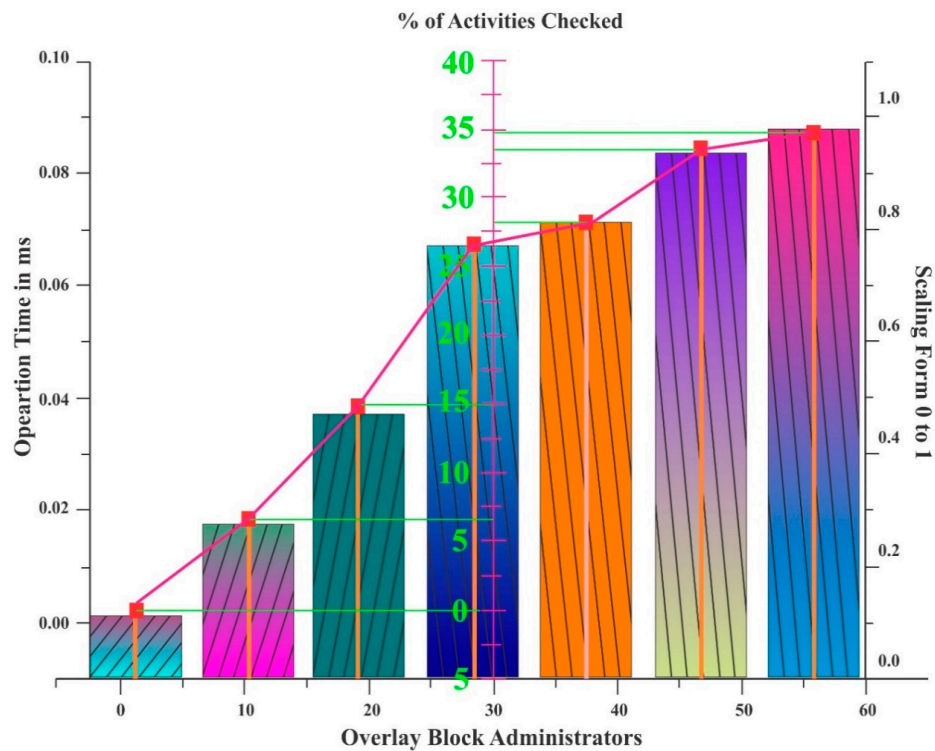


Figure 7. Existing system lightweight scalable blockchain operating time and % of activities checked.

The results shown in Tables 4–6, highlight that the proposed system simple size extensible blockchain performs well when compared to the existing systems such as baseline overhead and lightweight, scalable blockchain with respect to the percentage of activity checked and operating time. It also minimizes the percentage of activity checked as well as the operating time of the blockchain environment. The percentage of activity checked ranges from 0.40855 to 22.2046, which is shown in Table 6 and Figure 8. Meanwhile, the existing baseline overhead system utilizes a percentage of activity checked ranging from -0.0375 to 86.1933 , which is shown in Table 4. The existing lightweight scalable blockchain system utilizes a percentage of activity checked that ranges from -0.00987 to 34.757 , as shown in Table 5.

Table 6. Proposed system simple size extensible blockchain operating time and % of activities checked.

Simple Size Extensible Blockchain		
Number of OB Administrators	Operation Time in Milliseconds	% of Activities Checked
1.12973	0.00102	0.40855
10.1794	0.00714	2.01806
19.2232	0.01849	6.97686
28.2681	0.02879	13.6073
37.4593	0.03491	15.6363
46.4983	0.05044	19.3378
55.68	0.06492	22.2046

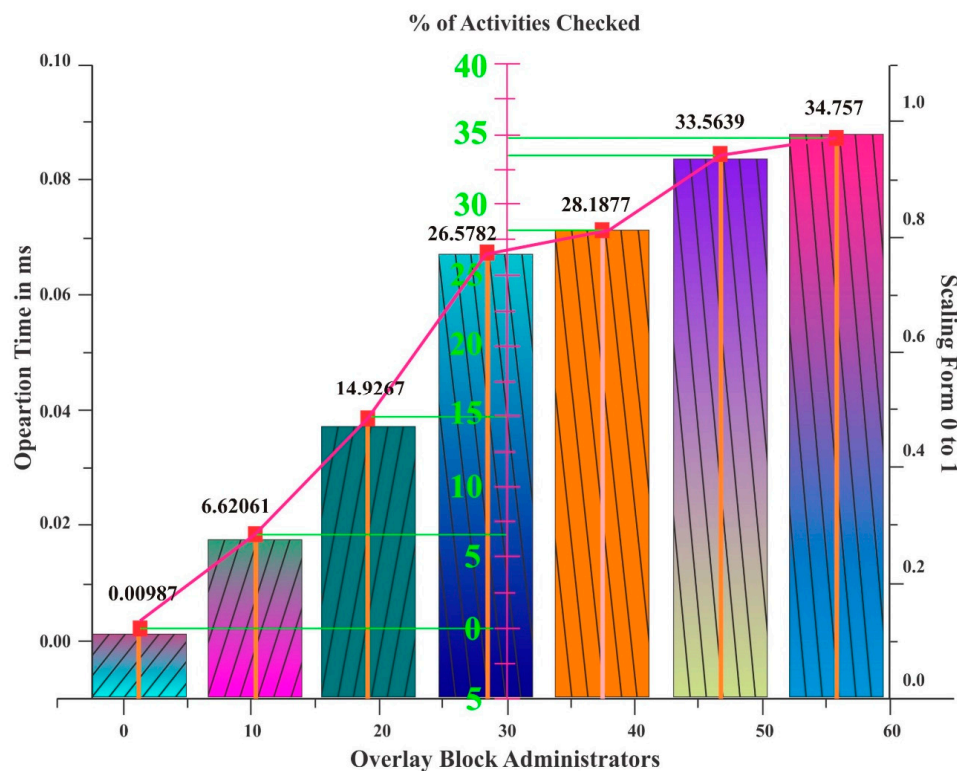


Figure 8. Proposed system simple size extensibility blockchain operating time and % of activities checked.

5. Conclusions

The objective of this research was to enhance the security and handling of the inconspicuousness in the IoT, when combined with blockchain. Many issues are not resolved by the existing systems with respect to the security and scalability in the IoT combined blockchain environment. In this context, this research work proposes a simple size extensible blockchain algorithm to solve the above-mentioned issues. Two algorithms, the shared-time depending agreement algorithm and the shared throughput administrator algorithm are proposed to enhance the efficiency of the simple size extensible blockchain. The work and performance achieved by the proposed algorithm has been detailed and the results show that the proposed system achieves minimum packet overhead, minimum operating time, and better security. It also achieves a minimum percentage of activity checking. In the near future, our work will focus on enhancing the proposed algorithm to provide an efficient communication channel for the blockchain with enhanced security by introducing the concept of exponential evaluation.

Author Contributions: Conceptualization, B.S.B. and P.V.R.; methodology, P.V.R., B.S.B. and S.P.; software, B.S.B. and P.V.R.; validation, B.S.B. and P.V.R.; formal analysis, A.N. and S.P.; investigation, B.S.B. and P.V.R.; resources, P.V.R., A.N. and P.S.; data curation, P.V.R. and B.S.B.; writing—original draft preparation, B.S.B., P.V.R. and A.N.; writing—review and editing, A.N.; visualization, B.S.B. and P.V.R.; supervision, A.N., P.S. and S.P.; project administration, A.N., S.P. and P.S.; funding acquisition, P.S. All authors have read and agreed to the published version of the manuscript.

Funding: The Research received no external funding.

Acknowledgments: Authors like acknowledged the Department of Energy Technology, Aalborg University, Esbjerg 6700, Denmark for technical assistance and expertise shared.

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

References

1. Khan, M.A.; Salah, K. IoT security: Review, Blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [\[CrossRef\]](#)

2. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*; Available online: www.bitcoin.org/en/bitcoin-paper (accessed on 1 January 2020).
3. Yeoh, P. Regulatory issues in blockchain technology. *J. Financ. Regul. Compliance* **2017**, *25*, 196–208. [CrossRef]
4. Vukolić, M. *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. Bft Replication*; Springer: Berlin, Germany, 2015; pp. 112–125.
5. Wei-Fund. 2017. Available online: www.weifund.io (accessed on 1 January 2020).
6. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
7. Gilad, Y.; Hemo, R.; Micali, S.; Vlachos, G.; Zeldovich, N. Algorand. Scaling byzantine agreements for cryptocurrencies. In Proceedings of the 26th Symposium on Operating Systems Principles, Shanghai, China, 28–31 October 2017; ACM: New York, NY, USA, 2017; pp. 51–68.
8. Lu, Z.; Wang, Q. Bars: A blockchain-based anonymous reputation system for trust management in vanets. In Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 98–103.
9. Zhang, Z.-K.; Cho, M.C.Y.; Wang, C.-W.; Hsu, C.-W.; Chen, C.-K.; Shieh, S. IoT security: Ongoing challenges and research opportunities. In Proceedings of the International Conference on Service-Oriented Computing and Applications (SOCA), Matsue, Japan, 17–19 November 2014; pp. 230–234.
10. Nayyar, A.; Vikram, P. Smart Farming: Iot Based Smart Sensors Agriculture Stick for Live Temperature and Moisture Monitoring Using Arduino, Cloud Computing & Solar Technology. In *Communication and Computing Systems, Proceedings of the International Conference on Communication and Computing Systems, ICCCS, Gurgaon, India, 9–11 September 2016*; CRC Press: Boca Raton, FL, USA, 2016; pp. 673–680.
11. Vora, J.; Nayyar, A.; Tanwar, S.; Tyagi, S.; Kumar, N.; Obaidat, M.S.; Rodrigues, J.J. BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.
12. Tal Yellin, Dominic Aratari, Jose Pagliery. 2009. Available online: www.https://money.cnn.com/infographic/technology/what-is-bitcoin/index.html (accessed on 1 January 2020).
13. Deep, G.; Mohana, R.; Nayyar, A.; Sanjeevikumar, P.; Hossain, E. Authentication Protocol for Cloud Databases Using Blockchain Mechanism. *Sensors* **2019**, *19*, 4444. [CrossRef] [PubMed]
14. Mazieres, D. The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus. *Stellar Dev. Found.* **2015**, *32*, 1–45.
15. Saberi, S.; Kouhizadeh, M.; Sarkis, J.; Shen, L. Blockchain technology and its relationships to sustainable supply chain management. *Int. J. Prod. Res.* **2019**, *57*, 2117–2135. [CrossRef]
16. Astarita, V.; Giofrè, V.P.; Mirabelli, G.; Solina, V. A Review of Blockchain-Based Systems in Transportation. *Information* **2020**, *11*, 21. [CrossRef]
17. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and IoT Integration: A Systematic Survey. *Sensors* **2018**, *18*, 2575. [CrossRef] [PubMed]
18. Cachin, C. Architecture of the Hyperledger blockchain fabric. In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*; IBM Research: Zurich, Switzerland, 2016.
19. Liu, J.; Xiao, Y.; Chen, C.L.P. Authentication and access control in the internet of things. In Proceedings of the 32nd International Conference on Distributed Computing Systems Workshops, Macau, China, 18–21 June 2012; pp. 588–592.
20. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 2084–2123. [CrossRef]
21. Eth-Twitter. 2017. Available online: [www.github.com/yep/eth-tweet](https://github.com/yep/eth-tweet) (accessed on 1 January 2020).
22. Fullprofile. 2017. Available online: www.fullprofile.com.au (accessed on 1 January 2020).
23. Kowsigan, M.; Balasubramanie, P. A novel resource clustering model to develop an efficient wireless personal cloud environment. *Turk. J. Electr. Eng. Comput. Sci.* **2018**, *27*, 2156–2169. [CrossRef]
24. Hashemi, S.H.; Faghri, F.; Rausch, P.; Campbell, R.H. World of empowered IoT users. In Proceedings of the IEEE First International Conference on Internet-of-Things Design and Implementation, Berlin, Germany, 4–8 April 2016; pp. 13–14.
25. Popov, S. *The Tangle*; 2016; Available online: https://assets.ctfassets.net/r1dr6vzfxfhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf (accessed on 1 January 2020).

26. Aitzhan, N.Z.; Svetinovic, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 840–852. [CrossRef]
27. Graph Coin. 2019. Available online: <https://graphcoin.net/graphcoinwhitepaper.pdf> (accessed on 1 January 2020).
28. Tomescu, S.D. Catena: Efficient non-equivocation via Bitcoin. In Proceedings of the 38th IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017; pp. 393–409.
29. Dorri, S.S.; Kanhere, R. Jurdak. MOF-BC: A memory optimized and flexible blockchain for large scale networks. *Future Gener. Comput. Syst.* **2019**, *92*, 357–373. [CrossRef]
30. de Angelis, S.; Aniello, L.; Baldoni, R.; Lombardi, F.; Margheri, A.; Sassone, V. PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain. In Proceedings of the Italian Conference on Cyber Security, Milan, Italy, 6–8 February 2018.
31. Baliga, A. Understanding Blockchain Consensus Models. *Persistent* **2017**, *4*, 1–14.
32. Cooper, D. Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile. *RFC* **2018**, *5280*, 1–151.
33. Sahraoui, S.; Bilami, A. Compressed and distributed host identity protocol for end-to-end. In Proceedings of the International Conference on Next Generation Networks and Services (NGNS), Casablanca, Morocco, 28–30 May 2014; pp. 295–301.
34. Kousaridas, S.; Falangitis, P.; Magdalinos, N.; Alonistioti, M. SYSTAS: Density-based algorithm for clusters discovery in wireless networks. In Proceedings of the IEEE 26th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Hongkong, China, 30 August–2 September 2015; pp. 2126–2131.
35. Kosba, A.; Miller, A.; Shi, E.; Wen, Z.; Papamanthou, C. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017; pp. 839–858.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).