International Journal of Applied Engineering Research ISSN 0973-4562 Volume 15, Number 4 (2020) pp. 377-384
© Research India Publications. http://www.ripublication.com

Secure IoT Based on Blockchain: Quantitive Evaluation and Analysis of the Correlation Between Block Mining Time and Blockchain Efficiency

Fatimah Hussain Al-Naji[1], Rachid Zagrouba[2]

Department of Computer Science[1], Department of Computer Information Systems[2],
College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University,
P.O. Box 1982, Dammam 31441, Saudi Arabia.

Abstract

This research study aims to quantitively analyze the correlation between block mining time and blockchain efficiency with the integrity and scalability aspects under different parameters. The results showed that, hash difficulty value has strongest positive relationship with block mining time, while the data length has weakest positive correlation. Also, this study shows that, block mining time has correlation with the data length, number of blocks, and hash difficulty, while its efficiency corollate only with the hash difficulty.

Keywords: Blockchain, Internet of Things, Security, Integrity, Consensus Mechanism.

I. INTRODUCTION

Recently, many companies are looking to integrate IoT applications with their business to achieve higher efficiency and lower cost. On the other hand, because of connecting to the Internet, unauthorized data tampering, threaten data privacy, or even denial of service may be much easier [2]. Subsequently, security and privacy are the main key challenges determine the success or failure of IoT applications.

Blockchain (BC) technology has the potential to deliver innovative solution to tackle privacy and security challenges in IoT. BC provides a high level of security from consensus mechanism known as Proof of Work (PoW) which is used in the process of appending new block to the BC. In term of privacy, it is mainly come from using changeable Public Key (PK) to identify user's identity and ensuring data integrity [3].

The main contribution of this paper is quantitively analyze the correlation between block mining time and blockchain efficiency with the integrity and scalability aspects under different parameters.

The rest of the paper is organized as follows: section II reviews the theoretical background of the blockchain technology and IoT. The literature review appears next in section III. Research methodology appear next, followed by data analysis and results evaluation. Comparison between block mining time and blockchain efficiency regarding the affected parameters represented on results discussion section. This paper concludes with the research conclusion and future works.

II. BACKGROUND

A. Blockchain

In recent decades, cryptocurrency technology has attracted the attention of both researchers and industries. Bitcoin was the first digital currency, proposed in 2008 and implemented in 2009 based on blockchain mechanism [4].

Blockchain powering the next generation of the database. It also called Distributed Ledger Technology (DLT). It is a distributed database which shifts the power authority of its data away from one central node and make it available in a network of peer-to-peer participants without intermediaries. Each node contains entire copy of the blockchain. Blockchain regarded as a public ledger which hold all committed transactions in a chain of blocks which is continuously grows by appending new block to the chin [5].

1) Blockchain Architecture

Blockchain is a sequence of blocks connected with each other. The basic structure of each block contains the following fields [1]:

- *Block Number field:* first block called Gensis block.
- *Nonce field:* an arbitrary number used by the miners in calculating block hash value.
- *Data field:* contains the transaction ledger.
- *Previous Block Hash field:* a pointer to the previous block. In case of Gensis block, the value of this field will be zero.
- *Current Block Hash field:* as shown in figure 1, all the fields passed to the cryptographic hash function which gives the hash of the current block and used it as the previous hash of the next block. The main encryption algorithm used to calculate the hash value is SHA-256.

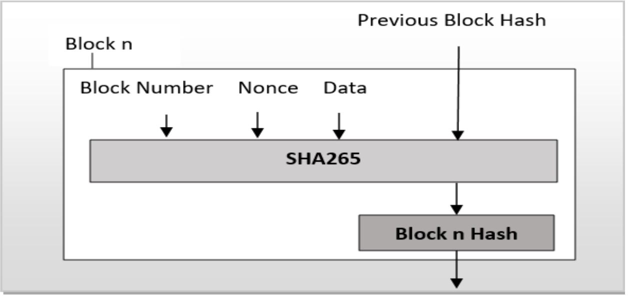

Fig. 1. Hashing of Block

2) Blockchain Process

Consensus mechanism is crucial in adding new block to the blockchain to make the distributed copies alignment and make sure all nodes that maintain the blockchain are synchronized with each other. Proof of Work (PoW) is the first mechanism to reach blockchain consensus [5]. When a new transaction occurs, all nodes in the network will receive it as a pending transaction. Any node can be a miner which is responsible for mining new block and appending it to the end of the blockchain. Miners will expend their resources and compete to:

a) *Validate the transaction:* each transaction signed by the private key of the sender, and the public key of the sender used to validate the signature contained within the transaction.

b) *Search for the key that will solve the cryptographic puzzle:* each network set a target value known as difficulty value to regulate how quickly blocks are solved. Miners will hash basic block fields, if the first nonce value does not achieve a value less than the difficulty, it will be increment and perform another hash until find a valid hash that become the next block.

The first miner does that, will add the transaction to its chain and share it to all distributed nodes in the network at the same time.

3) Blockchain Applications

Blockchain technology is capable to be used in a wide range area. The most widely used applications are the following:

a) *Bitcoin:* is a digital currency and online payment system based on blockchain technology. Money transfer can be achieved immediately without relying on third trusted parity [6].

b) *Ethereum:* is a blockchain platform handles smart contract. It is a tiny computer program containing a set of rules to facilities, verifies, and enforces the performance of transactions [7].

c) *Hyperledger:* is an open source blockchain platform by Linux foundation to create a standard distributes ledger which will facilitate building more applications on blockchain technology [8].

d) *Other Applications:* there are many use cases of blockchain technology such as, government voting, IOT, insurance, international payment, prediction market, traceability in supply chain, and patient's privacy in medical treatments [9,10].

4) Taxonomy of Blockchain Systems

Blockchain technologies can be roughly classified into three main categories which are [11]:

a) *Public Blockchain:* any node can join blockchain network and participate mining process and accessing data without any permission. The typical representative of public blockchain are Bitcoin and Ethereum

b) *Consortium Blockchain:* selected nodes can be chosen in advance and give them the authority. Blockchain data can be either public or private. The typical representative of consortium are Hyperledger and R3CEV.

c) *Private Blockchain:* there is a restricted authority on blockchain network and not every node can participate mining process and accessing data. The typical representative of private blockchain are MONAX and Multichain [12].

5) Blockchain Characteristics

a) *Immutability:* during block mining process, immutability achieved via POW mechanism to prevent unauthorized data tampering and improve system integrity [13].

b) *Decentralization:* overcomes many-to-one traffic delay and single point of failure problems which leads to complete transactions faster and more efficiently. All nodes participate with their resources to ensure system scalability, robustness and avilability [13].

c) *Transparency and Openness:* blockchain data kept transparent and open to all network participants hold the same copy, which create greater trust between them. Conversely it may harm users' privacy since blockchain content open to all nodes on the network [14].

d) *Traceability:* historical transaction data help to improve tracing transaction back to its origin and verify its authenticity [14].

B. Internet of Things

Internet of Things technology proposed by Kevin Ashton in 1999. It is an evolution of Internet technology which makes countless of devices connected and communicate with each other with minimal human intervention. This type of connectivity is not limiting to connected laptops, tablets and smartphones, it is going towards connected cars, smart homes, wearables, smart cities, industries and healthcare.

Due to the advancement communication among IoT devices, Wireless Sensor Networks (WSN), Radio Frequency Identification (RFID), and cloud computing technologies took a key role [15]. According to Gartner, "the Internet of Things will cover 26 billion objects by 2020" [16]. While the number of connected devices increase exponentially, the difficulty of controlling data security increases accordingly which presents a significant challenge to the IoT.

1) IoT Architecture and Characteristics

As shown in figure 2. The basic architecture of Internet of Things represents its characteristics. The architecture consists of three main layers which are the following [17]:

a) *Physical Layer:* also called perception layer. Represent the perception characteristic of the IoT, where the main task of this layer is to perceive the physical properties of the objects through sensing technologies (e.g. RFID).

This process will convert the information to digital signals to be more convenient for network transmission.

b) *Network Layer:* represent reliable transmission characteristic of the IoT, where the main task of this layer is to transfer massive amount of data received from the physical layer to the application layer through various network media such as, wireless and wired networks include 3G / 4G, Wifi, Bluetooth, Zigbee,infrared technology, and so on. This layer depends on cloud computing as a primary technology to analyse and process the huge amount of data, which represent the intelligent processing characteristic of the IoT.

c) *Application Layer:* this layer constitutes the front end of IoT framework. It provides IoT applications which use the processed data which is received from network layer.

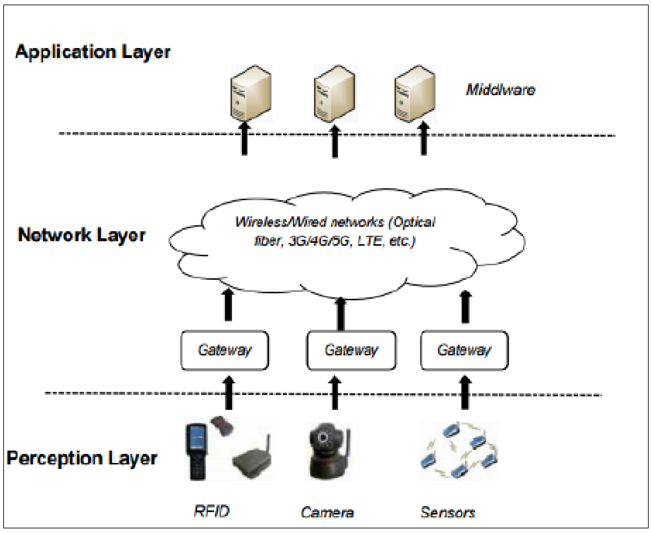

Fig. 2. Internet of Things Architecture [18]

2) *IoT Security Requirements*

IoT security requirements are the following [18]:

a) *Availability:* as the dependence on IoT services increased, it is necessary to deliver highly available data all the time for the authorized user.

b) *Privacy:* wherever the data transmitted across the IoT network, it is necessary to be processed securely and accessed only by the authorized user.

c) *Integrity:* it is important to secure IoT data from unauthorized modification.

d) *Authentication and Authorization:* confirms the identity of the user and determine the access levels.

e) *Scalability:* when the number of transactions grows, the blockchain increases in size, and it becomes expensive to store it, especially for IoT devices with limited resources.

III. LITERATURE REVIEW

This research paper is mainly about securing IoT based on Blockchain technology aiming to analyze the correlation between block mining time efficiency with the integrity and scalability aspects under different parameters.

As a first step of this research, literature review was conducted to have an evidence of the level of scalability, and integrity of the blockchain. Accordingly, the following questions are formulated [25]:

- What are the use cases of the blockchain beyond cryptocurrencies?
- Are there any use cases applicable to the IoT?
- What are the implementation differences with respect to the Bitcoin blockchain and which mining techniques are used?
- What is the degree of integrity, scalability and anonymity of the blockchain?

A. Literatures Comparison and Analysis

The results of the questions from the analyzed papers are organized sequentially.

The author in [19] shows that, blockchain can be used in managing access policies and protecting users' personal data. Similarly, the authors in [20,21] used blockchain in managing data storage contracts. In rating system cases, the author in [22] found that, blockchain is capable to be used for tracking users points in social voting system, and the author in [23] implement rating system based on blockchain, where customers can give feedbacks about the purchases.

The study in [24] shows that, some cases are applicable to the context of IoT. As shown in [25, 26] studies, blockchain used for managing public keys update, registration and revocation, where each device is identified by a public key to interact with other devices through the blockchain. Moreover, in trading of goods and data field, blockchain could be used for trading data collected by sensors of IoT devices and other goods [27,28].

Table 1 summarize the use cases of the Blockchain beyond cryptocurrencies and applicability to use it in IoT. However, there are several researches implemented blockchain technology in a way differs from the ones of the Bitcoin, and they are less computationally expensive compared with it [24]. Table 2 compares between the mining techniques according to the way of chosen the miner.

Integrity, scalability, and anonymity are three major challenges in blockchain technology in general and in IoT cases in specific. Blockchain is vulnerable to some attacks which could threaten the integrity. As shown in [29] study, selfish miner does not follow the normal process of creating a block. Instead, it maintains its track privately and decides not to publish the blocks it finds until the public one approaches its length. Then, it publishes its own private branch, which could become the longest one and could be accepted also by honest miners. So, after some time, the public branch and the data contained in it would be discarded. In [30] study, the authors show that, an attacker could delay delivery of blocks to other nodes in network. This could cause denial of service, because, if the attacker controls several nodes, it can prevent dissemination of information. Table 3 compares the de-anonymization techniques and the way of causing anonymity risks.

Table 1. Blockchain Use Cases and Applicability to IoT

Category	Blockchain Usage	Applicability to the IoT
Data Storage Management	• Managing access policies • Protecting users' personal data	✓
Rating Systems	• Tracking users points in social voting system • Feedbacks about the purchases	✗
Trade of Goods and Data	Trading data collected by sensors	✓

Table 2. Mining Techniques

Mining Technique	Miner Selection Method
Proof of Stake Velocity (PoSV)	Depending on the coin age
Proof of Space (PoSpace)	Depending on the amount of space

Table 3. De-anonymization Techniques

De-anonymization Technique	Anonymity Risk
Multiple Addresses Inputs	When a transaction issued with multiple addresses as inputs all the input addresses belong to the same issuer user [35], [37], [39]
Associations with IP	Through analyzing network traffic, it is possible to associate Bitcoin addresses with IP addresses [35], [39].
Usage of Centralized Services	Usage of centralized services allows keeping track of associations between the addresses of the same user [36], [37].

There are several causes of scalability issues shown on the analyzed papers which are the following:

- The huge number of transactions and sensors data permanently stored on every node [37].
- Computations and data storage done by each node of the network [38].
- Every node of the blockchain should verify each block and transaction [39].

B. Literatures Results Discussion

Blockchain Use Cases and IoT: Blockchain technology was developed in 2008 by Satoshi Nakamoto, It was originally for the Bitcoin cryptocurrency [39]. Subsequently, it has been used in several cases beyond cryptocurrency such as, data storage management, rating system, trade of goods and data, identity management, and more. The IoT is applicable to conduct Blockchain technology in data management field, where each device is identified by a public key to interact with other devices through the blockchain. Also, blockchain is used for trading data collected by sensors of IoT devices.

Table 4. De-anonymization Techniques

De-anonymization Technique	Anonymity Risk
Multiple Addresses Inputs	When a transaction issued with multiple addresses as inputs all the input addresses belong to the same issuer user [35], [37], [39]
Associations with IP	Through analyzing network traffic, it is possible to associate Bitcoin addresses with IP addresses [35], [39].
Usage of Centralized Services	Usage of centralized services allows keeping track of associations between the addresses of the same user [36], [37].

Blockchain Implementation Differences: since the PoW requires very high computational power, IoT devices with limited capabilities would not be able to mine new blocks and add it to the blockchain. As shown from the analyzed papers, there are alternative techniques to PoW with less computational expensive which are the following:

- Proof of Stake Velocity (PoSV) technique, where the miner is chosen depending on its coin age.
- Proof of Space (PoSpace) mining technique, where the miner is chosen according to the amount of space.

Blockchain Challenges:

Misbehaving miners which hold high computational power, could cause integrity risks in a way of losing past data and holding invalid transactions. The study in [24], argue that, high difficulty of the PoW and the large number of honest miners ensure the integrity of the blockchain, but it limits blockchain scalability. The author in [37], proposed an architecture to solve both challenges at the same time. The solution separates the blockchain from application layer, where low performance IoT devices are not required to compute the PoW.

Furthermore, total user anonymity does not be guaranteed through pseudonymization, because it is possible to de-anonymize a user by analyzing the blockchain since it is public or by analyzing network traffic. Authors in [10, 38, 42], proposed mixing protocols as a solution for anonymity challenge, where two different addresses used by a user, one for sending the coins and the second one to receive them back making it difficult to discover the correspondence between input and output addresses of the same user.

IV. RESEARCH METHODOLOGY

A. Research Design

This study is an applied research. The investigation nature of it is quantitative. This study simulates Blockchain as a web-based system using HTML and Jade languages, the algorithm of the hash is SHA-256.

B. Measuring Method

Pearson's Correlation Coefficient analysis method is used to measure the strength of the association and the direction of the relationship between block mining time and two main parameters which are the data length, and hash difficulty. The result value of the correlation coefficient is ranging from (+1) and (-1). As the value goes toward 0, the association between two constructs will be weaker. The sign of the result value indicates the direction of the relationship; where the positive sign indicates a positive direction and the negative sign indicates a negative direction.

C. Evaluation

Evaluate the end results under the following aspects:

1) *Integrity:* To evaluate the integrity, block mining time is analysed in re-mining the whole blockchain after tampering data lengths as the following:

- Efficiency = re-mining time (s) / data lengths
- Efficiency = re-mining time (s) / blocks number

2) *Scalability:* The scalability is the ability of dealing with the high-density work. In this study, the work pressure is from increasing data length and blocks number as the following:

- Efficiency = mining time (s) / data lengths
- Efficiency = mining time (s) / blocks number

3) *Efficiency:*

Blockchain efficiency is the quality of being able to mine blocks successfully, without wasting time. It is the ratio between the amount of time a block needs to be mined, and the hash difficulties that it will calculates.

V. DATA ANALYSIS AND RESULTS

Block mining time is measured under different parameters values within one block, one blockchain, and within distributed blockchain.

A. Statistical Analysis of One Block

To find the correlation between mining time and difficulty, three measurements were conducted under different data lengths. As shown from the result of correlation analysis in figure 3, mining time rises exponentially with the increase of difficulty. Accordingly, there is very strong positive relationship between difficulty and mining time.

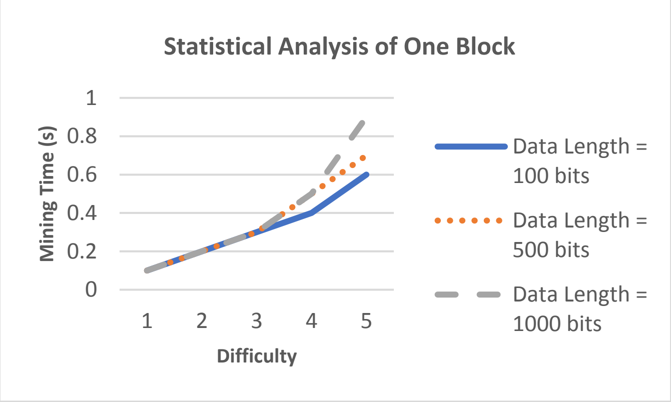

Fig. 3. Mining Time and Difficulty Under Different Data Lengths of one Block

To find the correlation between mining time and data length, three measurements were conducted under different difficulties. As shown from the result of correlation analysis in figure 4, there is strong positive relationship between data length and mining time.

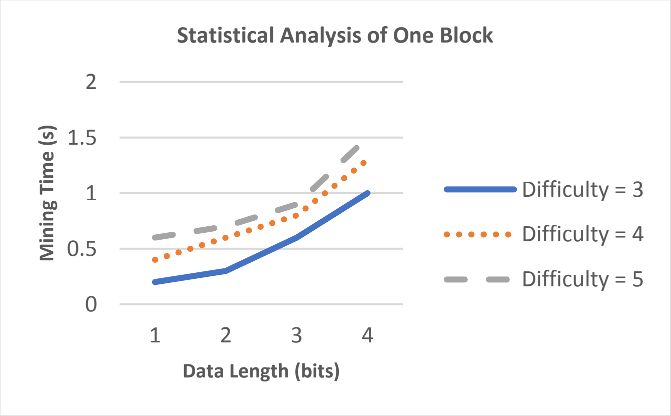

Fig. 4. Mining Time and Data Length Under Different Difficulties of one Block

B. Statistical Analysis of One Blockchain

To find the correlation between mining time and difficulty, three measurements were conducted under different data lengths. As shown from the result of correlation analysis in figure 5, mining time rises exponentially with the increase of difficulty. Accordingly, there is very strong positive relationship between difficulty and mining time.

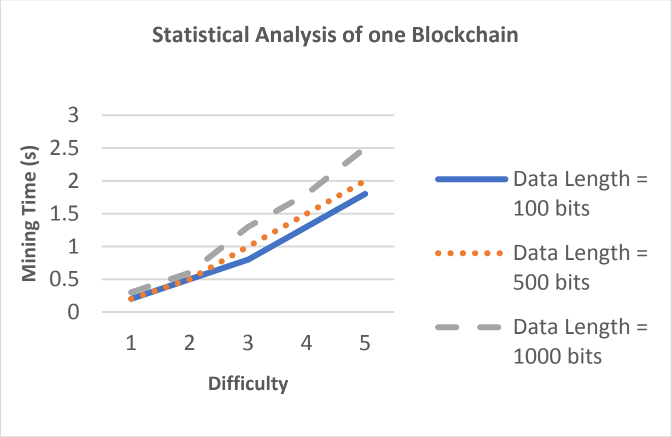

Fig. 5. Mining Time and Difficulty Under Different Data Lengths of one Blockchain

To find the correlation between mining time and data length, three measurements were conducted under different difficulties. As shown from the result of correlation analysis in figure 6, there is strong positive relationship between data length and mining time.

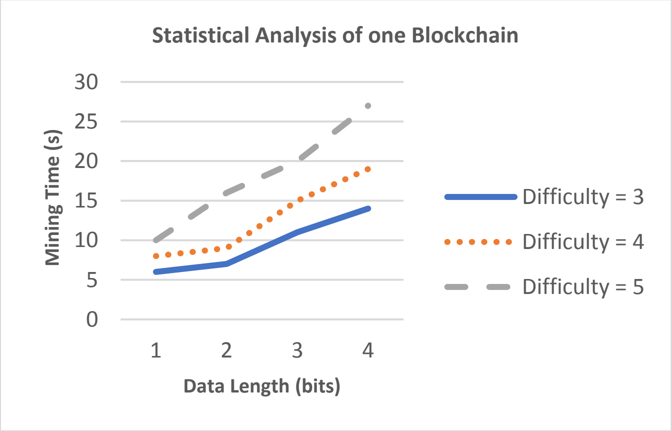

Fig. 6. Mining Time and Data Length Under Different Difficulties of one Blockchain

C. Statistical Analysis of Distributed System

To find the correlation between mining time and difficulty, three measurements were conducted under different data lengths. As shown from the result of correlation analysis in figure 7, mining time rises exponentially with the increase of difficulty. Accordingly, there is very strong positive relationship between difficulty and mining time.

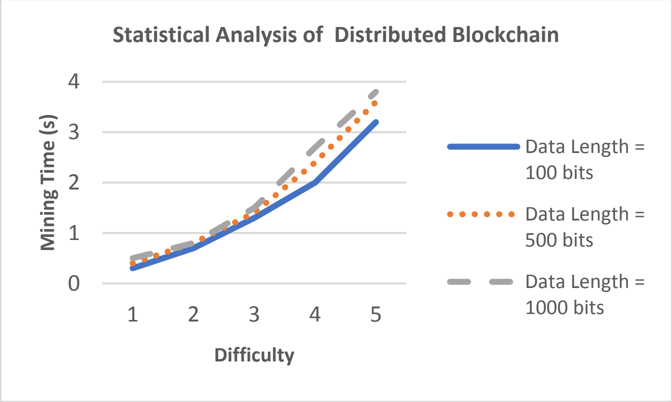

Fig. 7. Mining Time and Difficulty Under Different Data Lengths of Distributed Blockchain

To find the correlation between mining time and data length, three measurements were conducted under different difficulties. As shown from the result of correlation analysis in figure 8, there is strong positive relationship between data length and mining time.

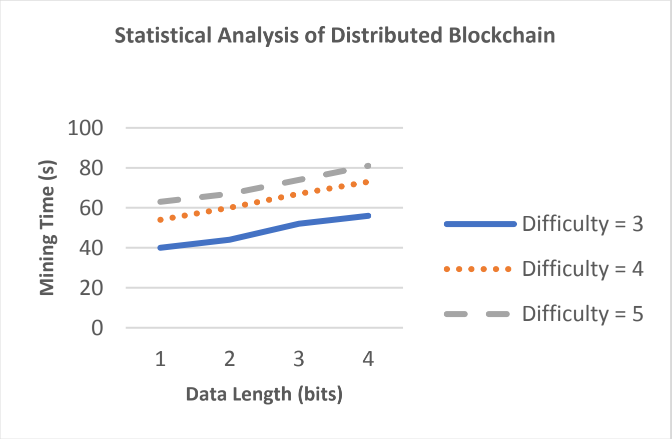

Fig. 8. Mining Time and Data Length Under Different Difficulties of Distributed Blockchain

VI. RESULTS DISCUSSION

This research study aims to quantitively analyze the correlation between block mining efficiency with the integrity and scalability aspects under different parameters.

From the results of measurements:

- The efficiency of block mining is directly related to the hash difficulty. As the difficulty increased, the efficiency increased accordingly.
- By increasing scaling, the data length, the speed of block mining becomes lower.
- The re-mining efficiency is higher than the normal mining efficiency.

Generally, the statistical analysis results show that, hash difficulty value has the highest correlation with block mining time, while the data length has the lowest correlation. The following table gives a conclusion about whether a parameter has correlation with efficiency and block mining time or not.

Table 5. Block Mining Time and Blockchain Efficiency

Parameter	Blockchain Efficiency	Block Mining Time
Data Length	×	✓
Number of Blocks	×	✓
Difficulty	✓	✓

VII. CONCLUSION AND FUTURE WORK

In conclusion, the main emphasis of this paper is to highlight major security challenges of IoT particularly the scalability and integrity, focusing on quantitatively analyze how they corollate with block mining efficiency. This study measures the strength of the association between block mining time and two main parameters namely data length, and difficulty. The findings show that, hash difficulty value has the highest correlation with block mining time, while the data length has the lowest correlation. Also, this study shows that, block mining time has correlation with the data length, number of blocks, and hash difficulty, while its efficiency corollate only with the hash difficulty. Further studies could be analyzing the correlation between block mining efficiency with the integrity and scalability aspects under sensors number parameter.

REFERENCES

[1] Karimi, K., & Atkinson, G. (2013).*What the Internet of Things (IoT)* Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2017). FairAccess: a new Blockchain-based access control framework for the Internet of Things. doi: 0.1002/sec.1748

[2] Dorri, A., Kanhere, S. S., & Jurdak, R. (2017, April). Towards an optimized blockchain for IoT. In *Proceedings of the second international conference on Internet-of-Things design and implementation* (pp. 173-178). ACM.

[3] "State of Blockchain Blockchain Funding Overtakes Bitcoin – CoinDesk" (2019). Retrieved from http://www.coindesk.com/state-of-blockchain-q1-2016/

[4] Zheng, Z., Xie, S., Dai, H. N., & Wang, H. (2016). Blockchain challenges and opportunities: A survey. *Work Pap.–2016*.

[5] Lin, I. C., & Liao, T. C. (2017). A Survey of Blockchain Security Issues and Challenges. *IJ Network Security*, *19*(5), 653-659.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[6] Bahga, A., & Madisetti, V. K. (2016). Blockchain platform for industrial internet of things. *Journal of Software Engineering and Applications*, *9*(10), 533.

[7] Cachin, C. (2016, July). Architecture of the hyperledger blockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers* (Vol. 310).

[8] Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016, October). A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 17-30). ACM.

[9] Tsai, W. T., Blower, R., Zhu, Y., & Yu, L. (2016, March). A system view of financial blockchains. In *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*(pp. 450-457). IEEE.

[10] Lin, I. C., & Liao, T. C. (2017). A Survey of Blockchain Security Issues and Challenges. *IJ Network Security*, *19*(5), 653-659.

[11] Blockchains & Distributed Ledger Technologies. (2019). Retrieved from https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

[12] Decker, C., Seidel, J., & Wattenhofer, R. (2016, January). Bitcoin meets strong consistency. In *Proceedings of the 17th International Conference on Distributed Computing and Networking* (p. 13). ACM.

[13] Hooper, M., & Hooper, M. (2019). Top five blockchain benefits transforming your industry - Blockchain Pulse: IBM Blockchain Blog. Retrieved from https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/

[14] HP News - HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. (2019). Retrieved from https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676

[15] Abdmeziem, M. R., Tandjaoui, D., & Romdhani, I. (2016). Architecting the internet of things: state of the art. In *Robots and Sensor Clouds* (pp. 55-75). Springer, Cham.

[16] Romdhani, Imed & Abdmeziem, Riad & Tandjaoui, D. (2015). Architecting the Internet of Things: State of the Art.

[17] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[18] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," (2015). IEEE Symposium on Security and Privacy Workshops. IEEE Computer Society, pp. 180–184.

[19] D. Vorick and L. Champine, "Sia: Simple Decentralized Storage,"2014. [Online]. Available: https://sia.tech/assets/globals/sia.pdf

[20] C. Bocovich, J. A. Doucette, and I. Goldberg, "Lavinia: An auditpayment protocol for censorship-resistant

storage." (2017). In Financial Cryptography and Data Security.

[21] D. Vandervort, "Challenges and Opportunities Associated with a Bitcoin-Based Transaction Rating System," (2014). Financial Cryptography Workshops, ser. Lecture Notes in Computer Science, vol. 8438. Springer, pp. 33–42.

[22] Conosq`zzza 4centi, M., Vetro, A., & De Martin, J. C. (2016, November). Blockchain for the Internet of Things: A systematic literature review. In *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*(pp. 1-6). IEEE.

[23] L. Axon, "Privacy-awareness in Blockchain-based PKI," 2015. [Online]. Available: http://goo.gl/3Nv2oK

[24] C. Fromknecth, D. Velicanu, and S. Yakoubov, "CertCoin: A NameCoin Based Decentralized Authentication System,"2014. [Online]. Available: https://courses.csail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov-certcoin.pdf

[25] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," (2015). ICIN. IEEE, pp. 184–191.

[26] I. Eyal and E. G. Sirer, "Majority is not Enough: Bitcoin Mining is Vulnerable," (2013). CoRR, vol. abs/1311.0243.

[27] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun, "Tampering with the Delivery of Blocks and Transactions in Bitcoin," (2015). ACM Conference on Computer and Communications Security. ACM, pp. 692–705.

[28] D. W¨orner and T. von Bomhard, "When your sensor earns money: exchanging data for cash with Bitcoin," (2014). UbiComp Adjunct.ACM, pp. 295–298.

[29] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: Decentralized Computation Platform with Guaranteed Privacy," (Jun. 2015). [Online]. Available: http://enigma.media.mit.edu/enigma full.pdf

[30] S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to Better – How to Make Bitcoin a Better Currency,"(2012). Springer, vol. 7397, pp. 399–414.

[31] M. Spagnuolo, F. Maggi, and S. Zanero, "BitIodine: Extracting Intelligence from the Bitcoin Network," (2015). Financial Cryptography, ser.

Lecture Notes in Computer Science, vol. 8437. Springer, 2014, pp.457 468.

[32] J. Herrera-Joancomart´ı, "Research and Challenges on Bitcoin Anonymity"in DPM/SETOP/QASA, ser. Lecture Notes in Computer Science,vol. 8872. Springer, 2014, pp. 3–16.

[33] M. Moser, R. Bohme, and D. Breuker, "An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem." (2017). Available: https://maltemoeser.de/paper/money-laundering.pdf

[34] S. Feld, M. Sch¨onfeld, and M. Werner, "Analyzing the Deployment of

Bitcoin's P2P Network under an AS-level Perspective" (2014) Procedia Computer Science, vol. 32. Elsevier, pp. 1121–1126.

[35] P. Koshy, D. Koshy, and P. McDaniel, "An Analysis of Anonymity in Bitcoin Using P2P Network Traffic" (2014). Financial Cryptography, ser. Lecture Notes in Computer Science, vol. 8437. Springer, pp.469–485.

[36] L. Valenta and B. Rowan, "Blindcoin: Blinded, Accountable Mixes for Bitcoin," (2015). Financial Cryptography Workshops, ser. Lecture Notes in Computer Science, vol. 8976. Springer, pp. 112–126.

[37] J. Herbert and A. Litchfield, "A Novel Method for Decentralised Peerto-Peer Software License Validation Using Cryptocurrency Blockchain Technology" (2015). CRPIT, vol. 159. Australian Computer Society , pp. 27–35.

[38] J. Herrera-Joancomart´ı, "Research and Challenges on Bitcoin Anonymity,"(2014). Lecture Notes in Computer Science,vol. 8872. Springer, pp. 3–16.

[39] E. Heilman, "One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner" (2014). IACR Cryptology ePrint Archive, vol. 2014, p. 7.