ETHEREUM BASED BLOCKCHAIN IMPLEMENTATION IN HOME AUTOMATION FOR DECENTRALIZED DEVICE TO DEVICE COMMUNICATION

SARAVID A/L SUCHAAD

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Master of Philosophy

Malaysia-Japan International Institute of Technology
Universiti Teknologi Malaysia

SEPTEMBER 2022

DEDICATION

This thesis is dedicated to my lost brother, Darid Char who always looks up to me and accompany me. Also, to my father, mother, siblings, my love, and friends who gave me support through and through again directly or indirectly.

ACKNOWLEDGEMENT

In preparing this thesis, I was running into a lot of undesired situations which that had bring me down many times. Thanks to my supervisors, Prof. Koichiro Mashiko, Dr. Ooi Chia Yee and Madam Nordinah Bt. Ismail that always support me despite my shortcomings. They have encouraged me to keep me strong to fight. For me, they are my guardians during my stay in the university. Thanks to my fellow lab members for their support and comments which helping me out direct or indirectly.

My highest gratitude to my lost brother, Darid Char always accompanied with many online chats during my stay in university. You had kept my fire glowing. Thanks to my family and my love who always believe in me. Finally, thanks to all my friends for keeping cheering for me both direct and indirectly.

ABSTRACT

Home automation recently started becoming a commodity due to the advancement of computer design and manufacturing, making it cheap for common folks. Home automation devices allow home appliances, such as television, air conditioner and refrigerator, to be connected to the internet; providing innovative and smart services to humans. Many state-of-the-art IoT is highly centralized and not necessarily suited for home IoT because of the difficulty of scaling, the many-to-one nature of traffic, and the single point of failure. Centralization also forces us to trust the provider of a service. As for smart home devices, it is more trivial to protect and secure our privacy at home, which is very private and personal. To guarantee a completely trusted, transparent environment, we propose a blockchain decentralized solution for smart homes. The advantageous features of Blockchain are decentralization, anonymity, and security. These can be beneficial to IoT, adding more security layers and relieving dependence on the central server. However, as evident from the operation of Bitcoin businesses, existing Blockchain cannot directly be applied to IoT applications expected from homes or industries because of real-time operation and memory consumption. Therefore, a decentralized Ethereum-based private home automation platform with sufficient real-time performance for home use is needed. In this research, the implementation of blockchain for home automation using Ethereum is developed as an intermediary for data exchange between home devices. To fit various types of device computing power, the node is configured as an active node and a passive node while still maintaining the decentralized communication between devices. Using a private blockchain, the private operation and data of the user are confined between user IoT devices and maintain speed. The developed scheme IoT operations, memory consumption and real-time operation by measuring one-way communication are compared to a centralized scheme made using MQTT protocol and is shown to be competitive in terms of speed with just 7ms slower in latency. However, it comes with a drawback, in which its storage memory usage expands for every 3-4 transactions; yet with future improvement such as routine storage clean-up this shortcoming can be overcome. Finally, some recommendations and future works are laid out to improve the performance and pave a road to guide future blockchain research related to home automation and IoT.

ABSTRAK

Kebelakangan ini, rumah automasi semakin menjadi satu komuditi. Hal ini kerana kepesatan dalam reka bentuk and pembuatan komputer menjadikan ia lebih mampu dimiliki. Peranti rumah automasi membolehkan perkakas rumah (seperti televisyen, penghawa dingin dan peti sejuk), disambungkan ke Internet dan menyediakan perkhidmatan yang inovatif dan pintar kepada manusia. Kebanyakan sistem keselamatan yang canggih tertumpu kepada satu pusat (pemusatan atau *centralized*) dan tidak sesuai untuk IoT kerana kesukaran dalam pembesaran saiz, sifat trafik yang banyak-ke-satu dan satu pusat kegagalan. Pemusatan juga menyebabkan pengguna perlu untuk mempercayai pembekal perkhidmatan. Bagi peranti rumah pintar, adalah lebih penting untuk melindungi privasi di rumah. Untuk menjamin persekitaran yang telus dan boleh dipercayai sepenuhnya, kami mencadangkan penyelesaian desentralisasi (komunikasi terpencar atau *decentralized*) mengunakan *Blockchain* untuk rumah pintar. Kelebihan ciri *Blockchain* ialah desentralisasi, anonim dan keselamatan. Ini boleh memberi manfaat kepada IoT, menambahkan lebih banyak lapisan keselamatan dan tidak perlu bergantung pada pelayan pusat. Walau bagaimanapun, seperti yang terbukti daripada operasi *Bitcoin*, *Blockchain* yang sedia ada tidak boleh digunakan secara terus pada aplikasi IoT yang digunakan dari rumah atau industri kerana operasi secara lansung dan penggunaan memori. Dalam penyelidikan ini, *Blockchain* menggunakan *Ethereum* direka untuk pengautomatikan peralatan rumah sebagai medium penghantaran data antara peralatan. Untuk memastikan keserasian dalam operasi dalam pelbagai jenis pengkomputeran peranti besar dan kecil, nod ditetapkan sebagai nod aktif dan nod pasif tetapi masih mengekalkan komunikasi desentralisasi di antara peranti-peranti. Dengan menggunakan *Blockchain* peribadi, operasi privasi dan data pengguna dihadkan antara peranti IoT pengguna dan mengekalkan kelajuan pertukaran data. Operasi, penggunaan memori dan operasi secara langsung dibandingkan dengan skim berpusat yang menggunakan protokol MQTT. Skim yang direka menunjukkan hasil kompetitif dari segi kelajuan dengan hanya 7ms lebih perlahan. Walau bagaimanapun, skim ini datang dengan kelemahan iaitu penggunaan memori storan semakin berkembang untuk setiap 3-4 transaksi, tetapi ini boleh diatasi dengan pembersihan storan rutin. Akhir sekali, beberapa cadangan akan dibentangkan untuk meningkatkan prestasi dan membimbing penyelidikan *Blockchain* di masa hadapan yang berkaitan dengan sistem automasi rumah dan IoT.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

API	-	Application Programming Interface
ASIC	-	Application Specific Integrated Circuit
DAG	-	Directed acyclic graph
DNP3	-	Distributed Network Protocol 3
DTLS	-	Datagram Transport Layer Security
FOSS	-	Free and Open-source Software
GETH	-	Go-Ethereum
GPIO	-	General-Purpose Input Output
IoT	-	Internet of Things
ISP	-	Internet Service Provider
JSON	-	JavaScript Object Notation
MQTT	-	Message Queuing Telemetry Transport
NAT	-	Network Address Translation
P2P	-	Peer-to-Peer
PBFT	-	Practical Byzantine Fault Tolerance
POA	-	Proof of Authority
PoW	-	Proof of Work
PyPI	-	Python Package Index
QoS	-	Quality of Service Levels
RAM	-	Random Access Memory
SPV	-	Simplified Payment Verification
TCP/IP	-	Transmission Control Protocol/Internet Protocol
UDP	-	User Datagram Protocol
UID	-	User interface device
VM	-	Virtual Machine

LIST OF SYMBOLS

T	-	Time
Σ	-	Sum of

CHAPTER 1

INTRODUCTION

1.1 Background

Since services over the internet and cloud become versatile and inexpensive, the Internet of Things (IoT) seems to be widely utilized in our society and daily lives. Almost everything revolves around automation, data exchanges, cloud, cyber-physical systems, robots, Big Data, AI and semi-autonomous industrial techniques that further motivates the generations of research and development of IoT devices and services [1]. Some reports predicted that there might be up to 29 billion connected devices by 2022 with 16 billion of are short-range devices [1]. Smart home is a part of the application for those short-range devices, the number of which surpassing mobile devices by twofold [1] Smart homes allow home appliances (such as television, air conditioner and refrigerator) to be connected to the internet and providing innovative and smart service to homes [2]. This can be interpreted as these smart devices automates the home task. In this thesis, the expression “home automation” is used interchangeably with “home IoT”. We can remotely control our home devices over the internet and gather information about our home directly to our smartphones. Figure 1.1 below illustrates how communications between user devices where, a cloud service acts as a central communication centre to relay information between devices. Some IoT devices also allow direct communication with user mobile phones and computing devices.

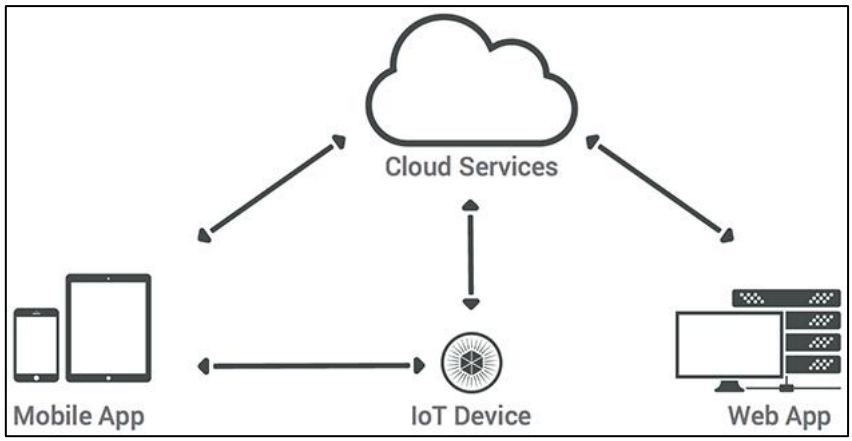

Figure 1.1 Overview of home IoT devices [3]

IoT device generates, processes, and exchanges a lot of safety-critical data and privacy-sensitive information, hence it is an appealing target of various cyber-attacks [4]. Many state-of-the-art security frameworks are highly centralized and not necessarily suited for IoT because of the difficulty of scaling, the many-to-one nature of traffic and the single point of failure [4, 5]. Centralization also forces us to trust the provider of a service. Sometimes, a controversial event may happen, such as the Facebook-Cambridge Analytica scandal where private user data is compromised [6]. As for smart home devices, it is strongly required to protect and secure our privacy within our private and personal homes[7]. In order to guarantee a completely trusted and transparent environment, we proposed a decentralized solution for smart homes using blockchain. Blockchain is a technology used in cryptocurrencies such as Bitcoin [8], provides an attractive technology for addressing the security and privacy challenges in IoT. Advantageous features of Blockchain are 1) decentralization, 2) anonymity and 3) security [9]. These advantages can add existing IoT applications to more security layers and relieving dependence on a central server. They also provide tampered resistance data structure by 1) timestamp, 2) data encryption and 3) distributed consensus furnished within blockchain technology. Also, the reduction of central servers reduces the maintenance cost.

1.2 Problem Statement

Dependence on a centralized server or cloud can increase security risks if being attacked. Data in the server can be tampered and causes distrust [10]. Furthermore, looking at the recent trend on consumer IoT devices manufactured by large companies, most of these devices rely on online servers hosted by those companies [11]. This situation can be a severe concern for home privacy and longevity of the IoT devices. If data is stored on remote servers, they are vulnerable to hackers or even the company's own employees to misuse the data for cybercrimes. Even third parties who signed off with the IoT provider can access consumer data to cause mistrust. Besides that, software and server support for IoT can be costly. Some IoT providers may stop supporting those devices, in the long run, rendering them useless and contributing to e-waste [12].

Blockchain has been proven to provide a solution for the security issues of IoT networks [13, 14]. In addition to that, Blockchain provides a scalable distributed ledger feature that requires consensus across all participating nodes. Ethereum blockchain is a good candidate due to its more modern approach and highly customizable. However, as it is evident from the operation of both Bitcoin and Ethereum, existing Ethereum Blockchain cannot be directly applied to IoT applications expected from homes or industries because of 1) power consumption, 2) real-time operation, 3) memory consumption, and 4) operation cost. Hence, some researchers adopted customizable blockchain and others developed completely new blockchain schemes for IoT uses. However, most schemes are targeted to be used with a public blockchain, which is sometimes slow and costly to maintain [4]. Another shortcoming is less privacy in public blockchain due to the permissionless nature of ensuring all participants can validate the data and come to a consensus [15].

The problems of the current status of home automation can be summarized as follows:

1) Today's scheme for home automation using centralized servers and public blockchain has a potential concern for security, privacy, performance, or cost.

2) Decentralized Ethereum based private home automation platform with sufficient real-time performance for home use is needed.

1.3 Research Objective

Considering these facts, in this research, an implementation of blockchain for home automation with privacy is developed to provide decentralized, secure, and private communication for home IoT devices. This implementation is made using well supported Ethereum-based blockchain as a core communication protocol for the IoT devices. In order to fit various types of device computing power, the node is configured as both active and passive node while still maintaining the decentralized communication between devices. Using a private blockchain, the private operation and data of the user are confined between user IoT devices and maintain speed without public blockchain cost.

In summary, the objectives of this project are:

(i) To develop a decentralized private home automation platform based on Ethereum blockchain as intermediary for data exchange between home devices.

(ii) To evaluate the performance of the real-time operation of the developed low-powered home automation platform using modified blockchain parameters.

1.4 Scope of Study

This study covers the implementation of Blockchain decentralized communication using Ethereum and data structure design for use on low powered IoT devices for home automation. A private Ethereum blockchain will be implemented using Python3's web3 API to replace the conventional server-host data exchange with peer-to-peer decentralized data exchange and device communication. This also covers the implementation of Ethereum Blockchain for home automation using two type of

node configuration which is big and small node to provide flexibility incorporating into low powered devices with the target performance better than industrial standard.

1.5 Significance of Study

The major contributions of this research are:

- A new method of data exchange for home automation devices using Blockchain technology which improves on reliability

- A modified Blockchain design with an appropriate architecture for real-time operation use in small, inexpensive and low powered IoT devices in a home.

- Application and implementation of Blockchain technology for home use of IoT with privacy design in mind utilizing a private blockchain.

REFERENCES

1. Minteer, A., *Analytics for the Internet of Things (IoT)*. 2017: Packt Publishing Ltd.
2. Ali, W., et al. *IoT based smart home: Security challenges, security requirements and solutions*. in *2017 23rd International Conference on Automation and Computing (ICAC)*. 2017. IEEE.
3. Akhtar, M.M. and D. Rizvi, *IoT-chain: security of things for pervasive, sustainable and efficient computing using blockchain.* EAI Endorsed Transactions on Energy Web, 2020. **7**(30): p. e7.
4. Falco, G., et al. *Neuromesh: Iot security enabled by a blockchain powered botnet vaccine*. in *Proceedings of the International Conference on Omni-Layer Intelligent Systems*. 2019.
5. Fovino, I.N., et al. *Modbus/DNP3 state-based intrusion detection system*. in *2010 24th IEEE International Conference on Advanced Information Networking and Applications*. 2010. IEEE.
6. Kleinman, Z. *Cambridge Analytica: The story so far*. 2018 [cited 2019 January 10]; Available from: https://www.bbc.com/news/technology-43465968.
7. Dang, T.L.N. and M.S. Nguyen. *An approach to data privacy in smart home using blockchain technology*. in *2018 International Conference on Advanced Computing and Applications (ACOMP)*. 2018. IEEE.
8. Huh, S., S. Cho, and S. Kim. *Managing IoT devices using blockchain platform*. in *2017 19th international conference on advanced communication technology (ICACT)*. 2017. IEEE.
9. Sicari, S., et al., *Security, privacy and trust in Internet of Things: The road ahead.* Computer networks, 2015. **76**: p. 146-164.
10. Thakore, R., et al., *Blockchain-based IoT: A survey.* Procedia Computer Science, 2019. **155**: p. 704-709.
11. Xu, J., et al., *Edgence: A blockchain-enabled edge-computing platform for intelligent iot-based dapps.* China Communications, 2020. **17**(4): p. 78-87.
12. Lechelt, S., et al. *Designing for the End of Life of IoT Objects*. in *Companion Publication of the 2020 ACM Designing Interactive Systems Conference*. 2020.
13. Reilly, E., et al. *An IoT integrity-first communication protocol via an ethereum blockchain light client*. in *2019 IEEE/ACM 1st International Workshop on Software Engineering Research & Practices for the Internet of Things (SERP4IoT)*. 2019. IEEE.
14. Arif, S., et al., *Investigating smart home security: Is blockchain the answer?* IEEE Access, 2020. **8**: p. 117802-117816.
15. Dorri, A., et al. *Blockchain for IoT security and privacy: The case study of a smart home*. in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*. 2017. IEEE.
16. Huang, Z., Z. Mi, and Z. Hua, *HCloud: A trusted JointCloud serverless platform for IoT systems with blockchain.* China Communications, 2020. **17**(9): p. 1-10.

17. Lee, Y., et al., *A blockchain-based smart home gateway architecture for preventing data forgery.* Human-centric Computing and Information Sciences, 2020. **10**(1): p. 1-14.
18. Fernández-Caramés, T.M. and P. Fraga-Lamas, *A Review on the Use of Blockchain for the Internet of Things.* Ieee Access, 2018. **6**: p. 32979-33001.
19. Minoli, D., *Positioning of blockchain mechanisms in IOT-powered smart home systems: A gateway-based approach.* Internet of Things, 2020. **10**: p. 100147.
20. Atlam, H.F. and G.B. Wills, *Intersections between IoT and distributed ledger*, in *Advances in Computers*. 2019, Elsevier. p. 73-113.
21. Zhao, W., et al., *ETC-IOT: Edge-node-assisted transmitting for the cloud-centric internet of things.* IEEE Network, 2018. **32**(3): p. 101-107.
22. Polianytsia, A., O. Starkova, and K. Herasymenko. *Survey of hardware IoT platforms*. in *2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*. 2016. IEEE.
23. Nagasai. *Classification of IoT Devices*. 2017 [cited 2020 December 02].
24. Nakamoto, S. and A. Bitcoin, *A peer-to-peer electronic cash system.* Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 2008. **4**.
25. Hill, B., S. Chopra, and P. Valencourt, *Blockchain Quick Reference: A guide to exploring decentralized blockchain application development*. 2018: Packt Publishing Ltd.
26. Standards, N.I.o. and T.T. Administration, *Secure hash standard*. Vol. 180. 1993: US Department of Commerce, Technology Administration, National Institute of ….
27. Christidis, K. and M. Devetsikiotis, *Blockchains and smart contracts for the internet of things.* Ieee Access, 2016. **4**: p. 2292-2303.
28. Qiu, T., R. Zhang, and Y. Gao, *Ripple vs. SWIFT: transforming cross border remittance using blockchain technology.* Procedia computer science, 2019. **147**: p. 428-434.
29. Popov, S., *The tangle.* White paper, 2018. **1**(3).
30. Alphand, O., et al. *IoTChain: A blockchain security architecture for the Internet of Things*. in *2018 IEEE wireless communications and networking conference (WCNC)*. 2018. IEEE.
31. Team, I., *IoTeX: A Decentralized Network for Internet of Things Powered by a Privacy-Centric Blockchain.* support@ iotex. io, Tech. Rep., July, 2018. **12**.
32. Thangavel, D., et al. *Performance evaluation of MQTT and CoAP via a common middleware*. in *2014 IEEE ninth international conference on intelligent sensors, sensor networks and information processing (ISSNIP)*. 2014. IEEE.
33. Sahadevan, A., et al. *An offline online strategy for IoT using MQTT*. in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*. 2017. IEEE.
34. Lao, L., et al., *A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling.* ACM Computing Surveys (CSUR), 2020. **53**(1): p. 1-32.
35. Ammi, M., S. Alarabi, and E. Benkhelifa, *Customized blockchain-based architecture for secure smart home for lightweight IoT.* Information Processing & Management, 2021. **58**(3): p. 102482.

36. Lamtzidis, O. and J. Gialelis. *An IOTA based distributed sensor node system*. in *2018 IEEE Globecom Workshops (GC Wkshps)*. 2018. IEEE.
37. Xu, Q., et al. *Building an ethereum-based decentralized smart home system*. in *2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)*. 2018. IEEE.
38. Zhou, Y., et al. *Improving iot services in smart-home using blockchain smart contract*. in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. 2018. IEEE.
39. Author, T.g.-e. *Installing Go Ethereum*. 2018 [cited 2018 March 13].
40. endorphin. *ETHEREUM VIRTUAL MACHINE (EVM)*. 2021 [cited 2021; Available from: https://ethereum.org/en/developers/docs/evm/.
41. *Benchmarking Raspberry Pi GPIO Speed*. 2015 [cited 2020; Available from: https://codeandlife.com/2012/07/03/benchmarking-raspberry-pi-gpio-speed/.
42. Kodali, R.K. and V.S.K. Gorantla. *Weather tracking system using MQTT and SQLite*. in *2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*. 2017. IEEE.
43. De Vries, H.J., J.P. de Ruijter, and N. Argam. *Dominant design or multiple designs: The flash memory card case*. in *2007 5th International Conference on Standardization and Innovation in Information Technology*. 2007. IEEE.
44. Pei, C., et al. *WiFi can be the weakest link of round trip network latency in the wild*. in *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*. 2016. IEEE.
45. Kenitar, S.B., et al. *Evaluation of the MQTT protocol latency over different gateways*. in *Proceedings of the 3rd International Conference on Smart City Applications*. 2018.

LIST OF PUBLICATIONS

Suchaad, S. A. L., Mashiko, K., Ismail, N. B., & Abidin, M. H. Z. (2018). *Blockchain use in home automation for children incentives in parental control.* Paper presented at the Proceedings of the 2018 International Conference on Machine Learning and Machine Intelligence.

Abidin, M. H. Z., **Suchaad, S.**, Mashiko, K., & Ismail, N. (2019). *Ethereum Blockchain Network Implementation for IoT Platform*. International Journal of Integrated Engineering, 11(7), 1-6.