INTERNATIONAL JOURNAL ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 06th Feb 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=ISSUE-02

DOI: 10.48047/IJIEMR/V12/ISSUE 02/04

Title **Secure MQTT Protocol for Interoperable Exchange of Information using Block chain Network**

Volume 12, Issue 02, Pages: 32-38

Paper Authors

Y Ashwini, Byra Pardha Saradhi, Ravela. Chitti Babu

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Secure MQTT Protocol for Interoperable Exchange of Information using Block chain Network

Y Ashwini[1], Byra Pardha Saradhi[2], Ravela. Chitti Babu[3]
[1,2]Assistant Professor, Madanapalle Institute of Technology, Madanapalle.
[3]Assistant Professor, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur.

Abstract: The Internet of Things (IoT) has been evolving for more than a decade and it became a part of our daily life. The conventional used device is becoming more smart and autonomous due to the advancement of the technology. The connected devices are increasing exponentially, and it leads to the more security issues. Blockchain plays a crucial role to address these security related issues. Many people have realized that the use of blockchain is beyond the crypto currency. Some organizations, such as Ethereum and Rootstock, have built decentralized application platforms at the top of block Chain. These decentralized platforms also have the ability to run blocks of code, so there is a chance to create decentralized software programs. In this article, we discussed the various issues like inter operability and security issues in the current IoT infrastructure, and a detail literature survey in implementation of Blockchain using various approaches and their adaptation with IoT. This article is mainly focused for testing the capacity of ethereum blockchain to check the constrained equipment and it is possible to implement the management of the access management aspect whether it is globally or not. This is done through the implementation and evaluation of simplified block chains in Python. Finally we discussed the limitations and future scope of the proposed system.

Keywords: Internet of Things, Blockchain, MQTT, Etherium

Introduction

With the help of Satoshi Nakamoto, with the introduction of bit coin [11], block chain has now become almost 9 years. Many people have started catching the foundation of blockchain and have realized that the use of blockchain is beyond the crypto currency [5,16]. Some organizations, started building platforms to support decentralized applications at the top of block Chain. These decentralized platforms also have the ability to run blocks of code, so there is a chance to create decentralized software programs. In this we mainly focused on testing the capacity of etherium blockchain to check the constrained equipment and it is possible to implement the management of the access management aspect whether it is globally or not. Many simulation tools are available to simulate the block chain implementation and evaluation. In this paper we used the Python programming language and Contiki operating system to implement and evaluate the results.

Motivation

Current IoT systems rely on centralized or brocade models which require huge computational and storage capabilities. So the existing IoT system follows the client-server model, therefore the setup is expensive, due to high cost associated with cloud server infrastructure(s) and maintenance as well as other factors such as network equipment. Apart from this, there is no existing platform which supports communication between all devices, and there is also a lack of guarantee that the services provided by the mobile device manufacturers have been ered existing on the cloud [10]. While the client-server pattern plays an important role in connecting common devices with each other for decades, but not adequate to support the current challenges stemming from the growing development of the IoT economy. So using peer-to-peer decentralized communication approaches will not only reduce the cost of server clusters and maintenance costs, but will also share a large number of devices on the IoT network without sharing the processing and space requirements. No additional resources, Blockchain provides a solution that corresponds to the needs of such platforms [15]. Some of the problems like interoperability[12] and security, which are main concern in MQTT (Message Queue Telemetry Transport) protocol and where the Blockchain contributed are discussed below [9].

Literature Survey

Ethereum Blockchain for IoT

Bitcoin initially started Blockchain technology for its implementation, but Ethereum has practically worked as well. Ethereum allows developers to create their own decentralized contract where they specify rules, functionality and even a unique coin. Remember the explosion of ICOs in 2017? The equipment of Ethereum gave entrepreneurs the ability to make those unique cryptogens, on which a developer can create a unique crypto currency is a testament to the ethereum ecosystem, the developer community of ethereum and the Atrial block Chain. Computing power and storage requirements of conventional blockchains such as bitcoin and ethereum have been aborted. For example, specific atrial nodes use the GPU to process the block because the CPU is very slow and each block store is around 1TB of historical blockchian transactions. As the ethereum stands today, it is slow, expensive and energy-efficient compared to centralized cloud services. Viable data transport option to become consensus time and mining fee.

These issues have not been ignored by the leadership team of Ethereum. Over the years, core developers are working on a project called Casper. Casper will push Blockchain's consensus beyond a computational intensive operation called Proof-Off-Stack, a risk-based operation called Proof-Off-Work. Casper will have significant impact on the as per market. For IoT projects, the results will be positive because this transaction will reduce processing costs and allow computationally constrained devices to confirm the block. In May, Casper team released version 0.1.0 and seven days later version 0.2.0.

In January, the Ethreum[3] Foundation approved scaling issues by announcing two subsidy programs, where developers received a grant of $ 50,000 to $ 1,000,000 or more to work on the proposed solution. In particular, the foundation outlined two strategies, which they wanted to work in parallel - Blockchain Sharing and Layer-2 Protocol. Sharing will allow Ethereum's network of nodes to work on multiple blocks at once. In short, how does it alter MongoDB data in different partitions. The only project we have found working on sharing is prysmaticlabs.com. For IoT devices, sharing is another way, ethereum has widely planned to reduce the time of consensus. The Layer-2 protocol is usually defined as SideChains. Borrowing many features of Ethereum, these payments create an independent chain, where there are many data transactions in the Etherem series. After all, a sidechain will be remembered as the main ether block channel.

Typically IoT will create a scanning for constrained devices by the Sidechain data flow device → Sidechain → BlockChain where the MQTT Data Flow Client → Broker → Central Database. Using "broker" to interact with constrained devices, on the other end, the Sidechain sync on the "side" transaction set. Interval with main Ethereum series two remarkable Sidechain projects being developed are Raiden and Plasma.With a focus on the issue of so many ethereum-based projects and scale of developers, Ethereum can soon become a popular choice of conventional message queue + database architecture, together with a Sidechain.

IPFS for IoT

An exciting and currently practical implementation of Distributed Ledger Technology is the Interplanetary File System (IPFS). IPFS creates a distributed file system in independent nodes. IPFS can be used to host websites, files and even videos. IPFS nodes only store the content in which they are interested, in contrast to the traditional blockchains that need to be fully localized. IPFS may be very different from traditional blockchains, but are stored in multiple nodes in a network similar to cryptographic hashes. Claim of fame for IPFS is a bold suggestion that centralizes HTTP servers instead of IPFS used in the entire public Web. Each client has access to the full network of files. Client nodes can decide to store hash and if no nodes are disconnected in doing so, then the file is available through other nodes as if nothing happened. In addition to storage devices, this app exposes to developers, IPFS also exposes a Pub / Sub Event Bus similar to MQTTT. Unlike MQTT, there is no centralized broker, IPFS provides a fully decentralized and distributed broker. This means that every customer interested in an event also collectively works for broker event syndication for other interested clients. Then, there is also an added benefit of built-in cryptographic protection.

You can use the IPFS pub / sub all today, but you will quickly take part in this reality that IPFS needs nodes to opt-in to personal data. For this reason, large projects built on top of IPFS provided value by running the same project application to "network" of structures, libraries, and all nodes. A project built on IPFS Computes.io is. Founder, Chris Matthew wrote a blog post that was an IoT pub / sub instance using an Arduino last year - the creation of an IoT super computer. Super computer words can increase your eyebrows, but consider this demo where a brute force password attack is calculated using many computers.

Helium for Distributed Machine Network IoT

Helium is another startup that has attracted our attention on the hologram. They are building a decentralized machine network, which is a new word they are using to describe their product. Helium's network connects a physical block channel, wireless technology and open-source software specifically to create a distributed blockchain with IoT. When Helium announced its website for the first time a decentralized machine network: "IoT failed." Because of their logic protocols and proprietary technologies, IoT was not up to the promotion.The solutions they are developing include Gateway and low power wireless modules, which are called WHIP, using a new wireless protocol. At the top of it, he has created an incentive platform for working as a hotspot provider for individuals. The idea is that if you install a gateway and provide internet access to IoT devices, then you will earn crypto currency [15].

Helium also developed novel cryptographic evidence for the promotion and maintenance of its network. Rather than providing computerized cycles and electricity to some electric-hunger mining function instead of Gateway, Helium

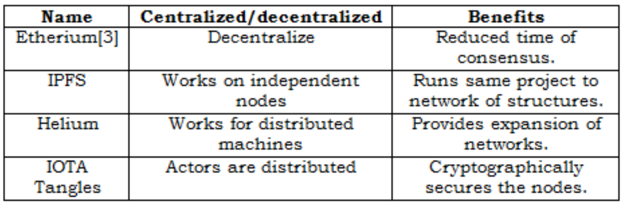
Gateway provides a realistic geographic area of expansion of its network, as has been verified by coverage proof of helium proof. The end result is that the gateway receives a reward for paying.Let's move through the helium network IoT machines will safely use the WHIP protocol for many local gateways within the range. Once joined, a device sends the encrypted data to all the gateways. At the end of each entrance block, the block adds to the global blockchain of helium. Data object will have forward sensor data about the router. Gateway sends data to specific router to provide this data transfer service, the gateway expects payment from the router.The router decrypts the data that completes the process. This explanation can be cumbersome as it is currently under development. We enumerate this process and weigh the better terminology.

IOTA tangle for IOT

Another technique that is available today is the IOTA. This project introduces its concept of a confused network rather than a network operated by the traditional Blockchain. Tangle is a new form of distributed accounting technology designed to keep Internet of Things in mind. Contrary to Blockchain, a tangle is a complex network of users rather than just miners nodes. The idea is that, for any device or user that does the transaction, it will also process the next two transactions [3]. This plan allows fast transactions with fees. IoT devices can also be used for sensor data or functionality. A fun claim from IOTA is safe against quantum computing-based attacks. This claim is impossible, the IOTA white paper runs through mathematics, they use "specifically the Quantum Resistant Cryptographic Algorithm", which reduces the effectiveness of some quantum attacks by 1 million.

In the future, where many city infrastructures is affected by the management and sensor networks and the actors are distributed, it is worth noting that the attack that spoils the identity or wrongly involves the datacan be frightening. A quantum-resistant cryptographically protected IoT network will help stop the life cycle attacks.

Comparison of all the technologies discussed above:



Name	Centralized/decentralized	Benefits
Etherium[3]	Decentralize	Reduced time of consensus.
IPFS	Works on independent nodes	Runs same project to network of structures.
Helium	Works for distributed machines	Provides expansion of networks.
IOTA Tangles	Actors are distributed	Cryptographically secures the nodes.

Existing Problems and Solutions

Is it possible to implement IoT device management, specifically in constrained devices, on blockchains, on a global level?

Blockchain's distributed replication model provides the ability to access and supply IoT information for clients as well as organizations, without the need for a central management server. Blockchain can also be used to pay for services or the usage of device resources is tracked in view of the terms already agreed.

What advantages does the use of blockchain bring to IoT?

The main advantage of using blockchain in transparency, privacy, non-repatriation, integration and confidentiality [7], IoT is that it is public and transparent; any person participating in the blockchain network will get an opportunity to see all the transactions and blocks. Parties involved in the transaction are private because they carry out transactions under their respective accounts, and their personal information is protected by their private keys. Blockchain technology includes hashing, to check the integrity of the information which is stored in blockchain.

Decentralization, reliable without blocking, has been decentralized, no central entity is involved in approving the transaction or certain transactions are set to accept the conditions. So it is a highly trusted network, and a consensus among all the participants is required to accept the transaction.

The most important thing, irreversible, it is safe from the view that once recorded data cannot be changed, and can act as a single source of truth. However, try to change the data for malicious nodes or deny that the transaction occurred. But in such a case, the malicious minor will be left behind, or discyncritions will be dropped from the network and in return will run to run its own small blockchain network, which will not be of any use to it.

Ability to track the history of data exchange, consistent with the data of each single IoT device is also an important implication of the cost of data tracking transactions and is highly beneficial when used in a prudent manner.

What are the caveats and challenges of using blockchains for management processes in constrained devices, specially considered at a global perspective, and how can they be mitigated?

There are some drawbacks to using blockchain for IoT.

Storage scalability is one of them, scalability issue. It includes aspects such as “bootstrap time”, “transaction cost”, “throughput”, “latency time” [CDE16]. Bootstrap timing refers to the time taken by a new full node to fully co-ordinate with BlockChain. Transaction cost involves the cost of resources, for which there is a condom remixed transaction.

Energy Consumption When a cryptocurrency occurs in its newborn stage, the resources needed to mine the currency are not very high. But when the level of Y cult of crypto currencies mining increases, then the miners have to resort to very powerful hardware, and as we know, the more operating hardware is a cience, the more energy consumes. . With the increase in mining fields around the world, blockchain mining has very little relation to stability.

MQTT[2] works with the help of a broker. If broker is not there, MQTT will not be able to transfer data from publisher to subscriber. Blockchain, on the other hand, connects everybody at the same place, with no extra password security and helps people communicate with each other in a more data secure way. We have done implementation of MQTT through Local Host as well as CloudMQTT [10]. On the local host, the commands include topic, a publisher and a subscriber. The flow of information from one end to the is shown over there. MQTT, when implemented with the cloud, can connect many devices to one another if sensor data and implementation on a wider scale is included.

In MQTT, for security, username and password are required while this is not the case of blockchain.In MQTT, data loss is a common issue, which is eliminated in blockchain technology.In MQTT, connectivity is a common issue. Blockchain works on blocks and helps connectivity by saving address of previous block in the next block.

How MQTT is implemented?

Step 1:
First of all, the MQTT[13] is implemented using Mosquitto MQTT, where direct communication of publisher and subscriber has taken place. The broker is sending data from the publisher to the subscriber. The message exchange is taking place with the help of broker and there are topics which have been subscribed from the subscriber.

Step 2:
The second step implementation has been done using CloudMQTT where the data exchange has been done using the cloud. The data, which is exchanged has been saved on the cloud and can be reviewed at any place of time. The drawback is, the protocol works for only low bandwidth devices.

Step 3:
The fake data of temperature sensors is processed and saved into the databases.

As MQTT usually works with implementation of sensors data, the data is processed, listened and implemented using MQTT protocol.

How blockchain is implemented?

Step 1:
As the execution of blockchain takes place, every block with a unique block number is generated.

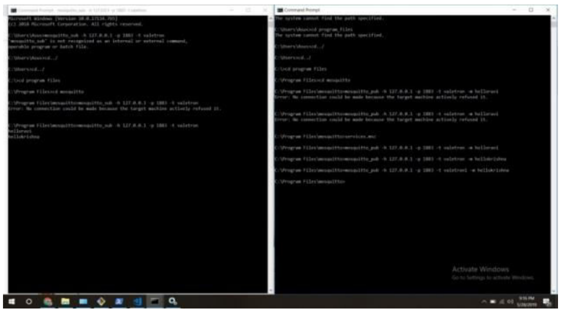
Step 2:
Every block has a unique hash which is used for security purpose so that if any data loss happens, the blocks are easily identifiable.

Step 3:
Every next block that is created, it contains the address of the previous block and that address of the previous block ensures the connectivity within each block at a certain point of time.

The blockchain implementation ensures that the data loss, which is a common issue visible in MQTT protocol has been eliminated and with that other issues have also been taken into consideration. For security purpose, hashes are there which ensures that any block can be identified if needed. In case of alteration of data, The new blocks are added behind the previous blocks and the address of the previous blocks is saved inside the next block because of which connectivity is ensured.

Implementations and Results:

Step 1:
Implementation of MQTT on a base level is done. In the first screenshot, the commands of MQTT[13,14] are executed which are showing direct data transfer with the help of a centralized broker. With data, the port number, the topic and the IP address are also associated so that data reaches the exact place. First, the subscriber subscribes to a topic, then the publisher publishes the data and then subscriber receives the data.



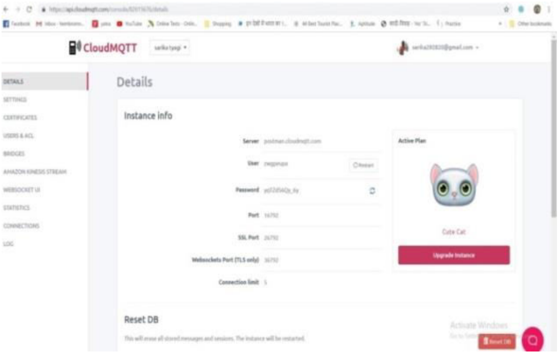
```
Microsoft Windows [Version 10.0.17134.765]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Asus>mosquitto_sub -h 127.0.0.1 -p 1883 -t valetron
'mosquitto_sub' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Asus>cd../

C:\Users>cd../

C:\>cd program files

C:\Program Files>cd mosquitto

C:\Program Files\mosquitto>mosquitto_sub -h 127.0.0.1 -p 1883 -t valetron
Error: No connection could be made because the target machine actively refused it.

C:\Program Files\mosquitto>mosquitto_sub -h 127.0.0.1 -p 1883 -t valetron
helloravi
hellokrishna
```

```
The system cannot find the path specified.

C:\Users\Asus>cd program_files
The system cannot find the path specified.

C:\Users\Asus>cd../

C:\Users>cd../

C:\>cd program files

C:\Program Files>cd mosquitto

C:\Program Files\mosquitto>mosquitto_pub -h 127.0.0.1 -p 1883 -t valetron -m helloravi
Error: No connection could be made because the target machine actively refused it.

C:\Program Files\mosquitto>mosquitto_pub -h 127.0.0.1 -p 1883 -t valetron -m helloravi
Error: No connection could be made because the target machine actively refused it.

C:\Program Files\mosquitto>services.msc

C:\Program Files\mosquitto>mosquitto_pub -h 127.0.0.1 -p 1883 -t valetron -m helloravi

C:\Program Files\mosquitto>mosquitto_pub -h 127.0.0.1 -p 1883 -t valetron -m hellokrishna

C:\Program Files\mosquitto>mosquitto_pub -h 127.0.0.1 -p 1883 -t valetron1 -m hellokrishna

C:\Program Files\mosquitto>
```

Activate Windows
Go to Settings to activate Windows.

Fig 1:Implementation of MQTT

Step 2:
The data transfer through CloudMQTT[10] is shown over here. In CloudMQTT, the data is saved in the cloud and can be accessed whenever needed. The port number, username and password in my case were auto-generated but when we work on a broader view, the id, password and other information are private to the users.



Details

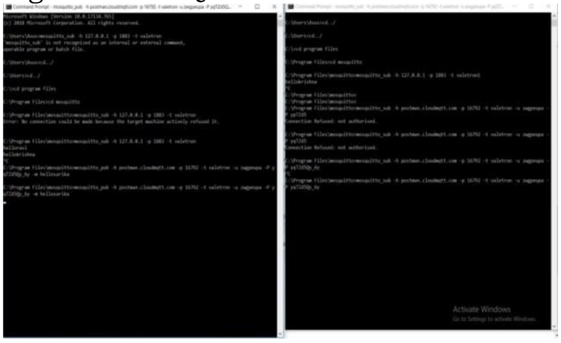
Instance info

Server postman.cloudmqtt.com
User zwgpnupa
Password yqT2d5Qy_6y
Port 16792
SSL Port 26792
Websockets Port (TLS only) 36792
Connection limit 5

Active Plan
Cute Cat

Reset DB
This will erase all stored messages and sessions. The instance will be restarted.

Fig 2: CloudMQTT account creation



```
Microsoft Windows [Version 10.0.17134.765]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Asus>mosquitto_sub -h 127.0.0.1 -p 1883 -t valetron
'mosquitto_sub' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Asus>cd../

C:\Users>cd../

C:\>cd program files

C:\Program Files>cd mosquitto

C:\Program Files\mosquitto>mosquitto_sub -h 127.0.0.1 -p 1883 -t valetron
Error: No connection could be made because the target machine actively refused it.

C:\Program Files\mosquitto>mosquitto_sub -h 127.0.0.1 -p 1883 -t valetron
helloravi
hellokrishna
^C
C:\Program Files\mosquitto>mosquitto_pub -h postman.cloudmqtt.com -p 16792 -t valetron -u zwgpnupa -P y
qT2d5Qy_6y -m hellosarika

C:\Program Files\mosquitto>mosquitto_pub -h postman.cloudmqtt.com -p 16792 -t valetron -u zwgpnupa -P y
qT2d5Qy_6y -m hellosarika
```

```
C:\Users\Asus>cd../

C:\Users>cd../

C:\>cd program files

C:\Program Files>cd mosquitto

C:\Program Files\mosquitto>mosquitto_sub -h 127.0.0.1 -p 1883 -t valetron1
hellokrishna
^C
C:\Program Files\mosquitto>
C:\Program Files\mosquitto>
C:\Program Files\mosquitto>mosquitto_sub -h postman.cloudmqtt.com -p 16792 -t valetron -u zwgpnupa -
P yqT2d5
Connection Refused: not authorised.

C:\Program Files\mosquitto>mosquitto_sub -h postman.cloudmqtt.com -p 16792 -t valetron -u zwgpnupa -
P yqT2d5
Connection Refused: not authorised.

C:\Program Files\mosquitto>mosquitto_sub -h postman.cloudmqtt.com -p 16792 -t valetron -u zwgpnupa -
P yqT2d5Qy_6y
^C
C:\Program Files\mosquitto>mosquitto_sub -h postman.cloudmqtt.com -p 16792 -t valetron -u zwgpnupa -
P yqT2d5Qy_6y
```

Activate Windows
Go to Settings to activate Windows.

Fig 3: Data Transfer through CloudMQTT

Step 3:
In the following screenshot, when we execute the code[6], Blocks are getting created, each block has its own block number, a block hash for the previous block and a hash for the current block. The previous block hash concept is there to ensure no data loss happening and for security purpose as well.

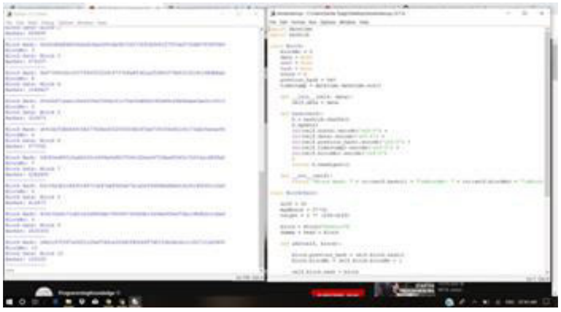


Fig 4: Creating the blocks using Etherium Blockchain

Future Scope and Conclusion:

Future work

There are so many limitations of MQTT which should be resolved. It is a very light weight protocol but then we know there is always a scope of improvement. The security obviously is a major issue and hence needed to be resolved. There is not much work done on Blockchain using hyper ledger because hyper ledger[1,4] is relatively a very new concept. MQTT along with hyper ledger has not yet been implemented and hence a major attention is needed to be thrown so that more acknowledgements can be achieved on the inter-relation of these two concepts. In my point of view, if hyper ledger will be implemented in even broad manner, using other protocols of IOT and MQTT as well, that will make the community of IOT even stronger. Hence there is still a vast area to work upon.

Conclusion

I hereby conclude that there are quite a few problems with MQTT,instead of it being a light weight protocol, there are so many points lacking which need to get improved. Hyper ledger Fabric[8], being a very new technology, needs a vast amount of research and work done. If MQTT is improved in terms of security, timeliness, efficiency and redundancy, it has to compromise in terms of its light weight and compact behavior. Hence it is being replaced with the help of IOT frameworks.The assessment also showed the limitations in the “proof of the concept system” implemented. Especially, scalability, energy consumption, cost and time of block generation was examined in detail. These issues need to be resolved in order to adopt Block system widely. blockchain technology has several advantages that can be leverage in a broad domain applications. The researchers are looking into the current challenges posed by difference applications and how can these challenges be overcome by blockchain especially in security related issues. Hope the blockchain will potentially change the way the system operates currently in the world.

References

[1]. https://espeoblockchain.com/blog/a-practical-guide-to-hyperledger-fabric-security/

[2]. https://hologram.io/iot-platforms-should-be-planning-blockchain-integrations/

[3]. https://merehead.com/blog/comparison-ethereum-hyperledger-fabric-r3-corda/

[4]. https://hyperledger-fabric.readthedocs.io/en/latest/build_network.html

[5]. https://blockgeeks.com/guides/what-is-blockchain-technology/

[6]. https://coinnewstelegraph.com/yes-you-can-put-iot-on-the-blockchain-using-python-and- the-esp8266-hackaday/

[7]. https://www.ibm.com/blogs/blockchain/2018/04/hyperledger-fabric-enables-confidentiality-in-blockchain -for-business/

[8]. https://blockchain-fabric.blogspot.com/

[9]. https://espeoblockchain.com/blog/pros-cons-blockchain-advisor

[10]. https://espeoblockchain.com/blog/cloud-blockchain-infrastructure/

[11]. https://www.clearias.com/blockchain-technology/

[12]. Christopher Ferris “https://www.ibm.com/blogs/blockchain/2018/10/blockchain-interoperability-i-do-not-think-it-means-what-you-think-it-means/” on Oct 22,2018

[13]. https://www.hivemq.com/blog/mqtt-security-fundamentals-tls-ssl/

[14]. https://www.infoq.com/articles/practical-mqtt-with-paho/

[15]. https://www.coindesk.com/information/applications-use-cases-blockchains