BRIEF SURVEY AND TESTBED DEVELOPMENT FOR BLOCKCHAIN BASED INTERNET OF THINGS

by

Aishwant Ghimire

A thesis submitted to the faculty of The University of Mississippi in partial fulfillment of the requirements of the Sally McDonnell Barksdale Honors College.

Oxford

Dec 2019

Approved by

Wang Feng

Advisor: Dr. Feng Wang

Reader: Dr. Philips Rhodes

Reader: Dr. Charles Fleming

Acknowledgement

First and most of all I would like to thank Dr. Feng Wang for his advice, guidance, and patience throughout the process of writing this thesis. His motivation and sincerity have deeply inspired me to write this thesis. I would also like to thank my committee members Dr. Philip Rhodes and Dr. Charles Fleming for their encouragement, support, suggestion, and instruction. Without their help, this thesis would not have been possible.

Second, I would like to thank Sally McDonnell Barksdale Honors College for giving me a wonderful opportunity to write this thesis. I would like to extend my sincere acknowledgment to the exceptional faculty in the Computer Science department for the past amazing four years here in the University of Mississippi. I would also like to thank my family. My dad, mom, and sister despite the distance, always encouraging me with their wise word to strive for success.

Last, of all, I would like to thank my friends for sticking with me throughout this project. I would like to thank them for their love and support. They all kept be going for the completion of this project.

Abstract

Blockchain and the Internet of Things are uprising in today’s technology world. Internet of Things or IoT are the devices with unique identifiers that share data or information over the internet whereas, Blockchain is a peer to peer network with a distributed ledger that contains a list of blocks that are linked together by cryptography. Fascinated and motivated by blockchain and Internet of Things (IoT), this thesis provides a review on blockchain based internet of things and also introduces a working testbed that integrates the two together. It also uses IoT device to invoke transactions into the blockchain. The reasons behind combining of blockchain and IoT is because the present centralized architecture won’t hold the exponentially growing use of IoT, blockchain implementation can reduce cost and moreover, decentralization will remove the bottleneck from the centralized server.

Table of Contents

LIST OF FIGURES

1 INTRODUCTION

Blockchain and the Internet of Things are two buzz words in today's tech-savvy world. Many have heard of these terms but only some are familiar with it. IoT development and usage is increasing exponentially to meet the necessity of today's technological world. The number of connected devices at the end of 2018 was 22 billion worldwide and is expected to reach 38.6 billion by 2025 and 50 billion by 2030 [1]. Internet of Things or IoT are the devices with unique identifiers that share data or information over the internet. The devices include wearable watches, wireless sensors, RFID scanners, LED lights, body sensors, etc. These devices have made our daily lives a lot easier. Similarly, blockchain, the technology behind many big cryptocurrencies like Bitcoin, Ethereum and Litecoin has made researchers and big companies interested in its advantages. It was first introduced in Bitcoin by Satoshi Nakamoto in 2008 and since then it has been adopted in many other blockchain technologies. Blockchain is a peer to peer network with a distributed ledger that contains a list of blocks that are linked together by cryptography. The first block in a blockchain is called the genesis block. Each block has transaction data, the hash of its block, hash of its previous block, its index in the chain and timestamp. However, the previous hash in the genesis block is null [2]. Blockchain does not permit alteration and the addition of the data to the chain requires consensus from all of the nodes participating in the network. This helps the technology to track and coordinate transactions. The technology can manage a large number of devices that can eliminate the dependency of IoT on a centralized cloud and promote the creation of applications for the integrated system [3]. Due to the increasing fascination and curiosity in blockchain-based internet of things, this thesis provides a review on both the systems, as to why the systems should be integrated and also an overview of the testbed created to implement the systems together.

2 BACKGROUND AND MOTIVATION

2.1 IoT

‘Internet of Things' or IoT is combined from two words, "Internet" and "Things". The ‘internet’ is a global system of an interconnected network of computers that follows a standard Internet Protocol Suite (TCP/IP). This network consists of public, private, academic, business, and government networks, of local to global scope, that is interconnected by a wide range of electronic, wireless and optical networking technologies. Things are the devices or sensors that have Unique Identifiers (UIDs) and can share their data through the internet without any human to human or human to computer interactions [4]. IoT has brought technological uprising and can be considered the future of computing and communication. It has stroke bigger interests in both business and research. Some application includes smart home appliances, personal assistants like Amazon Echo, Google Home, Apple Home Pod.

2.1.1 Applications of IoT devices

IoT has been applied in many different fields. Some applications are:

- Different health monitoring IOT devices for patients which work remotely to provide data. [5]
- Systems like vehicle monitoring gives live feedback of the vehicle movement and track its performance. [6]

- Smart Exam based IOT that provides a system to take exams provide analytic on student's performance and help access student's disability to attempt exam questions. [7]
- Surveillance [8]

2.1.2 Communication

Within IoT, different types of the communication might exist, which embody device-to-device (D2D), device-to-human (D2H) and vice versa. Communication can be among intradomain or interdomain networks that are either the same network or completely different heterogeneous networks, respectively. Moreover, communication between devices can be a single hop or multiple hops. In single-hop, a base station or an access point is responsible for communication between devices. In multiple hops, relay of information between devices takes place within each other without the help of centralized control and therefore an end to end communication between source and destination is achieved. The network for the devices to operate is called constrained and unconstrained networks. The constrained networks involve short-range wireless networks, low-power networks, delay tolerant networks, and wireless sensor networks. [9] The devices in this network operate in the unlicensed spectrum. Unconstrained networks consist of high coverage range and capacity which involves cellular network (Wireless Wide Area Network) and WiMAX (Worldwide Interoperability for Microwave Access). The devices in this network operate in the licensed spectrum. [10] Wireless Personal Area Network (WPAN) is designed for near range communication and is the main method of connecting sensors to the IoT.

WPANs include different communication technologies like Bluetooth, Zigbee, Z-Wave, IEE 802.15.4-based networks.

2.2 Blockchain

Blockchain was first introduced in 2008 by Satoshi Nakamoto's white paper as a peer to peer electronic system [2]. The blockchain is a distributed peer to peer network with a digital ledger that holds past transactions. A transaction is the exchange of information among the different peers which is broadcasted to the network. The transactions are then stored in blocks in chronological order, and every block contains a hash of the previous block creating a chain of blocks. The first block does not contain the hash of the previous block and is called the genesis block.

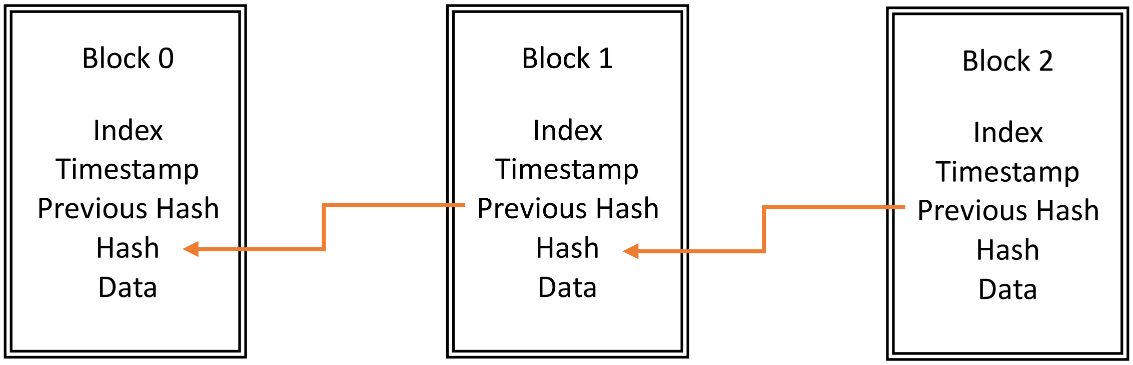

Fig 1: Structure of Blockchain

2.2.1 Types of Blockchain

- **Public Blockchain:** Blockchains like Bitcoin and Ethereum are distributed networks which runs through a native token. They have open-source code which is maintained by their community and are open to anyone to participate. The participants in the network are anonymous [11].
- **Permissioned Blockchain:** Blockchains like Hyperledger and Ripple have control to what individuals can function in the network. They are also a distributed network which may use native token. They may or may not have open-source code. The participants in the network are not anonymous [11].
- **Private Blockchain:** Blockchains like SoluLab and Eleks are similar to permissioned blockchain but do not use native token. The membership is closely controlled. These blockchains are only used among businesses that have trusted members where trade highly confidential information. The participants in the network are not anonymous [11].

2.2.2 Features of Blockchain

- **Smart Contract:** One of the main features of blockchain is Smart Contract. A smart contract is an application that is applied on the blockchain network and can execute automatically as part of transaction validation [12]. Contracts are code that serves as programmed agreement between the participants [13]. It also helps in credible transfer assets from one party to another under certain conditions
- **Consensus:** A mechanism that necessitate all the participants in the chain to mutually agree on a given value required for computational purposes. Blockchain

can use numerous algorithms for consensus which include proof of work (PoW) or proof of stake (PoS) [14].

- **Distributed Ledger:** All the participants in the blockchain network has a copy of the ledger which holds information about the blockchain, transactions and configuration and policy updates [14].
- **Security:** Data integrity is preserved as data cannot be altered or tampered once committed to the network. Moreover, data is tied together cryptographically, and data cannot be accessed by unauthorize users [13] [14].

2.2.3 Application of Blockchain

Some major applications of blockchain are:

- **Cryptocurrency:** Blockchain was first introduced by Bitcoin, a cryptocurrency which is widely used today. More and more cryptocurrencies have started adopting blockchain and have excelled in the crypto market.
- **Business:** Different companies like IBM has implemented blockchain in supply chain. Hyperledger fabric is being used in their project heavily because of the unique approach to consensus which is faster but also preserves privacy [15].
- **Entertainment:** Blockchain has also been used in the field of entertainment. KickCity is a blockchain-powered marketplace where influencers get paid for recommending events. B2Expand is a gaming company that develops games using Ethereum. Their first game “Beyond the Void” was the first on steam with crypto currency.

3 INTEGRATE BOTH TOGETHER

3.1 Why Integrate Blockchain into IoT

The IoT ecosystems is growing day by day. The number of connected devices is expected to reach 38.6 billion by 2025 and 50 billion by 2030 [1]. The enormous amount of IoT devices connected to the internet is going to very difficult to handle with a centralized architecture. These cloud infrastructures require lots of investment to run and let alone manage that number of devices will cost a fortune. These can be eliminated with blockchain that helps connect devices in a peer to peer decentralized network. The devices can communicate with one another securely, use smart contracts to execute instructions. Moving to a more decentralized blockchain platform will also benefit IoT as there is no single point of failure whereas centralized cloud servers could be down sometimes due to software bugs, cyberattacks, power faults or other problems [16]. When frequent updates and control queries, a standalone centralized access control server could be a bottleneck. Adopting blockchain, the need for centralized access control management can be eliminated and different advantages like mobility, accessibility, concurrency, lightweight, transparency and scalability can be achieved [14]. Here, instead of connecting all the devices to a central server, the devices get distributed to the peers (servers) in the network thus making it more decentralized. Here, the participants for the network are the IoT devices and the peer servers. However, we look more into making the IoT device connection secure, decentralized and scalable.

3.2 Brief survey on State of Art

Some examples that include the integration of the systems together are:

- [17] uses **Ethereum to manage and configure different IoT devices**. The keys are managed using RSA where the private keys are stored on the device and the public keys are stored on the blockchain. Three different Raspberry Pis are used to simulate the IoT devices and a smart phone is used for the user to set up policies. When the user sets up the policies the data is recorded into the Ethereum network. Moreover, the devices are receiving policies periodically from the network. The policies are first check for digital signatures examine if the source was correct.

Fig 2: Devices connected to Ethereum [17]

- [18] uses **Ethereum for ownership management of medical IoT devices (MIoTs)**. The system contains of manufacturer, IoT devices, and smart contract for manufacturer and IoT devices is written. The smart contract for manufacturer is used to deploy smart contract for IoT device when a new device is manufactured. The smart contract on the network also provide the owner with choice for transferring ownership of the MIoT without any third a centralized entity. The contract also enables the device owner the right to change rules and policies of the device.

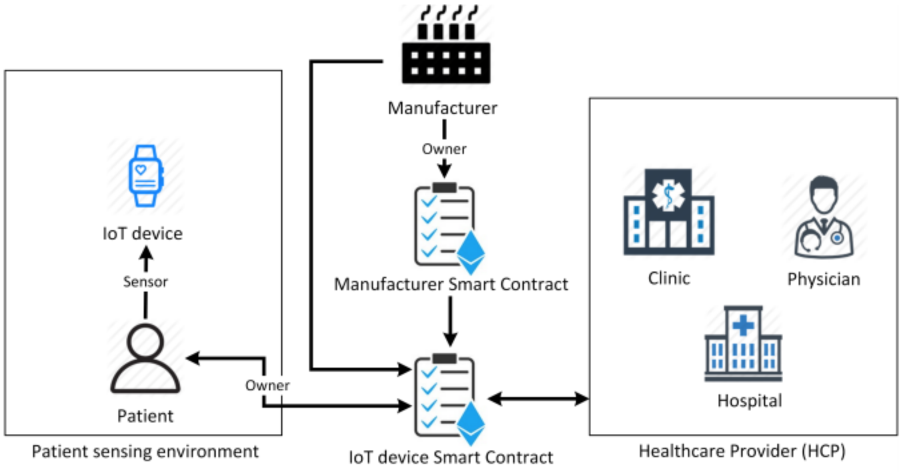
Manufacturer
Owner
Manufacturer Smart Contract
IoT device
Sensor
Patient
Owner
Patient sensing environment
IoT device Smart Contract
Clinic
Physician
Hospital
Healthcare Provider (HCP)

Fig: 3 System Overview of Ownership Management for MIoT devices

3.2.1 Discussion:

Both examples provide a very good implementation of blockchain based IoT systems using Ethereum. Both have the use of encryption to authenticate the device and store data. [17] uses digital signatures to store and retrieve policies whereas [18] uses digital signatures to authenticate and send data. Accountability is an issue for the first example when scaled to larger domains as there is no way to know what IoT device was responsible for what data. However, in the second example, each entity is assigned an address that takes accountability. Moreover, the transaction speed can get slower with the addition of more devices. Furthermore, the limitations in both the system are scalability, privacy, and confidentiality. When more devices are added to the network, the transaction speed will get slower with more communication. The traffic increases with the increase in devices. Also, the data and information in both the system are accessible by everyone participating in the network which is a major problem.

The first examples couldn't account for their limitations and thus, a better approach to address the limitation was needed. This bought forth the testbed development.

4 TESTBED DEVELOPMENT

4.1 Motivation

With the growing development of IoT and blockchain technologies as mentioned in the sections 2 and 3, very less resources can be found that incorporates the two technologies in one. The examples in section 3 account for most of the issues of a centralized server however scalability and confidentiality are the issues. The resources presented does provide some knowledge to how the system functions but a practical tool to observe the process and mechanism behind the system is not present. This testbed provides an overall view and tools to observe how the systems integrate together, and accounts for privacy and confidentiality issues in the previous approaches with a sketch of the network infrastructure and architecture.

4.2 Objective

The objective for this research was to create a testbed for a permissioned blockchain that provide connections for IoT devices and read the transactions to update the ledger with confidentiality in mind. The link is achieved through a proxy server created to read the data sent from the IoT device and in return act as a client and send data to the peer connected to the blockchain network. The reasons behind using Hyperledger fabric over the traditional blockchain like Bitcoin or Ethereum is because fabric is a permissioned blockchain, provides identity and has a very less resource consuming algorithm named selective endorsement whereas public blockchains prefers anonymity and has a very high resource consuming algorithm named proof of work or proof of stake.

4.3 Technologies Used

The technologies that were used in this development are:

- **Ubuntu Linux:** It is a free and open-source Linux distribution software package that powers an operating system providing an environment to run different applications. [19] Ubuntu is the development and deployment environment. The version of the software used is 18.04 LTS.
- **Hyperledger Fabric:** It is an open-source framework for building permissioned based blockchain applications. It provides confidentiality, resiliency, flexibility and scalability and enables solutions for variety of industries. It also allows plug and play membership services and consensus mechanism and uses Docker container to hold smart contracts termed as “chaincode” to provide logic for the application and the entire network. [20] The version of fabric used is 1.4.
- **Docker:** It provides Operating System level virtualization to deliver software in packages called container. The container can communicate with another through channels and each container can have their own packaged software, set of libraries and configuration files. [21] The version of docker used is 19.03.5. Each peer, orderer and chaincode run independently inside a container.

- **Node JS:** It is an open-source, asynchronous event-driven JavaScript runtime environment that can executes JavaScript code and build scalable network applications. [22] The version of node used is 8.16.1. The chaincode and the proxy server is written in JavaScript and compiled and run by this environment.
- **Git:** It is a version control system that helps track and record changes in the source code. The software helps keep track of all the changes made during development and also revert back to a specific version of the code if needed.

4.4 Network Architecture

Hyperledger fabric architecture consist of several important features such as [23]:

- **Fabric ledger:** It stores information about the blockchain, transactions and channel configurations. The ledger further is divided into world state ledger and blockchain ledger. The world state is a database that stores present values of set of ledger state. This makes it easier to run queries in the network. The blockchain ledger keeps log of the transactions and queries that takes place in the world state ledger.
- **Nodes:** Fabric has three separate nodes which are peer, endorsing peer and ordering node. The peer maintains ledger and commits transaction. The endorsing peer receives transaction proposal and endorses transaction either by permitting or rejecting endorsement. The ordering node is responsible for communicating with endorsing nodes and approval of transaction inclusions from peers. For testing purpose, only one ordering node is used.
- **Consensus:** The consensus in hyperledger fabric is not resource constraining. Once the transactional proposal is endorsed by the peers then the orderer validates for the

required endorsements and upon communication approves the transaction inclusion and thus, consensus is reached.

- **Chaincode:** Chaincode are smart contracts that is applied on the blockchain network and can execute automatically as part of transaction validation. It is also the logic to what data are queried or invoked in blockchain.
- **Channels:** It provides privacy between two or more specific network member and helps in conducting separate confidential transactions. An organization can be a part of multiple channels. Each channel has different sets of chaincode.
- **Fabric CA:** It is the optional default Certificate Authority (CA) which issues E-certs (a long-term identity to the participants)
- **Membership Service Provider:** It is responsible to manage set of identities inside a the blockchain network. The identities once issued by CA is provided to the peer, orderers, client applications and administrators. There can be multiple MSPs within a network but 1 per organization.

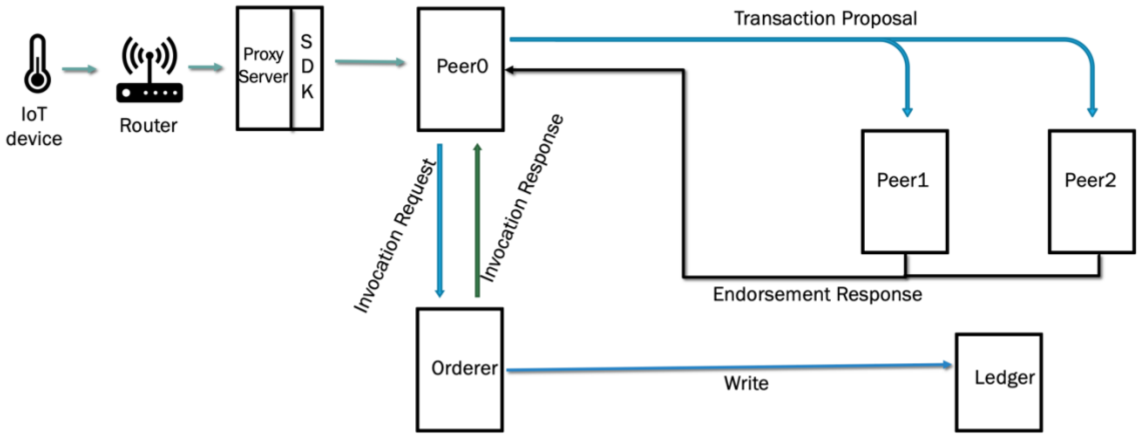

Fig2: Network architecture and transaction flow

4.5 Implementation

The blockchain network in the testbed consist of two organization, Org1 and Org2, respectively. Each organization contains two peers that is peer0 and peer1 where peer1s are the anchor peers which act as the bridge between two organizations. Therefore, the different nodes here on respective to their organizations are, peer0.org1.biot.com, peer1.org1.biot.com, peer0.org2.biot.com and peer1.org2.biot.com. Here, the biot.com is the name of the whole blockchain which could be changed if need be. For testing purpose, using docker, the peers are running into localhost, but the containers separate them from one another. Thus, acting as separate domain servers with their own set of configurations.

The IoT device used in the testbed is a wemos d11 mini device that records temperature in Celsius, temperature in Fahrenheit and humidity. A simple router is set up to receive the data from the IoT device and direct it to the proxy server which is running on localhost.

The startNetwork.sh script is used to bring the network online. The script first runs a generate certificates script which creates certificates for the orderers and peers in the organizations. Then it creates different docker container with the help of certificates created and the configuration yaml files that has configurations for each container.

Once the whole system is online, the admin certificates are used to enroll the admin to a specific organization. These certificates are issued by the CA servers which is running in a separate container named as ca0 and ca1. The issued certificates then are provided to the peers by the organization's respective MSP. Then the register script registers the user1 certificates with the admin certificates. The user1 certificates are used by the proxy server to invoke the data from the IoT device.

4.6 Transaction Flow

Explaining Fig1, the IoT device generates data periodically and it directs the data to the IP address of the proxy server with the help of the router. Once received, the proxy server reads the data and runs the invoke chaincode script which sends a transaction proposal to other peers or organizations in the same channel. The endorsing peers endorse the data upon checking the certificates provided by the peer handling the proposal. Once, the endorsement response is received by the peer it sends an invocation request to the orderer. The orderer upon communicating with endorsing nodes, approves the request and sends the response back to the peer and also updates the ledger.

5 CONCLUSION AND FUTURE WORKS

In this thesis, the blockchain and internet of things are surveyed with further explanation on the combination of the systems and development of testbed is introduced. The integration of the systems will make the IoT architecture more decentralized which removes the huge payload on a centralized server. This will also cut down the expenses for maintaining huge data centers. The examples of the two systems working jointly are discussed in section 3.2 which provides foundation knowledge for the testbed creation. However, there are some limitations in the approach such as processing time, cryptocurrency fees, high resource consumption, scalability, and confidentiality. These limitations motivated the development of testbed. The testbed solves most of the shortcomings with the consensus mechanism but mainly privacy is what we accounted for with the testbed.

The future work for this testbed has a series of updates that will involve scaling at more dynamics, enhancing capabilities, and a user interface for easier access. At the current state, we focused more on confidentiality however, with the further resource we will be looking into the scalability of the developed testbed. The scalability will be further divided into three different levels such as IoT devices, peer servers, and channels. To sum up, the combination of blockchain and IoT will provide more immutability, transparency, and security.

BIBLIOGRAPHY

[1] "Strategy Analytics: Internet of Things Now Numbers 22 Billion Devices but Where Is the Revenue?" Strategy Analytics: Internet of Things Now Numbers 22 Billion Devices but Where Is the Revenue? | Strategy Analytics Online Newsroom, 16-May-2019. [Online]. Available: https://news.strategyanalytics.com/press-release/iot-ecosystem/strategy-analytics-internet-things-now-numbers-22-billion-devices-where.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[3] T. M. Fernandez-Carames and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," IEEE Access

[4] Madakam, S., Ramaswamy, R., and Tripathi, S., "Internet of Things (IoT): A Literature Review." Journal of Computer and Communications, Scientific Research Publishing, 2015.

[5] D. Minoli, K. Sohraby, and B. Occhiogrosso, "Iot security (iotsec) mechanisms for e-health and ambient assisted living applications," in 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), July 2017, pp. 13–18.

[6] S. Wang, Y. Hou, F. Gao, and X. Ji, "A novel iot access architecture for vehicle monitoring system," in 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Dec 2016, pp. 639–642.

[7] Xheladini, S. Deniz Saygili, and F. Dikbiyik, "An iot-based smart exam application," in IEEE EUROCON 2017 -17th International Conference on Smart Technologies, July 2017, pp. 513–518.

[8] K. Gupta and R. Johari, “Iot based electrical device surveillance and control system,” in 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), April 2019, pp. 1–5.

[9] O. Bello and S. Zeadally, “Intelligent device-to-device communication in the internet of things,” IEEE Systems Journal, vol. 10, no. 3, pp. 1172–1182, Sep. 2016.

[10] O. Bello, S. Zeadally (2013) Communication Issues in the Internet of Things (IoT). In: Chilamkurti N., Zeadally S., Chaouchi H. (eds) Next-Generation Wireless Technologies. Computer Communications and Networks. Springer, London

[11] T. Laurence, “Blockchain for dummies. John Wiley Sons,” 2017.

[12] D. Fakhri and K. Mutijarsa, “Secure iot communication using blockchain technology,” in 2018 International Symposium on Electronics and Smart Devices (ISESD), Oct 2018, pp. 1–6.

[13] M. Swan, Blockchain: Blueprint for a New Economy, 1st ed. O’Reilly Media, Inc., 2015.

[14] O. Novo, ‘‘Blockchain meets IoT: An architecture for scalable access management in IoT,’’ IEEE Internet Things J., vol. 5, no. 2, Apr. 2018

[15] “Now Arriving: IBM Blockchain for Supply Chain” IBM, [Online]. Available: https://www.ibm.com/blockchain/industries/supply-chain

[16] N. Kshetri, “Can Blockchain Strengthen the Internet of Things”, IEEE Computer Society.

[17] S. Huh, S. Cho, and S. Kim, “Managing iot devices using blockchain platform,” in 2017 19th International Conference on Advanced Communication Technology (ICACT), Feb 2017, pp. 464–467.

[18] M. Alblooshi, K. Salah, and Y. Alhammadi, “Blockchain-based ownership management for medical iot (miot) devices,” in 2018 International Conference on Innovations in Information Technology (IIT), Nov 2018, pp. 151–156.

[19] "The story of Ubuntu," Canonical, [Online]. Available: https://ubuntu.com/about.

[20] "An Introduction to Hyperledger," [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf.

[21] "What is Container," Docker, [Online]. Available: https://www.docker.com/resources/what-container.

[22] “About Node.js,” NodeJS, [Online]. Available: https://nodejs.org/en/about/

[23] “Key Concepts,” Hyperledger Fabric, [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/key_concepts.html