

Performance of Hash Functions in Blockchain Applied to IoT Devices

Jéssica Ferreira

School of Technology and Management,
Polytechnic of Leiria, Leiria, Portugal
2180079@my.ipleiria.pt

Mário Antunes

School of Technology and Management,
Polytechnic of Leiria, Leiria, Portugal
Computer Science and Communication Research Centre,
CIIC, Leiria, Portugal
INESC-TEC, CRACS, University of Porto, Porto, Portugal
mario.antunes@ipleiria.pt

Mykyta Zhygulsyy

School of Technology and Management,
Polytechnic of Leiria, Leiria, Portugal
2180074@my.ipleiria.pt

Luís Frazão

School of Technology and Management,
Polytechnic of Leiria, Leiria, Portugal
Computer Science and Communication Research Centre,
CIIC, Leiria, Portugal
luis.frazao@ipleiria.pt

Abstract — The IoT (Internet of Things) is a network composed of several devices (things) connected to the Internet and to each other. IoT services are increasingly growing and are allowing companies to deploy scalable solutions with reduced costs and instantaneous data access. These solutions require seamless authentication, data privacy, security, robustness against attacks, easy deployment, and self-maintenance. Such requirements can be given to a company's IoT solution by applying blockchain technology. This paper analyzes the blockchain technology and the advantages and challenges behind its implementation in an IoT environment. A blockchain in IoT scenario was developed to evaluate the performance of different cryptographic hash functions in the IoT device RaspberryPi. Conclusions were drawn when it comes to the viability of some hash functions mainly based on the low resource characteristic shared by the IoT devices, which compromises the performance of the hash function.

Keywords - Internet of Things; Blockchain; Hash Function.

I. INTRODUCTION

Blockchain is a technology with a wide range of applications, being usually associated to cryptocurrencies. However, recently it has been successfully applied as a shared and immutable registry that eases the process of registering and consulting transactions [1].

As a comparative scenario we can think of transactions occurring in banks as blockchain transactions. Nowadays we rely on banks or other intermediary reliable entities to exchange money. It is agreed between the participants of a transaction that the company that processes the transaction has the necessary mechanisms to ensure that it is done successfully and, most importantly, in a safe manner. However, these intermediary entities may fail as it is the case of sudden bankruptcy and thus

the trust is lost and so are the transactions and goods confided to them.

Trust factor is considered in the blockchain technology by the use of cryptographic mechanisms that provide the mathematical proof of the success of the transaction. This proof is undeniably true, providing the participants of a blockchain security and transparency [2].

IoT devices can share information between each other enabling the awareness of all network participants and their surroundings. The IoT service is composed of a combination of sensors, actuators and connectivity. Solutions with some degree of IoT are being implemented at a fast rate with concepts like smart houses, smart cities and smart watches that point out their potential and successful use.

Given that, blockchain is a distributed registry technology and that the IoT architecture is distributed by nature, one can assume that their combination, may be beneficial in a practical scenario, thus contributing to the safety and transparency of the transactions occurred in IoT.

Blockchain is a technology in which the devices use considerable amounts of energy and computing power in order to guarantee the success of transactions. In the opposite, IoT is a network of things which typically have low resources so the combination of these technologies might also be counter-productive.

This paper aims to understand the use of blockchain technology on IoT scenarios, as well as the impact that several hashing algorithms have in limited resources devices. Initially, blockchain topic will be addressed in general as we aim to understand how the technology works and the processes behind

its usage. Topics such as Peer-to-peer networking, cryptography mechanisms, consensus algorithms, advantages and disadvantages and possible problems are addressed concerning blockchain. The third Section focuses on IoT and the implementation of blockchain in them. It addresses the problems these technologies might solve when implemented together as well as the challenges they will face. The fourth Section concerns the tests scenario, it has the focus of explaining the solution implemented, the tests performed, and analyzing the results obtained. Finally, some conclusions are drawn regarding the viability of the hash algorithms tested and future work is addressed.

II. BLOCKCHAIN TECHNOLOGY

This section explains the fundamentals of blockchain technology, namely P2P (Peer-to-Peer) networks, cryptography and consensus algorithms. It also describes the advantages and disadvantages of this components and its potential on IoT.

A. P2P Network

A distributed network architecture can be a P2P network if its participants share parts of their hardware resources such as processing power, storage and printers. These shared resources are necessary to provide the service and content available on the network [3].

Blockchain is a decentralized network with no servers to process data nor clients to request them. However, a *node* represents a participant of the network. Each node has the role of both server and client resulting in the inexistence of a hierarchy between them, and in all nodes having the same role.

Being blockchain technology distributed, a security mechanism should be considered, since there is no SPOF (Single Point of Failure) that may be attacked, and it is therefore harder to interfere with the data. However, this feature is not enough to guarantee security and integrity of data traveling through the network. To achieve that, blockchain relies on cryptography.

B. Cryptography

Generally speaking, blockchain implementations use two cryptographic mechanisms: public key cryptography and cryptographic hash functions.

For transactions to be digitally signed, it needs to use public key cryptography, which proves the identity of who initiated the transaction. It depends on a key to encrypt and a different key, mathematically related to the first, to decrypt. Both keys are computationally complex to discover, knowing only the cryptographic algorithm used to generate them to [4].

When someone signs their transaction with their private key, this guarantees authentication and integrity of the data because decoding is only made possible using the public key. If the decryption process is successful, they know that i) whoever signed the transaction is the owner of the private key and ii) the data is not corrupted nor it was tampered with, otherwise the decryption wouldn't be successful.

These functions convert the translation of any type of data to a series of characters. The same data will always result in the same hash, likewise, the smallest change in the starting data will produce a hash completely different from the previous one.

Creating a hash is a low processing task but the opposite doesn't apply. When the hash value is known it is computationally infeasible to perform the opposite operation and obtain the original data.

Every time a block is created in blockchain the cryptographic hash functions are used to validate a block before it can enter the chain of blocks. Each new block contains the hash of the previous block, which allows it to be persistently connected and that is the reason why the blockchain is immutable.

If an attacker tries to change a block that is part of a blockchain, its content would change along with its hash, in such a way that it wouldn't be aligned with the hash present in the next block [5].

C. Consensus Algorithms in blockchain

As previously stated, the blockchain is a distributed network with several nodes. It is safe due to cryptographic mechanisms and to the fact that all nodes in the network have a copy of the whole blockchain locally. In networks of this nature it is hard to find a method that provides consensus.

The goal of consensus algorithms is to solve the problems that arise when the network tries to reach an agreement when it comes to the data processed on it. When using these algorithms, the participants in the network reach an agreement, such as what block should be next in the chain or how to deal with collisions.

Collisions in blockchain happen when two nodes successfully validate the same block, and both have the potential to belong to the it. When that happens, a fork in the chain is created, which results in two similar chains that are both valid. It is the consensus algorithms job to ensure that the blockchain is the same across all nodes and deal with these collisions[6].

The most used algorithms in blockchain are Proof-of-Work and Proof-of-Stake[7]. Proof-of-Work is the consensus algorithm used in the cryptocurrency Bitcoin. The nodes provide their processing power to solve hard mathematical problems in order to validate a block. Since all nodes of a blockchain hold their own copies of it, properties need to be defined in order to identify which copy is updated and, therefore, the most valid. In the algorithm Proof-of-work such properties are size and computational work. The copy of the blockchain held by all the nodes is always the longest and the one with more computational work put in to it. All the nodes agree with this condition which makes the copy of the chain held by the participants constantly updated.

Proof-of-Stake is expected to be used in 2019 by the cryptocurrency Ether of the Ethereum Blockchain. In this algorithm a node is chosen to validate a block considering an initial monetary value which is returned with a successful validation. The bigger the monetary value, the bigger the chances to be chosen as a validator. However, if it validates invalid blocks the node loses the money invested initially.

D. Advantages and Disadvantages

As there is no central entity to manage the blockchain network, the only thing it needs to function properly is the collective efforts of its nodes to maintain the network stable. Since there is no single point of failure in blockchain, a

corrupted copy of the chain doesn't necessarily result in a corrupted network. It will just be replaced by a valid and updated version of the chain. Each transaction is available for consultation by all nodes, but it cannot be altered nor deleted. This characteristic provides transparency, immutability and reliability on the chain.

Given the large number of participants in the network that contributes to the validation of blocks, the time it takes to process these transactions is very fast compared to what it would take to process them by a third-party entity. When it comes to money transfers made by banks, for example, they can take up to 3 days to be completed, but with blockchain the time is reduced to a few minutes or even seconds.

Naturally, no technology is infallible and despite the enticing advantages that blockchain presents, there are disadvantages that must be taken into consideration. The most worrying drawback that can be pointed out when talking about this technology is its energy consumption. The validation process of a block requires some degree of computing power so that high quantities of energy must be produced to maintain an updated network, which is worrisome when we consider the environmental impact and monetary expenses. Examining Figure 1 referring to the Bitcoin cryptocurrency, during the summer of 2018 the energy consumption required to maintain it was around 72 TWh. For comparative purposes, Portugal generated during 2017 60TWh according to the statistical report of world energy consumption by BP [8].



Figure 1 - Energy consumption for Bitcoin blockchain [9]

To be a part of a blockchain network and to be able to validate blocks successfully, especially with the Proof-of-Work algorithm, the initial investment can be high, since hardware that allows for big processing power is very expensive. Therefore the high energy consumption to validate a block is an expensive task [10].

E. Possible Attacks and other Problems

Although the internal processes of the blockchain network have a high focus on security, there are some attacks to which it can be vulnerable to, and they are all derived from what is called the "51% attack"[11].

This attack occurs when one node tries to control a big part of the network, in such a way that their copy of the chain become the one unanimously accepted. Users usually come together and form what is called a mining pool so that they can join all their

processing power to validate blocks and increase their chances to mine it and collect money from it. As depicted in Figure 2, mining pools in Bitcoin already exist and are growing. It would only take the union of the largest 3 pools for this attack to become a reality [10][11].

III. INTERNET OF THINGS AND BLOCKCHAIN

IoT services are growing and are helping companies to enjoy a scalable solution of reduced costs and instantaneous access to data. It revolutionizes the way citizens and companies interact. According to *Key Information Systems* [12], automation, efficiency, reduced costs, communication and instantaneous access to data are some of the advantages. Some disadvantages are the lack of privacy and safety, since all our devices are permanently connected to the internet it is increasingly hard to guarantee that the data is always safe.

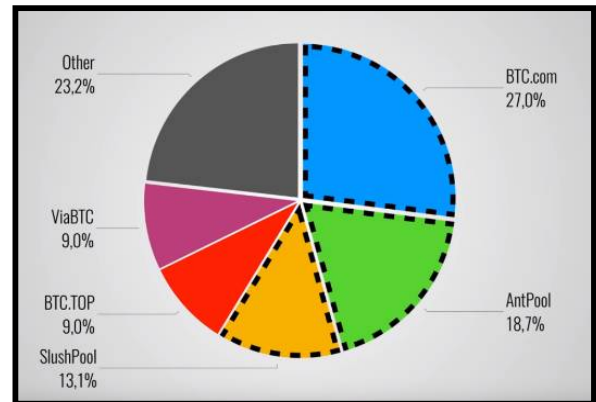


Figure 2 - Percentage per mining pool of Bitcoin [11]

A. Blockchain applied to IoT

Nowadays most IoT solutions depend on a centralized server/client paradigm, where clients connect through the Internet to servers hosted in the cloud. Although these solutions are viable, as IoT grows a new paradigm is needed. Decentralized solutions have been proposed but P2P alone cannot guarantee privacy and security [13]. Blockchain has the potential to answer to a lot of the challenges that arise from the usage of IoT:

- Most IoT solutions are expensive due to costs of central server maintenance in the cloud.
- Maintenance of millions of distributed smart devices is a challenge.
- To increase safety and trust, transparency is essential. An open-source solution is preferred and should be considered in the implementation of the next generation of IoT devices.
- Because IoT typically needs a central entity, the single point of failure issue is prominent. Aspects like time synchronization, registries, privacy and trust are hard to manage consistently [14].

The three biggest challenges of blockchain applied to IoT are [15]:

- **Scalability:** as the number of transactions grow, and so does the blockchain, it might result in centralization because it needs administration of registries, and that wouldn't be real blockchain.
- **Computing power and time:** IoT devices are known for their low processing power and low energy consumption. These devices might not be able to utilize the safest encryption algorithm as it takes a long time to process.
- **Storage:** all nodes keep a copy of all transactions that ever occurred in the blockchain since its creation. The size will increase as time goes by and IoT devices might not be able to store it.

The challenges of blockchain applied to IoT arise from its low resources. Although the processing power is low, these devices can still perform operations as long as algorithms and mechanisms optimized for them are used. The most processing demanding operations in blockchain are the ones that concern cryptographic operations, aspects such as hash functions need to be tested in order to assess its performance and obtain the most viable ones to be used.

IV. TEST SCENARIO

This section explains the solution implemented according to the premises of blockchain applied to IoT. It also presents the performance of several hash algorithms to investigate which one is more suitable for IoT devices.

A. Scenario

The experimental setup consists of two RaspberryPi, each one running a local web server. Two websites were developed using the Python Microframework Flask, with three web pages each. The first website has the following webpages:

- The first web page (Figure 3) allows the user to create a block by filling fields regarding the contents of it, such as the name of who initiates the transaction, the destination and the value it wants to transfer. The block will then be validated and added to the copy of the blockchain of the device who has validated it. Lastly, it will be broadcasted to the other RaspberryPi device which will check the block's integrity and add it to its own chain.
- In the second web page (Figure 4) the user can see the whole blockchain and consult its content. The information made available is: the content of each block in the chain, free space left on device, total current size of the blockchain, average block size, number of blocks that can still be stored in the device, total of hashes calculated and the time it took to process 10 blocks of the chain.
- The third web page (Figure 5) allows the user to verify the blockchain's integrity. Each block of the chain is analyzed regarding the hash contained in it and whether it matches the hash of the previous block in the chain. It is also verified whether the hashes comply with the rules of block validation which are addressed later in this document.

Figure 3 - Web page for creating a new block

The second website is like the first, except regarding how the blocks are made. Its purpose is to test the way blocks are created in IoT devices and networks. The information contained in these blocks are environmental values gathered by IoT sensors, such as temperature and humidity. Instead of entering information manually about the transaction, all the environmental values are sent through HTTP requests automatically by the IoT devices.

Figure 4 - Blocks in local web server

Figure 5 - Web page to verify block's integrity

B. Block Validation

This scenario uses an important concept about block validation in blockchain which is the idea of *NOncE* (*Number you can only use Once*).

When a block is created it must be validated before it can belong to the chain. To achieve that, a mathematical problem is proposed to all nodes: *The final hash of an entire block must result on a hash number less than to one defined by the current*

validation difficulty. Difficulty is an established number which allows for the calculation of a fixed hash. For a block to be valid, its total hash must be a number lower than the fixed hash calculated using the difficulty. In order to find a hash lower than the fixed one, a specific value must be found and added to the block. This value is called the *nonce*.

In a blockchain network such as Bitcoin, the difficulty changes every 2 weeks to ensure that the nonce is unique. This contributes to the safety of the entire chain when it comes to its persistency and immutability. The implemented scenario validates its blocks according to the blockchain nonce system.

C. Tests

As mentioned earlier, the tests compared the following cryptographic hash algorithms:

- MD5, 128 bits - Its was initially developed with the purpose of being a cryptographic hash function, but unfortunately several problems were immediately found. The main requirement of these functions is the infeasibility to find different data with the same hash value. MD5 fails in that department.
- SHA-1, SHA-224, SHA-384, SHA-512. These algorithms have the size of 160 bits, 224 bits, 256 bits, 384 bits and 512 bits respectively.

Each block contains the same information about a transaction such as its initiator, destination, value exchanged, nonce and hash of the previous block. Figure 6 represents the average size of a block validated using different hash functions. It was observed that the algorithm which produced smaller blocks was MD5 while SHA-512 is the largest. These results were expected since each function results on a fixed character value and size.

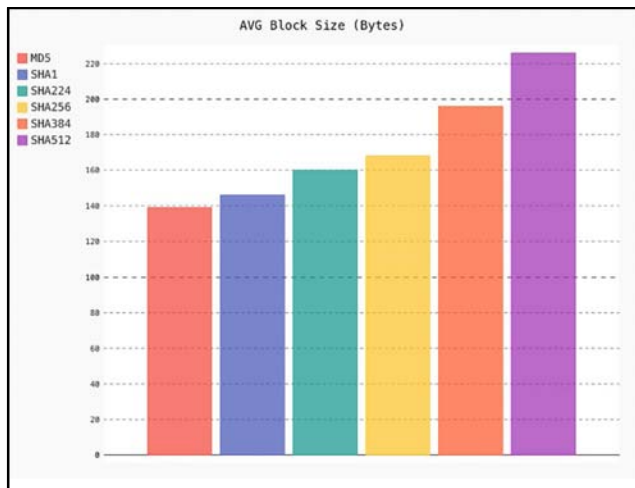


Figure 6 - Average block size for each hash function

During the validation of a block, hashes are calculated consecutively to meet the current difficulty requirements.

For testing purposes, the mathematical challenge calculates a *Nonce* which makes the final hash of the whole block to begin

by a fixed number of zeros. The bigger the number of zeros the harder it is to find the hash.

Figure 7 represents the number of hashes calculated until the Nonce value is found with the number of initial zeros, from 2 to 4. It is possible to observe that the number of hashes calculated with two zeros in the beginning was very similar across all algorithms. However, with four zeros, there is an abrupt change between them. The hash function that calculated more hashes was SHA-512 (9222953) while SHA-224 calculated fewer hashes (354037). These results were expected since the difficulty and the size of the final hash are factors that contribute for the number of hashes calculated in order to find the nonce value.

The difficulty is a factor purposely used in blockchain to increase the number of hashes calculated to find the nonce and, therefore, validate a block. It adds a challenge to the validation and contributes for its persistency and immutability, as it was mentioned earlier. Therefore, as the difficulty increases so will the number of hashes calculated.

Naturally, as the size of the final hash increases amongst the functions that were tested, the more hash values are possible to be calculated, so it is expected that the hash function with the biggest size will always calculate the most hashes, and the contrary is also possible to be observed in these tests.

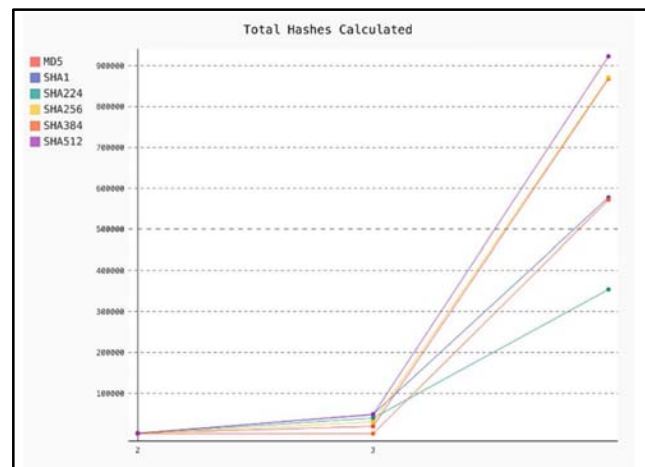


Figure 7 - Number of hashes calculated with different mathematical challenges

Given the same mathematical challenge mentioned previously, the total time it takes to validate 10 blocks was calculated for each number of zeros mentioned above.

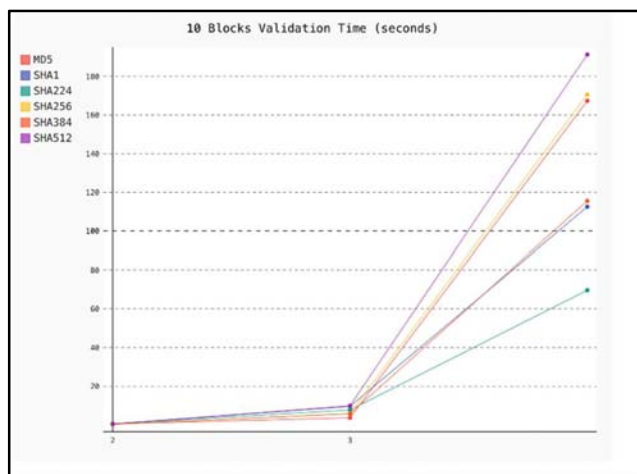


Figure 8 - Time to validate 10 blocks according to difficulty

Figure 8 shows that SHA-512 took the longest time to validate 10 blocks, in about 3 minutes and 20 seconds, while SHA-224 took the least amount of time, in about 1 minute and 15 seconds. These results were not expected since one would assume that the hash function that calculates hashes with the smallest size would be the one to validate blocks the quickest and that wasn't the case. As it is possible to observe, SHA-224 was the quickest to validate as MD5 and SHA1 which results in smaller hash values (128 and 160 bits respectively) and took almost twice the time.

D. Results Analysis

IoT mechanisms must use as few resources as possible because the devices do not possess a lot of computing power. Of all the hash functions tested the ones that would fit a blockchain in IoT scenario would be the ones that can provide low or no probability of collisions without occupying a lot of memory space and processing power whilst validating blocks.

The SHA-1 function appears to be a good choice, but there have been found collisions, different data with the same hash value, and that is not an option as it provides a security problem. According to the experiments, MD5 would also be a viable solution but it also has security and collision problems, so it is not the best option.

SHA-512 appears to be the safest and more robust, but its size and processing time make it unviable for IoT devices. The device used was the RaspberryPi 3 which has a reasonable computing power compared to most IoT devices. Despite that, it still had to dedicate over 3 seconds of processing time to validate blocks, which is too long.

In this chapter tests were made in a blockchain environment applied to IoT, developed in a RaspberryPi 3. The aspects analyzed were: block size, number of hashes calculated until complete block validation and the time it takes to fully validate 10 blocks. According to the experiments, the best cryptographic hash functions must be a variation of SHA-2 with reduced size. SHA-224 has produce the best results, but SHA-384 is also viable since its results were very similar to those obtained with SHA-224 [16].

V. CONCLUSIONS AND FUTURE WORK

In this paper the fundamental concepts of blockchain technology were discussed, such as how a P2P network works, what are digital signatures and what is their role in transaction's integrity, the meaning of hash functions and their role on network immutability, consensus algorithms and the dangers of the "51% attack".

Blockchain technology has the potential to provide IoT with a distributed mechanism to share information in a safe manner challenging the central management paradigm that exists nowadays on IoT.

A simple blockchain IoT solution was created using two RaspberryPi 3 devices. A website was developed in order to create the blockchain and its basic functionality and to test different cryptographic hash functions. Experiments gave us information about the average block size, number of hashes calculated until successful validation of one block and the time it takes to validate 10 blocks of the chain.

Through testing we were able to gather relevant information regarding the performance of hash functions in the IoT devices. It was concluded that the best hash function is a variation of SHA-2 due to its lack of collision problems, either SHA-224 or SHA-384, since these are amongst the ones that took less time to process blockchain functions but also produce the blocks with a smaller average size.

As future work, the same tests need to be done in different IoT devices. All the tests addressed in this paper were made in a RaspberryPi 3, which is frequently used in IoT environments, however, other IoT devices with even less resources, need to use cryptographic mechanisms if they wish to join a blockchain network. IoT networks are scalable and even though the devices can be very different from each other, the same hash function needs to be used in all of them to guarantee blockchain integrity.

ACKNOWLEDGMENTS

This publication is funded by FCT - Fundação para a Ciência e Tecnologia, I.P., under the project UID/CEC/04524/2019.

REFERENCES

- [1] M. Gupta, *Blockchain For Dummies®*, 2nd IBM Limited Edition. John Wiley & Sons, Inc., ISBN: 978-1-119-37123-6 2017.
- [2] S. M. Roman Beck, Jacob Stenum Czepluch, Nikolaj Lollike, "BLOCKCHAIN – THE GATEWAY TO TRUSTFREE CRYPTOGRAPHIC TRANSACTIONS" (2016). Research Papers. 153.
- [3] Schollmeier, Rüdiger. "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications." *Proceedings First International Conference on Peer-to-Peer Computing*. IEEE, 2001.
- [4] Stallings, William. "Cryptography and Network Security, 7th Edition". Pearson Education, ISBN: 978-0134444284. 2006.
- [5] Zheng, Zibin, et al. "Blockchain challenges and opportunities: A survey." *Work Pap.*–2016 (2016).
- [6] E. E. F. Xavier Olleros, Majlinda Zhegu, "Digital Transformations,". Edward Elgar Publishing Limited. ISBN: 978-1-78471-775-9. 2016.
- [7] B. Arati, "Understanding Blockchain Consensus Models".

- Persistent Systems Ltd. White Paper. 2017. Available: <https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf>
- [8] B. Dudley, "BP Statistical Review of World Energy 2018," 2018. Available: <https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2018-full-report.pdf>
 - [9] Digiconomist, "Bitcoin Energy Consumption Index - Digiconomist," *Digiconomist*, 2018. Available: <https://digiconomist.net/bitcoin-energy-consumption>.
 - [10] J. Golosova and A. Romanovs, "The Advantages and Disadvantages of the Blockchain Technology". In 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE) (pp. 1-6). IEEE..
 - [11] B. Martijn, "Preventing the 51%-Attack: a Stochastic Analysis of Two Phase Proof of Work in Bitcoin." 22nd Twente Student Conference on IT. 2015. Enschede, The Netherlands.
 - [12] C. Ivan, V. Miroslav, and H. Sinisa, "Classification of security risks in the IOT environment". *Annals of DAAAM & Proceedings* (2015): 731-741.
 - [13] T. M. Fernández-caramés and S. Member, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access* vol.6 (2018): pp.32979-33001..
 - [14] R. Gowri and B. Krishnamachari, "Blockchain and the Internet of Things: the IoT blockchain opportunity and challenge," *arXiv preprint arXiv:1805.02818* (2018).
 - [15] A. Banafa, "IoT and Blockchain Convergence: Benefits and Challenges". *IEEE Internet of Things*. 2017.
 - [16] S. Rajeev and G. Geetha, "Cryptographic Hash Functions: A Review". *International Journal of Computer Science Issues (IJCSI)* 9, no. 2 (2012): pp.461-479