Blockchain Security for IoT

Gustav Karlsson Anton Vänman
guska060@student.liu.se antva863@student.liu.se
Supervisor: Andrei Gurtov, {andrei.gurtov@liu.se}
Project Report for Information Security Course
Linköpings university, Sweden

Abstract

Recently there have been a surge of integration and usage of technologies such as Internet of Things (IoT) to improve the manufacturing of products. However, two of the main concerns of using IoT-devices is their poor data security as well as their scalability. One way to handle this is to implement a blockchain technology to counter act this lack of security. This report investigates the scalability and processing power needed to host a blockchain on an IoT-device as well as what security threats are possible when implementing the blockchain framework Hyperledger Fabric. The findings are that if nodes get compromised in the blockchain network it's still susceptible to attacks such as sybil attacks. The network is also prone to external attacks like a DDOS-attack. According to our findings hosting the network on a Raspberry Pi 4 seems to be a viable alternative performance wise. Although, the lack of support for ARM64 processors hinders the implementation.

1 Introduction

Factories and households are stepping into modern network infrastructures and are growing an interest in using Internet of Things (IoT) in the everyday production and lifestyle. This is everything from smart homes with lights being controlled by the phone to sensors collecting data in a production line. All these devices are constantly connected to the internet and consists of buttons, sensors etc. However, one common problem with lots of IoT devices and solutions have been their lack of security and communication between devices [1]. This makes them vulnerable to attacks both affecting the output as well as listening to its output. IoT devices are often weaker than standalone devices by nature and have limited performance in both power and capacity.

One solution to these problems is implementing blockchain technology together with the IoT-devices to handle data and security. Blockchain has gained a lot of popularity during the 2010s with cryptocurrencies such as bitcoin and Ethereum. Blockchain has much more uses than that and is appealing due to its scalability, modularity, decentralized structure, and security features which scales well with IoT-networks. Due to blockchain having an append only philosophy it's impossible to change the record of previous blocks.

One problem with using IoT together with blockchain is the performance limitation in the IoT devices and our focus on the performance valuation of using smaller IoT devices in a larger scale project. One problem with using IoT together with blockchain is the performance limitation in the IoT devices and our focus on the performance valuation of using smaller IoT devices in a larger scale project.

2 Background and theory

This section aims to cover key concepts necessary to understand blockchain and the framework used in this project. As well as the theoretical perspective that will be used in the analysis and conclusions parts of this paper.

2.1 Raspberry Pi

A Raspberry Pi (RPi) is a small single board computer (SBC) developed by the Pi foundation. The device is widely used because of its low price and its modularity options. The Raspberry Pi has both 32-bit and 64-bit versions and comes with an ARM based processor architecture [2].

2.2 Blockchain

The blockchain is used to create trust, as explained in "What is the blockchain?" by Massimo Di Pierro [4]. More specifically, trust in a distributed system. It is a way to detected tampering with stored documents. Documents that are stored with, in most cases, a time stamp and a hash. Short version, a hash is a way to hide what is in a string of characters. An input is given, and the hash changes it. It can later be changed back so that what was stored is readable. The document, the time stamp and the hash are what makes up a block in the chain. Each hash

points to a previous block in the chain down to the Genesis block, the first block. The documents that are stored are not necessarily shared around, but the hash sequence is. This makes it so that every change to the chain is recorded and cannot be altered without breaking the chain where the change happens, creating a new blockchain. This makes the blockchain an append only type of storage.

2.2.1 Permissioned blockchain and private blockchain:

A private blockchain is a permissioned blockchain in that it is only possible to join a private blockchain if given permission by the network's administrators.
Access, validation, and participation rights are restricted and can be given by a Membership Service Provider (MSP), existing members or any regulating body.
A private blockchain can be likened to an intranet, that is protected by a firewall. In this case the firewall is the permission to enter the network and have access rights. [5]

2.2.2 Smart contracts:

A smart contract can be described as using a ledger for distributing funds. An example of this can be a payment from 4 sources. The payers will then pay to the smart contract and if the funds are reached successfully, it will distribute the money to receiver. If funds are not reached however, the contract will be terminated, and money will go back to its previous owners. A smart contract can be trusted since it is both immutable since it is stored in a blockchain as well as distributed so every member of the blockchain network can spot any wrongdoing in the contract. [6]

2.2.3 Blockchain and Energy Usage

One of the main obstacles for widespread blockchain usage is the energy consumption used. For example, the popular cryptocurrency Bitcoin uses around 91 terawatt hours annually and is around 0.5% of the total global energy consumption [7]. One of the main reasons for the high energy consumptions of blockchain technologies is the usage of Proof of Work (PoW). Authors such as Gallersdörfer et al. notes that using energy-efficient algorithms together with the right security measures is key for finding a sustainable blockchain application [8].

2.2.4 Scalability

Various factors impact the scalability of a blockchain. Factors mentioned by Eklund and Beck [9], are size, complexity and how distributed or centralised the blockchain is. Complexity refers to for example how detailed and exhaustive the smart contracts are or how the consensus protocols are designed. Distributed to if there is a centralized hub with the ledger or if every node has its' own copy of it. Size, the blockchain will grow the longer it has been in use and the more transactions are listed in the ledger.

2.3 Hyperledger Fabric

Hyperledger Fabric is a blockchain technology. To be more precise Fabric has a ledger, utilizes smart contracts, has a modular architecture, and manages transactions. What separates Hyperledger Fabric from other blockchain frameworks is that it is a permissioned blockchain and that it is a private blockchain. This means that for example an MSP is needed to gain access to the blockchain. Which in turn means that Fabric has additional security compared to permissionless and public blockchains. [10]

Hyperledger Fabric is part of a larger project led by the Linux foundation, known as Hyperledger. The goal of Hyperledger is to support open-source collaborative development of blockchain technology [11]. Fabric is one of the available frameworks, there are more listed on Hyperledger's website, Iroha, Sawtooth, Quilt to name a few [11].

2.3.1 Ledger:

In Hyperledger fabric the ledger consists of two parts. The world state, which is the current state of things, which in turn is based upon the history of changes made, which is the second part, the blockchain. The blockchain consists of a chain of blocks. Each block contains a log of transactions made, that resulted in the world state when the block was created. [12]

2.3.2 Channel:

Channels can be described as subnetworks in the main network of Fabric. These subnetworks are more private in that they have their own ledgers and that a device needs permission to write to the channel blockchain [13].

2.3.3 Organization:

An organization is an entity that has access to channels. It also can give identities for participants in the organization so that every transaction is transparent and identifiable. [14]

2.3.4 Peers:

Peers can be seen as units that can access an organization and its different channels. The peer hosts all chain code and ledgers that is present on the network and are the only types of units that contains this information. Peers transmit this information via interaction with other peers. [15]

2.3.5 Application:

Is external to the blockchain network, it interacts with the network by doing transactions and receiving ledger updates [16]. So, the blockchain network will need to be set up first, followed by a local smart code testing environment, followed by setting up a connection profile and preparing identities, such as admin and user, then finally the application can be written [17].

2.3.6 Membership Service Provider (MSP)

The MSP is a version of asymmetric cryptography. The membership service provider exists on channels and within every organization in the channel. Its' job or role is to verify identities by handling the public key in a public-key cryptography pair. By virtue of being able to identify members of the blockchain it also informs about the members role in the blockchain. The MSP providing proof of membership is part of that Hyperledger Fabric is a permissioned blockchain.
[18]

2.3.7 Ordering Service

The ordering service groups transactions in order and ensures ledger consistency across the blockchain. The ordering service consists of nodes that are individually called orderers that together are the ordering service. A new transaction needs to be approved by all orderers before it is added to the ledger. So, the ordering service ensures that the order of transactions in the ledger is the same across the nodes, thus achieving ledger consistency.
[19]

2.4 Docker

Docker is a service that provides lightweight containers for deploying, creating, and executing systems [20]. Containers can have preinstalled environments allowing the application to be deployed as just a single package. Docker runs on the operating systems kernel and therefore consumes less memory than a traditional virtual machine would do [21].

2.5 Prometheus

Prometheus is an open-source metric monitoring toolkit developed by Soundcloud. Prometheus stores and collects all its metrics with timestamps, which makes mapping and graphing of the metrics possible.

Node exporter is a plugin by Prometheus which captures *NIX kernel metrics which are hardware and OS specific. [22] These metrics are then retrievable with the use of Prometheus.

2.6 Grafana

Grafana is a tool that lets the user visualize and query generated metrics. This is most often done with either graphs or a dashboard within in the Grafana server. [23]

2.7 Research questions:

Can a small-scale block chain network be hosted on a SBC machine such as a Raspberry Pi? How well will the performance keep up on the machine while maintaining the Blockchain.

How will implementing a Blockchain affect the security of an IoT device? What happens to the access control of a device when implementing a decentralized access control.

3 Method

How the project was conducted.

3.1 Setting up prototype/testing environment

For this project we have chosen to use the *Hyperledger Fabric* framework. It is a modular blockchain framework that functions as the foundation for our blockchain in this report.

3.1.1 Structuring the prototype

The prototype was a Raspberry Pi 4 with 4GB of RAM running a 64-bit version of Raspbian version 16.8. For setup and construction of prototype we looked and similar projects and how they had done it, noteworthy were Chinyati [24], Jedrzejczyk [25] and Hedlin [26]. Since there was no official documentation for set up and deployment, we leaned on unofficial GitHub repositories for perquisites and configurations. Prequisites consisted of Raspbian OS, some software packages for docker compose to function and Golang. Beyond this docker images needed to be altered for them to function on Aarch64/ARM64 architecture. After which they were built and config files and binaries were altered. To make sure that everything was working as intended we downloaded fabrics 2.3.3 and deployed the Hyperledger Fabric test network [27].

3.1.2 Receiving metrics

To capture the metrics, Prometheus and node-exporter was run at the Raspberry Pi. The timeseries metrics are then pulled via HTTP to a locally hosted server, and this is used together with the kit node-modules and Grafana to visualize the data.

3.2 Testing

For our testing network we are using one Raspberry Pi 4 and hosting both our clients and our server on this machine. This was due to our difficulty of setting up our network correctly and took lots of time away from actual testing of the network. The testing environment is shown on figure 1.

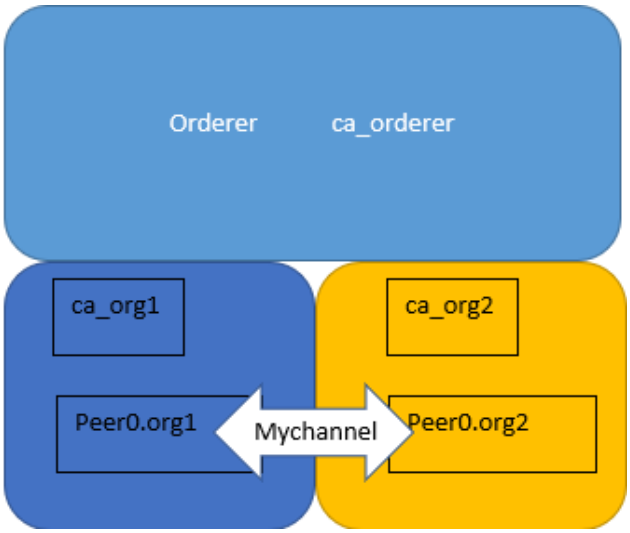

Figure 1 - Setup of the test-network

The testing was done via the test network provided by Hyperledger Fabric, which includes 2 clients and 1 host where a list of cars can be manipulated via CRUD operations via either of the clients. This is checked through the CA to validate the transactions sent by the different clients.

4 Performance Evaluation

After booting up the Hyperledger Fabric network on the Raspberry Pi 4, creating a channel for our two Peers, invoking the chain code and completing several queries and appending to the blockchain we generated the following graphs.

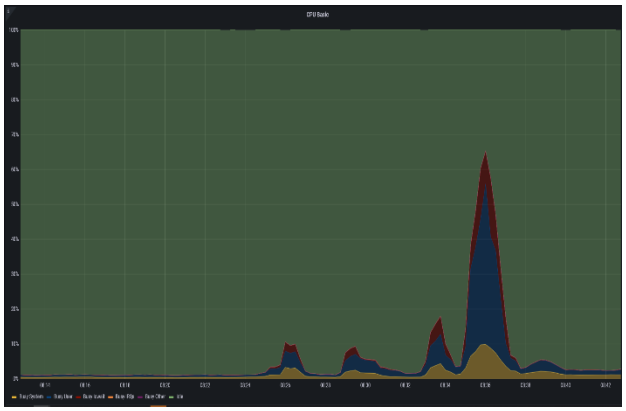

Figure 2 - CPU usage over time while using Hyperledger Fabric

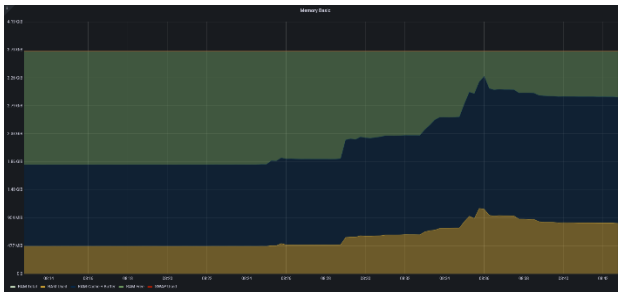

Figure 3 - RAM usage over time while using Hyperledger Fabric

In figure 2 and figure 3 you can see the generated graphs that were extracted from hardware using Prometheus and Grafana. Here we can see the different spikes in CPU usage where the first spike is launching the test network. Second spike is creating a channel on the test network. The last big spike is launching the chain code on the machine. The small bump afterwards is invoking on the chaincode, adding a new entity. The memory graphs timestamps are indicating a similar progression on the usage of memory while using the blockchain.

Attempts were made to deploy the Hyperledger Fabric on multiple Raspberry Pis as well as adding a remote host with a machine running Kali Linux. However, adding a host running an x64 architecture seemed to cause clashes in the packets. So due to time constraints setting up this other environment was cancelled.

5 Security Evaluation

One of the main concerns in IoT devices is the lack of security in the devices. An example of this can be seen in

a survey from Ouaddah et al. where the authors examined the current state of access control standards in IoT devices [3]. What the authors found was that there was no standardized way to ensure access control for IoT devices and the current implementation was very much lacking in capability.

Blockchain can be used to solve many of the problems inherent to IoT. In "IOT Security Issues Via Blockchain: A Review Paper", Sultan *et al.* [30] brings up blockchain's improvement of the integrity of information by spreading around copies of the information to multiple nodes or peers. That blockchain provides privacy by permission being required to gain access to the chain. For Hyperledger Fabric the permission is carried out via the creation of new channels with chosen participants that have access to the data. Accountability is provided by actions or transactions being recorded that cannot be altered without breaking the chain of blocks. Trusted accountability, however, inversely affects anonymity, good accountability leads to weaker anonymity. Blockchains decentralized nature with a distributed ledger also leads to higher fault tolerance, if one node disappears it doesn't mean that the entire network will go down, decreasing the single points of failure. However, Hyperledger Fabric has some centralized key features such as the MSP. A malicious MSP can potentially lead to catastrophic damage to a network which makes it a single point of failure, making the network less fault tolerant.
There are attacks that still work against the Hyperledger Fabric implementation of blockchain, in "Ripping the Fabric: Attacks and Mitigations on Hyperledger Fabric" Dabholkar *et al*. [31] describes viable attacks.

5.1 Sybil attacks

Due to Hyperledger Fabrics Membership Provider (MSP) being a centralized function its seen as a single point of failure. Therefore, if the MSP gets compromised it is an potential attack angle. One of the attacks which could be carried through from this angle is Sybil attacks. Sybil attacks is seen in peer-to-peer networks where a node or a peer has multiple identities which in turn disrupts the trust within the network [33]. Due to Hyperledger Fabrics lack of consensus algorithms against Sybil attacks such as Proof of Work or Proof of Stake, Fabric is vulnerable to this kind of attack. If the disrupted nodes control a majority of the network, it can then carry out a 51% attack. Due to having majority of the votes, the malicious nodes can hinder transactions from happening.

5.2 Intentional Fork attack

Hyperledger Fabric relies on deterministic consensus algorithms. It is predictable based on what has happened. Because of this each new block created is final and correct. Meaning cannot be changed. If the ordering service becomes malicious, due to a security breach, data leak or another working attack vector, it can lead to conflict in the network. If the ordering service sends out different new blocks to different peers, it will lead to the peers with new block A rejecting blocks from peers with new block B. Thus, distorting the network.

5.3 DDoS attack

If an attacker has managed to get hold of enough validating peers or if the blockchain network is large enough, has enough peers in ratio to the ordering service. An attack can be done by launching fetch requests to the ordering service, more than it can handle, thus overwhelming it and denying the blockchain of its' service, denying the possibility to add blocks to the chain.

6 Discussion

The results indicate that a Raspberry Pi is more than capable of hosting a small scale Hyperledger Fabric network. The different appending and querying actions in the network seemed to have only a miniscule stress factor on the IoT device however invoking the chain code seemed to cause larger amounts of stress. However, invoking a chain code is only done on rare occasions so could be consider a moot factor. Another metric which would have been interesting to acquire is the power consumption of the Raspberry Pi. Sadly this project couldn't get a hold of a measuring tool, but running several Raspberry Pi:s could be costly in the long run/ draining on IoT devices which do not have access to a constant power outlet, like drones.

The Hyperledger Fabric is not designed for ARM64/Aarch64 applications which hindered the implementation of running the Hyperledger Fabric network together with a host running a x64 operating system. Chinyati also share these problems in *Securing Internet of Things (IoT) devices using Hyperledger Fabric (Blockchain technology)* where blockchain packets would not be accepted by the ARM64 system if generated on a x64/x86 system, however the opposite would occasionally work [24]. Due to the good capabilities of the Raspberry Pi of hosting a Hyperledger Fabric network it would be appreciated if the software got official support to the ARM64 architecture. Especially regarding the smartphone market which almost exclusively utilize ARM64 processors and are strong enough to host and join blockchain networks such as HLF. The added support for ARM64 processors could also lead to more studies being

done on the subject due to the barrier of entry being lower.

Another aspect that would be interesting to examine is how the Raspberry Pi compares to other similar SBC:s like the Obroid-XU4 as well as how efficient the ARM64 architecture is versus the x86/x64 architecture. According to a study done by Dr.Yuan it seems that the ARM64/Aarch64 has greater performance gains to an x86_64 if the binaries are native, which they are in this project [28]. A follow up study could be done comparing the CPU and RAM usage of the different architectures running different sized Hyperledger Fabric networks.

One concern that was raised in the Background was the lack of access control in IoT devices. This can be traced to the centralized access control which is widely used in IoT devices. However, while implementing a blockchain such as Hyperledger Fabric the implementation of a decentralized access control seems to result in advantages in security [32]. The drawback of the increased security is worsening the ease of use where policies will be harder to keep updated. With the Hyperledger Fabric approach this won't be an issue due to the use of Smart contracts which are easily pushed to the blockchain. In this project the Network was launched locally, however it could be interesting to see how the access control of the data is changed when implementing Hyperledger fabric.

7 Related work

"Hyperledger Fabric Blockchain for Securing the Edge Internet of Things" by Houshyar Pajooh *et al.* [29], is similar to our study but uses two different environmental setups and a virtual machine desktop. They also used an earlier version of Hyperledger Fabric, 1.4 and four peers, aka four Raspberry Pi. We measured RAM and CPU usage, Pajooh *et al.* measured transactional throughput and latency, depending on batch size and block size, as well as computer resources and network resources. Showing what is required in terms of running a small IoT network.

In "Secure Drone Identification with Hyperledger Iroha" by Hashem *et al*. the usage of a different distribution of Hyperledger together with IoT devices is examined [34]. Here the authors used the Drone Remote Identification Protocol in its blockchain technology, and the authors simulated 100 to 200 drones in a remote network hosted on an AWS (Amazon Web Services) computer. Due to a limitation on the AWS system only 30 nodes could be used to simulate this drone network. The Iroha version struggles with the same type of security threats and uses a slightly different consensus algorithm for its blockchain the Yet Another Consensus Algorithm which is a Byzantine Fault Tolerance Algorithm. The results show how the size of the network, number of nodes and drones, and block size, number of transactions per block, impact response time, time until transactions are stored in the blockchain.

8 Conclusions

This project aimed to evaluate how applicable blockchain is for security in IoT devices. For this purpose, Hyperledger Fabric was deployed on Raspberry Pi 4. Hyperledger Fabric was chosen for its popularity of the Hyperledger Foundations frameworks and amount of documentation for it. Raspberry Pi 4 was used to simulate a device in an IoT network, the device used in a larger network will probably be weaker in CPU and RAM. The findings suggest that devices used for an IoT network can have smaller cache, RAM and CPU.

Hyperledger Fabric blockchain provides security to IoT mainly in that it is a permissioned and private blockchain. It improves and provides some properties, such as better privacy, integrity, fault tolerance, and access control. However, Fabric also brings some centralized features such as the MSP which creates a single point of failure to attack. Nevertheless, Fabric can lose nodes without losing the ledger. With that stated, attacks are feasible from compromised nodes on the network, such as a DDoS attack.

Further areas that could be of interest to study are different hardware setups, which could include IoT devices with similar architectures like phones or trying different architectures and software configurations of Hyperledger fabric.

References

[1] Sjoerd Langkemper "The Most Important Security Problems with IoT Devices" eurofins-cybersecurity.com https://www.eurofins-cybersecurity.com/news/security-problems-iot-devices/ (Accessed Mars. 28, 2022).

[2] Accessed Mars 12, 2021. [Online]. Available: https://www.raspberrypi.org/documentation/faqs/#introduction

[3] Ouaddah, A. et al. (2017). Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks*, 112, 2–3. Available from https://doi.org/10.1016/j.comnet.2016.11.007.

[4] M. Di Pierro, "What Is the Blockchain?," in Computing in Science & Engineering, vol. 19, no. 5, pp. 92-95, 2017, doi: 10.1109/MCSE.2017.3421554.

[5] Shobhit Seth "Public, Private, Permissioned Blockchains Compared", investopedia.com https://www.investopedia.com/news/public-private-

permissioned-blockchains-compared/ (Accessed April 29, 2022)
[6] Accessed April 29, 2022. [Online]. Available: What are smart contracts on blockchain? | IBM
[7] Times, N. Y., 2021. Bitcoin carbon footprint electricity. [Online] Available at: https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html
[8] Gallersdörfer, U., Klaaßen, L. & Koll, C., 2020. Energy Consumption of Cryptocurrencies Beyond Bitcoin. Joule, pp. 1843-1846.
[9] P. W. Eklund and R. Beck, "Factors that impact blockchain scalability" in proceedings *11th international conference on management of digital ecosystems*. November 2019 pages 126-133. Available: Factors that Impact Blockchain Scalability | Proceedings of the 11th International Conference on Management of Digital EcoSystems (acm.org)
[10] Accessed April 29, 2022. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/whatis.html
[11] Accessed April 29, 2022. [Online]. Available: https://www.hyperledger.org/
[12] Accessed April 29, 2022. [Online]. Available: Ledger — hyperledger-fabricdocs master documentation
[13] Accessed April 29, 2022. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/create_channel/channel_policies.html?highlight=channel
[14] Accessed April 29, 2022. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/glossary.html?highlight=Organization#organization
[15] Accessed April 29, 2022. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/peers/peers.html
[16] Accessed April 29, 2022. [Online]. Available: Application — hyperledger-fabricdocs master documentation
[17] Accessed April 29, 2022. [Online]. Available: How to use Node.js to develop applications using Hyperledger Fabric - YouTube
[18] Accessed April 29, 2022. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.3/membership/membership.html
[19] Accessed April 29, 2022. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.3/orderer/ordering_service.html
[20] Accessed April 29, 2022. [Online]. Available: https://docs.docker.com/get-started/overview/#what-can-i-use-docker-for.
[21] Accessed April 29, 2022. [Online]. Available: https://www.docker.com/resources/what-container.
[22] Accessed April 29, 2022. [Online]. Available: https://github.com/prometheus/node_exporter
[23] Accessed April 29, 2022. [Online]. Available: https://grafana.com/docs/grafana/latest/introduction/
[24] E. Chinyati "Securing Internet of Things (IoT) devices using Hyperledger Fabric (Blockchain technology)" M.S. thesis, Dept. Computer Science University of Westminster September 7, 2020.
[25] M. Jedrzejczyk "Deployment of Hyperledger Fabric on ARM64 architecture" GitHub.com https://github.com/maciejjedrzejczyk/hlf-arm64 (Accessed April 29, 2022).
[26] J. Hedlin "Hyperledger Fabric binaries for AArch64/ARM64 (Raspberry Pi 2/3/4)" GitHub.com https://github.com/busan15/fabric-binaries-pi (Accessed April 29, 2022).
[27] Accessed April 29, 2022. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.3/test_network.html
[28] Accessed April 21, 2022. [Online]. Available: https://www.infoq.com/articles/arm-vs-x86-cloud-performance/
[29] H. H. Pajoof, M. Rashid, F. Alam and S. Demidenko "Hyperledger Fabric Blockchain for Securing the Edge Internet of Things" in *Sensors*, January 2021 [Online]. Available: https://www.mdpi.com/1424-8220/21/2/359/htm
[30] A. Sultan, M. A. Mushtaq and M. Abubakar, "IOT Security Issues Via Blockchain: A Review Paper" in *Proceedings of the 2019 International Conference on Blockchain Technology*, March 2019 pages 60-65 [Online] Available: IOT Security Issues Via Blockchain | Proceedings of the 2019 International Conference on Blockchain Technology (acm.org)
[31] A. Dabholkar and V. Saraswat, "Ripping the Fabric: Attacks and Mitigations on Hyperledger Fabric" in *Applications and Techniques in Information Security*, *10th International Conference*, 2019, pp. 300-311, doi: 10.1007/978-981-15-0871-4_24
[32] Rocha, A. de la and María Teresa Nieto, T. (2020). TrustID: A New Approach to Fabric User Identity Management – Hyperledger. Hyperledger.Org. Available: https://www.hyperledger.org/blog/2020/04/21/trustid-a-new-approach-to-fabric-user-identity-management
[33] Zhang, Kuan & Liang, Xiaohui & Lu, Rongxing & Shen, Xuemin. (2014). Sybil Attacks and Their Defenses in the Internet of Things. Internet of Things Journal, IEEE. 1. 372-383. 10.1109/JIOT.2014.2344013.
[34] Y. Hashem, E. Zildzic, A. Gurtov, "Secure Drone Identification with Hyperledger Iroha" in *Proceedings of the 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, November 2021, pp 11-18, doi: https://doi.org/10.1145/3479243.3487305