Blockchain Applicability for Security and Privacy of IoT

Akihisa Nishikawa
18210393
School of Computing, Security and Forensics

Dublin City University
MCM Practicum
akihisa.nishikawa2@mail.dcu.ie

Supervisor
Renaat Verbruggen
4673 words
09/08/2019

***Abstract*—Blockchain is the latest technology that is used to record data across many nodes. It was an invention alongside Bitcoin and the recognition for its importance has rapidly grown over the past decade. Blockchain structure is yet to be fully utilized in practices other than cryptocurrency. Especially in IoT however, the potential impact is incalculable. The objective of this paper is to, first, explain blockchain structure in detail as it refers to the cryptocurrency system. Then it will address current Blockchain security and privacy concerns as well as other drawbacks. Finally, this paper will assess the overall applicability of Blockchain for IoT with collected data. The main objective of this paper is to assess the possibility of the use of blockchain with proof of work in IoT and give a comprehensive discussion with regards to security and privacy issues. (*Abstract*)**

Keywords—IoT, ledger, Internet of things, security, privacy, blockchain, proof of work (*key words****)***

I. INTRODUCTION

Cryptocurrency has quickly gained popularity over a decade and it is the primary service associated with blockchain. Since the Bitcoin cash system was published by Satoshi Nakamoto in 2008, the blockchain was revived and was attracted the world's attention to its new technology. [1] Nakamoto is believed to be the person who invented it, although the name is just used as an alias. It is unknown if he or she developed Bitcoin by themselves or worked as a group. Blockchain has a tremendous role of securing the integrity of blockchain transactions. Although it was an invention alongside the Bitcoin, the structure of blockchain was more and more highlighted as cryptocurrencies became well-known.

Blockchain is a chained list of blocks that contain transactions in Bitcoin. It acts as a public database or record that grows as the block appends to the chain. Each block contains an average of more than 1900 transactions under Bitcoin consensus. Each block is linked to the one block before by using a cryptographic hash function. This will be explained in more details in the Mining Section. The important point here is the steps of generating digest that meets requirement needs high computational power. [2]

With regards to usage of blockchain, it can be applied to IoT situations. In Bitcoin, transactions are stored inside of the block. However, they can be replaced by any data or program. [3] It also provides a distributed system within the network. Blockchain has a huge potential not only in IoT but also in other areas such as insurance, supply chain, or music. [4] In this paper, this paper will examine traditional blockchain with proof of work (PoW) and assess suitability in terms of security and privacy issues. Although blockchain is generally a public ledger, this paper examines the situation where blockchain needs to be private or permissioned since IoT deals with private, sensitive, and confidential information. The main objective of this paper is to discuss the applicability of blockchain to public and private or permissioned network.

II. METHODOLOGY

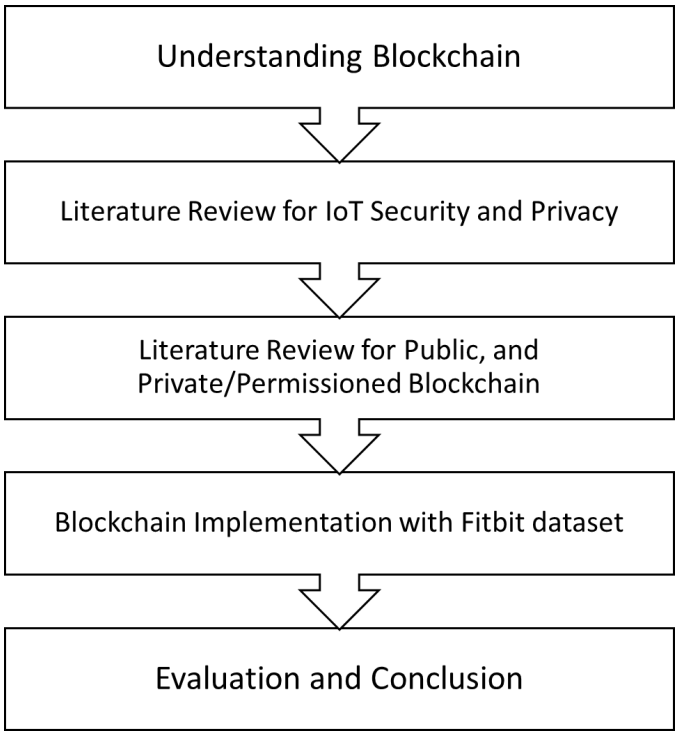

Figure 1 Stages of the project

The stages of this project are divided into five stages. The first stage is to understand general blockchain structure through cryptocurrencies. Then the literature review of the IoT security and privacy, and the blockchain network structure are conducted. The implementation in detail is explained in Section VII. Lastly, the fifth stage is the evaluation and the conclusion out of the collected data and the previous related paper.

III. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

The structure of blockchain results in the advantages of various situations. It is completely distributed inside of the

blockchain network. Also, it is immutable even though all parties has access to it. This is because of PoW. The strength of PoW is mainly by cause of chain structure using cryptographical hard problem. [2] In this section the blockchain details that have a huge impact on understanding security and privacy of IoT with Blockchain structure will be reviewed.

A. Structure of a block

In Bitcoin, a block contains thousands of transactions inside. And since it is a public ledger, all parties who are in the network have access to the chain and transactions. However, in an IoT situation, a block can consist of different data. Here is an example of a block structure:

Size	Field	Description
4 bytes	Block size	The size of block
80 bytes	Block Header	Multiple Parameters
1-9 bytes	Transactions Counter	Number of data
Any	Data	Transactions etc.

Table 1: Structure of a Block

In this case, transactions are known as the communication between the IoT devices. It is not necessarily to be digital cash transactions. This is one also form of the block structure. Each parameter can be adjusted to the consensus or purpose of an IoT network. In the data section, digital cash transactions are stored in Bitcoin. Smart contracts are also used often in practice. A smart contract is a computer protocol that enforces programs when an agreement is met between parties. Block Header is quite important since it is the only variable that will be hashed in the PoW consensus. [2]

B. Block Header Structure

The block header contains the metadata of blocks. It is chained to another block through inclusion of the hash value of the previous block. The block header is to be hashed and included in next block to make changing content harder for attackers. In the Bitcoin scheme, a block also contains version, Merkle Root, Timestamp and nonce. Although, other information can be included depending on objective. the table 2 shows a sample form of block header.

Size	Field	Description
4 bytes	Version	For protocol updates
32 bytes	Previous Block Hash	Hash of parent block
32 bytes	Merkle Root	Summary of data
4 bytes	Timestamp	Creation time of this block
4 bytes	Difficulty Target	Difficulty in PoW.
4 bytes	Nonce	An integer used for PoW

Table 2 Structure of the block header

- Difficulty target and nonce are discussed in the Mining Section
- Version is only additional if there is content/software update inside of the blockchain network. This variable will be the reference to match the protocol version.
- Timestamp is the creation time of the block in Unix Epoch second
- Merkle Root is a root of the Merkle Tree (binary tree) and its traditional purpose is to check the integrity of transactions [2]

Merkle Tree

The Merkle Root is utilized in every block of Bitcoin blockchain. It is useful for briefly checking if the specified data is in the block or not. The Merkle Tree is the process of summarizing all transactions to verify the large-scale data inside of a block. The Merkle Tree is created by recursively hashing each transaction until it reaches the top of the tree (Merkle Root). It first hashes every transaction using the SHA256 hash function. And those digests are concatenated together with another hash then to create new hash.

H_1 = SHA256(transaction 1)

H_2 = SHA256(transaction 2)

H_{12} = SHA256(H_1 + H_2)

where H is the digest of SHA256.

This process is continued until all the transactions are combined and have reached the top of the tree. The figure 1 indicates a Merkle Tree sample of four transactions. The output of SHA256 is a 32-byte string. Every H function is SHA256

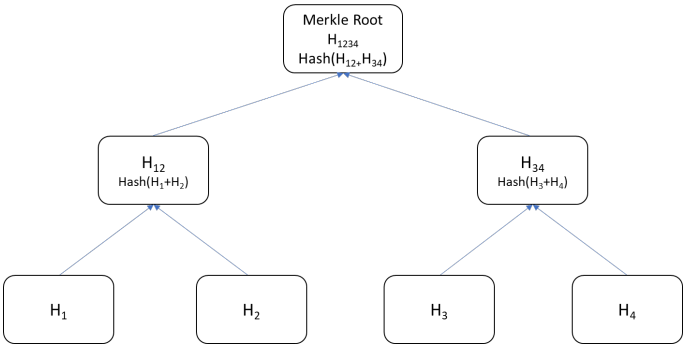

Figure 2 Merkle Tree

Clear Pictures are on the last page

If one of the nodes in blockchain network wants to verify if transaction 3 is in the block. Assume that the node knows the hash of transaction 3 and Merkle Root, the node gets H_4 and H_{12} from the database to compute the Merkle Tree partially instead of pulling all transactions in the block. Although, it is not mandatory field to have inside of a block. However, as the number of data increase inside of a block, the more computational power can be saved by utilizing the Merkle Root. [2]

C. Additional Background Information

Blockchain Network

When handling blockchain, the blockchain network is an important scope to look at since direct access to the network means nodes have access to the blockchain and contents inside of it. To give an example, there are many different cryptocurrencies now. Some of them derived from Bitcoin while others are completely new chains. In an incentive type of blockchain, the first person or group who successfully mined a new block gets certain amount of cryptocurrency. Anyone can join this network since it is an open peer to peer network. These networks are permission-less network. However, when blockchain is applied to IoT situations, there is need for decent authentication in order to decide who has access to the sensitive data. It can be private or permissioned depending on the purpose.

Genesis Block

Each block in the blockchain has the hash value of its parent block. At the very beginning of the chain, the first block, is called the Genesis Block and this block does not contain previous hash. Since every node has to start from at least one block, details of the genesis block must be known by all nodes. Indeed, in Bitcoin, the genesis block is statically hardcoded into the client software. Blocks are traceable by its hash and depth. Starting from 0 at the genesis block, the depth number increases as the blockchain grows. [1] [2]

D. Mining

Mining a block is the most significant part of the blockchain technology. Mining however is quite misleading name considering actual computing behind the scene. As I described in the previous sections, blockchain includes multiple data inside of a block. Each block contains the hash value of the previous block inside of the block header. Then the block header is the input to SHA256 to determine the hash value of the current block. Mining is essentially the computing hash of the block. Nevertheless, there is the consensus of mining in order to protect the integrity of the blockchain and it also makes hashing infeasible. [1] [2]

Structure of Blockchain

Figure 2 is a diagram of blockchain in order to help with understanding the structure of blockchain. Hash of each block is computed by PoW. It is an important part of blockchain to connect each block.

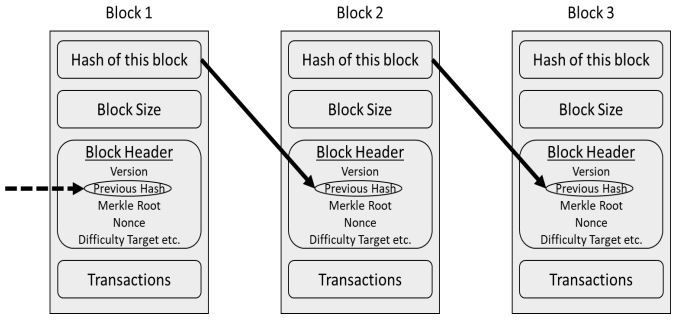

Figure 3 Structure of Blockchain

Consensus Algorithm

Consensus algorithm is a system or protocol used to achieve the agreement amongst the nodes inside of the blockchain network. Frankly, it is an algorithm of how to append a new block to the blockchain. In this paper, however, this paper focuses on the PoW consensus algorithm. [2]

Proof of Work

PoW Algorithm is a protocol to compute the hash value that meets the consensus requirement in Bitcoin, only the block header is hashed. It increments nonce until the digest of SHA256 contains multiple zeros in front. The number of zeros that are required in the digest is decided in mining consensus. The SHA256 hashing function takes any length of input however if the input is longer than 512 bit there is the initialization time cost. The output is 32 bytes String and this has to contain multiple zeros in front as substrings. The miners input the block header into SHA256. Nonce is initially set to zero, then miners increment it until they get required hash. This is called difficulty target. For example, if the difficulty target is 10, digest of the SHA256 has to begin with 10 zeros. [2] In Bitcoin, the difficulty target is set depending on how long the bitcoin community takes to mine a new block. It is set to take approximately 10 minutes. According to the latest block that is mined to the Bitcoin main chain in 2019-08-08 14:08:39, the difficulty target was 19. [5]

E. Consensus

Since mining require high computational power, it is computationally infeasible to alter past transactions in Bitcoin. Conventionally, after six blocks, it is considered impossible to alter the contents inside of the block. The important point is that this is retained by the fact that all parties in the blockchain network follows the consensus. [2] When focusing on a small IoT network, since it is not always public, the agreement needs to be adjusted depending on various factors such as difficulty target, and what data are included. With regards to the difficulty target the number of mining nodes is most likely quite limited in IoT situations. Hence, the difficulty target is quite critical to maintaining reasonable security. Also, IoT has tremendous type of protocols, applications, and devices. For instance, in the medical area, the budget for the installation is decent compared to cases like Smart homes. It means that mining node can be more than one and/or high-performance CPU and GPU needs to be installed which makes mining more efficient even if the difficulty target is high. Thus, the rational adjustment of consensus is inevitable based on what is available to the situation. [6]

One other factor to adjust the consensus is the block size. Bitcoin protocol limits a block's size to be maximum of 1MB, and it is an issue. [7] As mentioned earlier, each block takes an average of 10 minutes to be mined. When the massive blockchain network holds millions of nodes across the world, propagating a new block and reaching the other side of the world takes quite a long time. The

bigger block size is, the longer it takes to spread across the network. Croman et al. conducted that research on this problem and concluded the block size should not exceed 4MB. [8] Concurrently, the more transactions contained in a block, the faster each transaction is confirmed. There are varying arguments about block size and they are also the reason for cryptocurrencies to split up and create new currencies. This is at least in the field of cryptocurrencies. When it comes to IoT, various types of network scale can be expected so there is need for arrangement and optimization of the network and the block size

Forks

A distributed system also has disadvantages due to its structure. One of the issues on the blockchain is the Forks. Yet it can be solved thorough an agreement of how to handle this. Since every node has own copy of the blockchain, all nodes do not necessarily have the exact same copy. When two or more nodes successfully mine a new block, they would be eligible to add a new block to the chain and propagates throughout the network. This only happens when there is more than one mining node and they coincidentally mine similar blocks. When the network faces the issue, other nodes that are physically close to the mining node get an updated version of the chain faster. As a result, two different copies of chain propagate throughout the network. The solution in Bitcoin is to pick the one that has more "work" This means that the block which contains more transactions or has higher difficulty target gets chosen by nodes when the copy reaches nodes. [2]

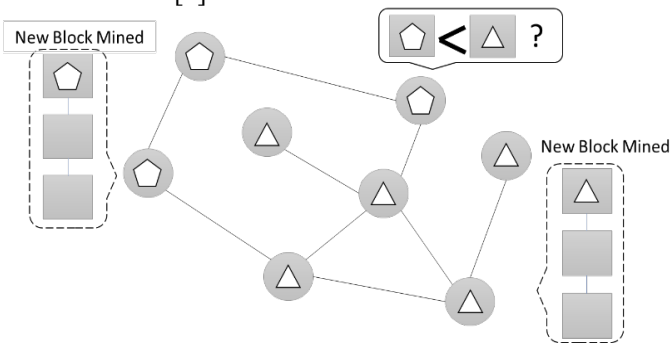

Figure 4 Image of Blockchain forks

F. General Drawbacks of Blockchain

Blockchain has drawbacks as well as merits attached to it. Even though cryptocurrency is quite popular now, there are general concerns such as:

- Energy Consumption
- Bloating
- High-End Hardware
- Network Security
- Infeasible to modify

These are the current obstacles that make blockchain extremely complicated and unstable. [2]

As for the energy consumption, mining consumes an incredible amount of electricity. In PoW, all parties compete to be the first one to mine a new block. The computational power helps parallelizing mining work. Because of this, high-end hardware is required, and they consume more energy. This spiral of escalating energy consumption is a major concern.

In addition, the chain size bloating is another problem to be considered. Due to the structure of blockchain, it is almost impossible to remove, discard or alter the previous transactions. Every block is connected consecutively, and tiny change can cause modification to the entire blockchain. Hence, as the block is added to the blockchain, it can be bloated up inside of nodes' devices. As of August 7th 2019, the size of Bitcoin main chain without any related database is approximately 233GB. [9] When it comes to IoT, there will be more devices and information that will be stored inside of a block. The size bloating issue is clearly unignorable. Moreover, mining does not guarantee network security. It ensures that no data inside of a block is maliciously modified by attackers. There needs to be measures such as an authentication, key exchanges, or security protocol.

Finally, the immutability ensures the integrity of data inside the block however, it can go against its purpose. When any error in the data is found inside of a block that is already mined and is part of a blockchain, it is almost impossible to modify. Even if there is security pitfall of a program, there are no exceptions.

IV. SECURITY REQUIREMENTS OF IOT

IoT technology has grown rapidly over few years. Billions of devices are now connected to the Internet. However, the security of communication, processing, or data storing is yet to be fully covered in every situation due to an enormous number of devices exist. In general, any security design is required to maintain Confidentiality, Integrity, and Availability (CIA) [10] [11] Furthermore, previous papers has described following security and privacy requirements.

- Access authentication
- Privacy
- Data Handling

These requirements should be considered during the risk management process. Access authentication is to ensure that any IoT node trying to access data must be authenticated. Privacy is to keep clients' personal data or information secure from third parties. Data handling is also an obstacle since IoT involves so many devices. Both storage and security while processing data must be considered. These are the security requirements for IoT as service. In practice, security awareness of users is always subject as well. [12]

In addition to the previous requirements, the related work [13] shows aspects to building a secure mobile

healthcare app which can be applied to situations of private/permissioned IoT. These aspects are:

- Secure the data during the communication between possible external sensor and the phone, or device, and during the transfer to a cloud environment
- Secure the data inside the phone and in the cloud environment
- Be transparent on how data is managed and by whom

When we are examining at circumstances like medical IoT or smart home, these criteria are important to be considered while building the IoT network.

Overall, since the acceleration of IoT is in high demands, security problems that accompanied IoT growth are not handled perfectly yet. The next section suggests blockchain as a solution and assess its applicability.

V. Applying Blockchain Structure on IoT

The main objective of the project is to assess the applicability of the blockchain to the IoT security and privacy problem. However, first let us understand how blockchain works with IoT.

Firstly, IoT devices usually consist of low-end hardware. This makes it difficult to involve in blockchain as mining node. Additionally, since blockchain grows when a new block added, the storage of IoT devices is another problem. Due to these factors, IoT devices should be eliminated from blockchain network. They would rather simply push data to blockchain.

This paper would like to propose two classifications depending on the scale of blockchain based IoT

A. Public Blockchain Network.

The first case is when data inside of the blockchain is not sensitive. The best example is digital cash transactions. This is the most common structure of a blockchain network. In the case of Bitcoin, all the digital cash transactions are open to every node in the network and every node can verify any transactions. By inspecting transactions, it retains its integrity. Similarly, in IoT, there will be multiple mining nodes to verify the transactions between IoT devices and possible incentive system can be used as well. The benefit of the blockchain in this case are:

- Peer to peer communication.
- Distributed Structure
- Autonomous coordination with devices

IoT devices here are clients to send transactions to the blockchain nodes for verification and mining. [14] Moreover, secure communication between nodes is also archived using smart contract. [15]

B. Private/Permissioned Blockchain Network.

In many cases in IoT, sensors, cameras, wearables devices or other devices handle personal information. For such cases, blockchain must not be public in order to preserve privacy. For sophisticated blockchain based IoT structure has proposed by [16] using smart home without PoW. This paper proposes similar structure with PoW.

Local Blockchain

Each small scale IoT has a local blockchain that stores and keep track of transactions between devices in hand. The genesis block is filled with genesis transaction from each device. Each block contains a traditional block header where the previous hash is stored to make the chain immutable. Plus, the policy header is included in their model. The policy header is needed to authorize devices and to execute the owner's policy. [16] This header can include parameters such as devices ID, firmware checker, and authentication key.

Local Miner

In private/permissioned blockchain with PoW, there is the limitation of mining node. Since mining node require high computational power and immense storage, centralized local miners process all transactions between IoT devices. When IoT devices communicate outside of a local network, the transactions go through the local miners as a gateway. The local miner is also in charge of generating genesis transactions, providing and updating authentication key. Although these functions can be done separated from mining node as well, but conventionally this paper included them in mining node. Moreover, additional storage can be installed in the local miner as required. Figure 4 describes the network structure.

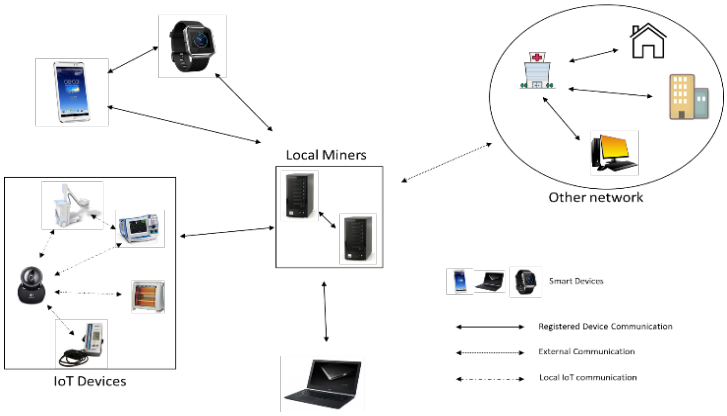

Figure 5 Structure of Private/Permissioned Blockchain

VI. Security and Privacy Analysis

There are two type this paper classified, public and private/permissioned. In public blockchain, there is no point of discussing confidentiality since it is open to anyone. Integrity of transactions inside is kept by blockchain under certain conditions and there are obstacles that need to be discussed:

Consensus Attack

Blockchain's integrity is assured by the PoW which needs computational power. Since it is chained to one block before, as the chain gets longer, the old block becomes more immutable. However, the new block contains only the previous hash. Modifying the latest block is nearly as hard as mining new block. It indicates that if the speed of mining new block is not fast enough in the network, and if attackers have much higher computational power than the community, they could perform fork and invalidate previous transactions. This can be applied to blocks at any depth.

In order to avoid this problem, the high-end hardware should be installed in mining nodes. Incentive system like Ethereum encourage mining nodes to have high computational power. It is not too difficult to overcome this problem with such a large-scale network

To summarize, public blockchain has no privacy over the data inside of the block. Integrity is maintained by enough computational power of the blockchain network.

As for the private/permissioned blockchain, the security assessment is also conducted by Ali et al. [16] Access to the chain is limited by local miners. and only authorized access can retrieve the contents inside of blockchain. Also, policy header includes unique device ID to make transactions transparent to nodes who have access. Similar to the public chain, integrity is maintained by blockchain. Even though local miners have relatively lower computational power or resource compared to public blockchain network, access authentication shuts attacker out of the blockchain itself. Since all incoming and outgoing transactions are audited by local miners, denial of service can be prevented even if IoT devices are physically compromised.

However, the only problem is that once an attacker compromises local miners' communication through 'as man-in-the-middle' attack for example, between IoT devices and local miners. Or local miners' hardware is remotely taken over by an attacker. Attacker can compromise entire network by pretending to be the local miners. On top of that, if the attackers have intensive computing hardware than true local miners, modification of previous blocks is also possible although it is a hard problem.

Overall, the security and privacy of IoT devices are secure with this structure except for minor issues.

VII. APPLICABILITY ASSESSMENT

In terms of security and privacy, it is theoretically secure with the structure, but the performance of the structure is highly dependent on the computational power of the machine that centrally controls and regulates the network. The local blockchain structure was implemented to test the performance of CPUs to assess how realistic it is for local miners to do PoW.

A. Implementation

Implementation of the blockchain is mostly following the structure from the table 2. For the transactions, the public dataset of the Fitbit wearable device was used. This dataset contains a total of one year of human activity that is detected from the Fitbit Charge HR. There are 10 features, Date, Calories, Steps, Distance, floors, Minutes of sitting, Minutes of slow activity, Minutes of moderate activity, Minutes of intense_ activity, and Calories Activity. There are a total 366 records in the dataset. Created blockchain consists of three blocks and each block contains, one third of dataset, 121 or 122 rows of the data and Merkle root of those data. Here is the structure of a block.


```
    {
      "Date": "05-09-2015",
      "Calories": "2885",
      "Steps": "10681",
      "Distance": "7.94",
      "floors": "1",
      "Minutes_sitting": "656",
      "Minutes_of_slow_activity": "240",
      "Minutes_of_moderate_activity": "15",
      "Minutes_of_intense_activity": "30",
      "Calories_Activity": "1356"
    }
  ],
  "blockheader": {
    "version": "1",
    "timestamp": 1565195497244,
    "merkelroot": "a9b95cc01d7215f8027397b9e482550705a25a7c33356028700dee5673167991",
    "previoushash": "00000cb34853cd88eedb2d12b035cf58afafbb8c6416da37faf2234bfcc2143c",
    "difficultytarget": 7,
    "nonce": 50060851
  },
  "instanceCounter": 121,
  "hash": "000000063b7f39061c91712fa7e9aaaf93a164c35f997a2f19ae7bfc5645b562"
}
```


Figure 6 Structure of the block

The last data is in the frame however, this block contains 121 transactions. The previous block is the genesis block and its difficulty target is set to 5. The difficulty target of main blocks is mostly set to 7. This is due to the fact that approximately 10 minutes are spent on mining for this difficulty in most of the machines that were available to this project. The version is set to 1, timestamp is in Unix Epoch second. Additionally, difficulty 5, 6 and 8 are also tested on several machines although difficulty 8 was impossible to mine in some machines. Moreover, the data inside of a block can be replaced by any data since executing time of Merkle Root is not considered here. Figure 7 shows the chart of executing time for each target.

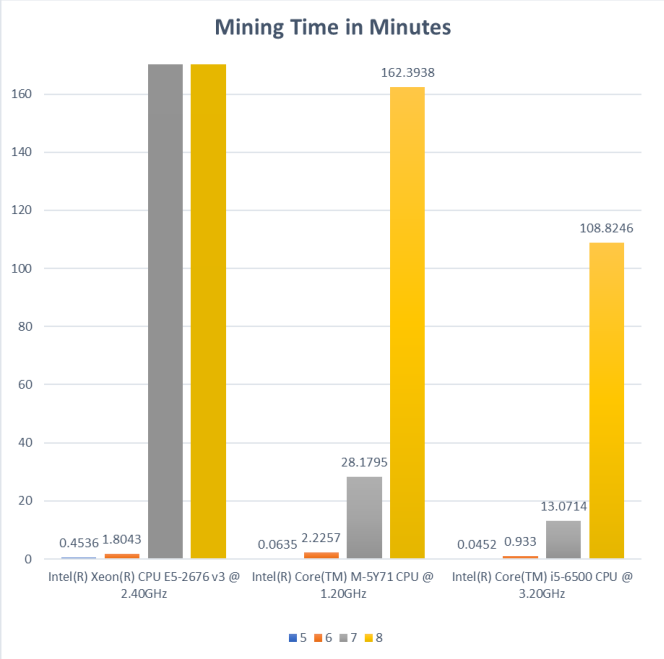

Figure 7 Mining Time for each CPU

The environment that is used for this testing includes the Intel Xeon CPU E5-2676 v3 2.40GHz Core 1 (AWS Instance), Intel Core M-5Y71 1.20GHz, and Intel Core i5-6500 3.20GHz. The mining time was measured for an average of ten blocks. In order to consider the randomness, a timestamp was always different for each block. It means that the output is always different since the SHA256 collision free. The executing time gets longer as the difficulty target increases. Additionally, the time difference between machines exponentially increase as the difficulty target goes up.

As the graph described, the mining time highly depends on the hardware. Even if high-end processors are installed, the mining time elevates dramatically after certain target. For AWS instance, time cost for target 5, and 6 are not excessively different from the other CPUs, however, it consumed nearly infinite time after target 7. In this testing, when the execution time exceed 6 hours, it is considered to be infinite time and the process was terminated.

Moreover, noticeable point was that the mining time also depends on the entropy. It is impossible to predict when the desired digest comes out from SHA256 and some input gives the output that meets the target in first hundred counts while other inputs do not provide it till million counts. The testing executed 10 times for each device and there was a tendency of fluctuation of the mining time since the input varies every time.

Overall, mining a block with PoW depends on randomness. Installing high-end device is not completely reliable to mine a block first. Although it is not consistent, but depending on the input, mining could be performed faster by randomness even with lower computational power.

B. Related Work.

Besides the execution time, previous paper has conducted research on mining efficiency and energy consumption by various hardware for Bitcoin mining. The hash rate of hardware and cost of running it are the primary causes of limiting Bitcoin mining performance. GPU can process more parallelized calculations however it consumes more energy. [17] To sum up, considering these factors, centrally taking care of proof of work with limited resource is quite inefficient.

VIII. CONCLUSION

The recognition of blockchain is skyrocketing over the years from many industries. Furthermore, IoT is gaining the attention accompanied by security and privacy issues. Unfortunately, IoT devices cannot take the role inside of an actual blockchain due to the low computational performance. This results in limiting the number of mining nodes especially in a private/permissioned blockchain network. Since computational power of the whole network directly impacts the integrity of the blockchain, PoW consensus algorithm cannot be confidently stated to be suitable for securing IoT structure. As matter of fact, very new technology like IOTA or Hyperledger Fabric utilize other consensus algorithms. For future research, blockchain with different consensus algorithm will be a significant mode in order to enhance IoT security and ensure the privacy of it.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] A. M.Antonopolous, Mastering Bitcoin, O'Reilly, 2014.

[3] Christopher Ehmke, Florian Wessling, Christoph M. Friedrich, "Proof-of-Property - A Lightweight and Scalable Blockchain Protocol," in *2018 IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, Gothenburg, 2018.

[4] M. Marchesi, "Why blockchain is important for software developers, and why software engineering is important for blockchain software (Keynote)," in *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, Campobasso, 2018.

[5] "Blocks mined on 08/08/2019," BLOCKCHAIN, August 2019. [Online]. Available: https://www.blockchain.com/btc/blocks.

[6] Marco Conoscenti, Antonio Vetrò, Juan Carlos De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Agadir, Morocco, 2016.

[7] J. Göbel, A.E. Krzesinski, "Increased block size and Bitcoin blockchain dynamics," Melbourne, 2017.

[8] Kyle Croman, Christian Decker, Email author, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, Emin Gün Sirer, Dawn Song, Roger Wattenhofer, "On Scaling Decentralized Blockchains," 2016.

[9] "Blockchain Size," BLOCKCHAIN, 08 08 2019. [Online]. Available: https://www.blockchain.com/en/charts/blocks-size. [Accessed 08 08 2019].

[10] Zhiyong Lu, Yunyan Zhou, "The Evaluation Model for Network Security," in *Fourth International Conference on Communication Systems and Network Technologies*, Bhopal, India, 2014.

[11] Parikshit Prasad, Badrinath Ojha, Rajeev Ranjan Shahi, Ratan Lal, Abhishek Vaish, Utkarsh Goel, "3 dimensional security in cloud computing," in *3rd International Conference on Computer Research and Development*, 2011.

[12] R. H.Weber, "Internet of Things – New security and privacy challenges," in *Computer Law & Security Report*, 2010.

[13] Chiara Braghin, Stelvio Cimato, Alessio Della Libera, "Are mHealth Apps Secure? A Case Study," in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, Tokyo, Japan, 2018.

[14] Madhusudan Singh, Abhiraj Singh, Shiho Kim, "Blockchain: A game changer for securing IoT data," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, 2018.

[15] Dinan Fakhri, Kusprasapta Mutijarsa, "Secure IoT Communication using Blockchain Technology," in *International Symposium on Electronics and Smart Devices (ISESD)*, 2018.

[16] Ali Dorri, Salil S Kanhere, Raja Jurdak, Praveen Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Kona, HI, USA, 2017.

[17] Karl J. O'Dwyer, David Malone, "Bitcoin Mining and its Energy Footprint," in *ISSC 2014 / CIICT 2014*, Limerick, 2014.