

**BLOCKCHAIN TECHNOLOGY FOR IOT SECURITY FOR
A SMART HOME**

MOHONA MOJUMDER

**BACHELOR OF SCIENCE IN INFORMATION AND
COMMUNICATION ENGINEERING**

**NOAKHALI SCIENCE AND TECHNOLOGY
UNIVERSITY**

BLOCKCHAIN TECHNOLOGY FOR IOT SECURITY FOR A SMART HOME

MOHONA MOJUMDER

Report submitted in partial fulfilment of the requirements for the award of the degree of Bachelor of Science in Information and Communication Engineering

Department of Information and Communication Engineering
NOAKHALI SCIENCE AND TECHNOLOGY UNIVERSITY

DECEMBER 2018

DECLARATION

This thesis proposal is submitted to the Department of Information & Communication Engineering, Noakhali Science & Technology University, Sonapur, Noakhali in partial fulfillment of the requirements for having the B.Sc. degree in ICE. So, I, here by, declare that this report has not been submitted elsewhere for the requirement of any kind of degree, diploma or publication.

(MohonaMojumder)

Roll No: BKH1511021F

Session: 2014-2015

Year: 4, Term: I

Department of ICE

Noakhali Science and Technology University,

Noakhali,Bangladesh.

ACCEPTANCE

I, hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Bachelor of Science in Information and Communication Engineering.

PROF. DR. MD. ASHIKUR RAHMAN KHAN

CHAIRMAN

DEPARTMENT OF INFORMATION AND COMMUNICATION ENGINEERING

NOAKHALI SCIENCE AND TECHNOLOGY UNIVERSITY,

NOAKHALI - 3814

ACKNOWLEDGEMENTS

I am grateful and would like to express my sincere gratitude to my supervisor Professor Dr. Md. AshikurRahman Khan for his germinal ideas, invaluable guidance, continuous encouragement and constant support in making this research possible. I appreciate his consistent support from the first day I applied to graduate program to these concluding moments. I am truly grateful for his progressive vision about my training in science, his tolerance of my naïve mistakes, and his commitment to my future career. I also sincerely thanks for the time spent proofreading and correcting my many mistakes.

I acknowledge my sincere indebtedness and gratitude to my parents for their lc dream and sacrifice throughout my life.

ABSTRACT

One of the key challenges of IOT world is security. In this article, my attempt is to critically view the use of blockchain technology to secure IOT. Blockchain is used for smart home so that the security can be enhanced. Blockchain enriches the security level. In this technology, the existing database can only be expanded and the previous record can not be changed. Local blockchain is a secure and private blockchain that is mined and stored by one device which is always in online. The local blockchain is only maintained by its owner. To increase the security level and to secure the data from sharing external environment, the blockchain technology is used.

TABLE OF CONTENTS

	Pag e No
TITLE PAGE	2
DECLARATION	3
ACCEPTANCE	4
ABSTRACT	6
TABLE OF CONTENTS	7
TABLE OF FIGURES	8
CHAPTER 1 INTRODUCTION	9
1.1 Introduction	9
1.2 Problem statements	12
1.3 Objectives	13
 CHAPTER 2 LITERATURE REVIEW	 14
 CHAPTER 3 METHODOLOGY	 16
 CHAPTER 4 RESULT	 19
4.1 Expected results	19

CHAPTER 5	CONCLUSION	20
------------------	-------------------	-----------

REFERENCES	21
-------------------	-----------

List of Figures

Figure name	Page No.
1.1 IOT security system	10
1.2 The working process of Blockchain Technology	11
3.1 Get a handle on Blockchain to solve IOT security problem	17
3.2 Flow diagram of user-1 sending a message to user-2 with a Blockchain	18

CHAPTER -1

INTRODUCTION

1.1 Introduction

There are a number of household ‘smart devices’ already available on the market, and these gadgets operate themselves. These range from thermostat devices, which allow your home’s heating to be controlled from any device with Wi-Fi, to hubs which operate all your other gadgets, like Echo. In the future, this trend is likely to continue. Smart devices are designed to make life easier and technology more efficient, allowing a single device to control everything else in your home. Imagine a world in which your alarm clock is set to not only wake you up but also tell your kettle to start boiling water for your morning cup of tea! As well as being highly convenient, these devices have the potential to save homeowners money on their energy bills and reduce waste of energy. In turn, this could have a positive impact on the environment by reducing carbon emissions and fossil fuel use. However, adopting the IOT technology on mass poses a number of problems.

Security is the main issue that the IOT currently faces. The question of how people will keep all of their individual devices secure to prevent mass-hacking and theft of personal data is yet to be answered. The current security methods in place are already struggling to keep personal data secure, with several high profile hacks and cyberattacks having occurred on a huge scale in recent years.

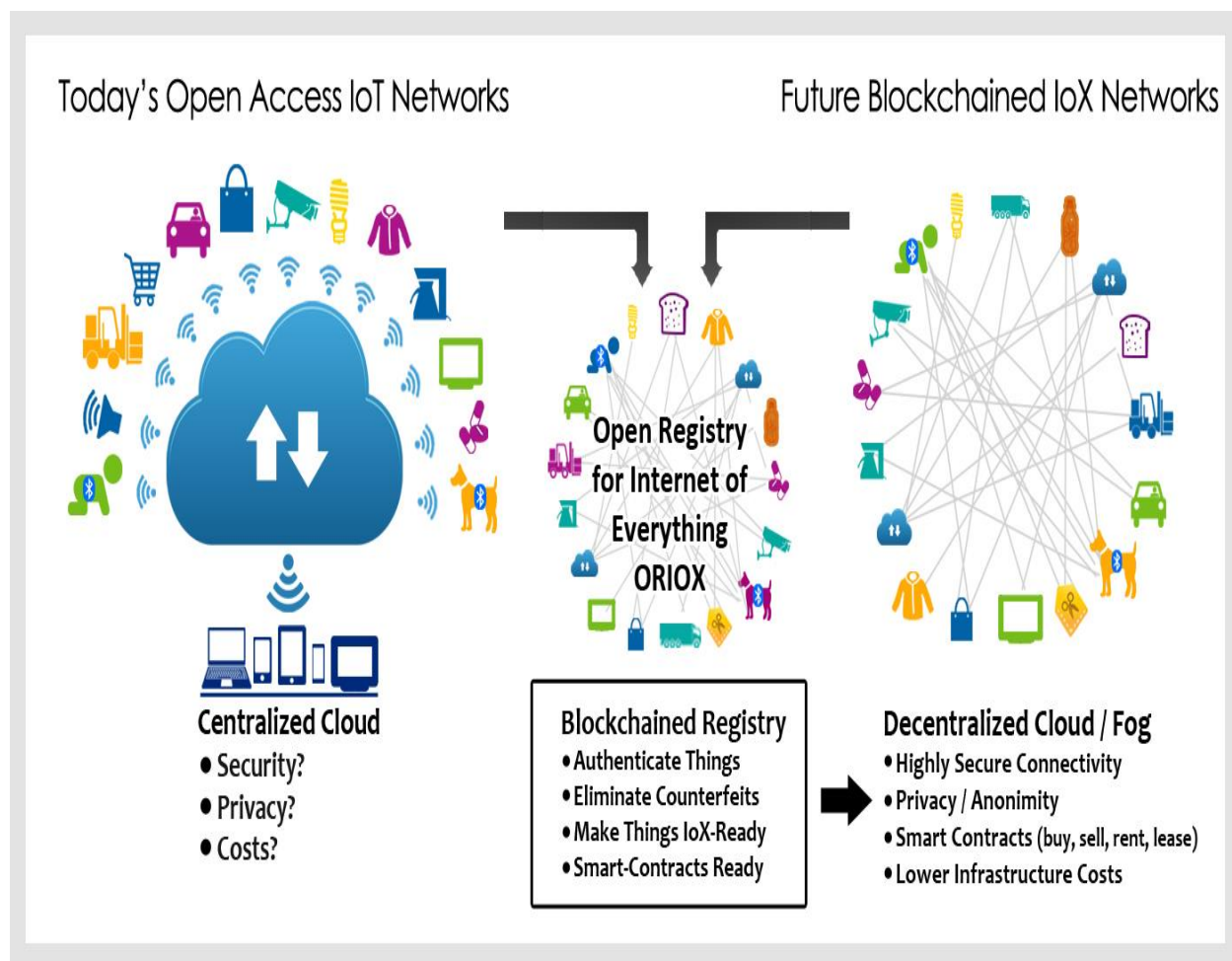


Figure 1.1: IOT security system

Blockchain is a distributed database technology that provides very hard to tamper, ledger records. It allows storage of all transactions into immutable records and every record distributed across many participant nodes. The security comes from use of strong public-key cryptography, strong cryptographic hash and complete decentralisation.

Blocks are the key concept of the technology. They are small sets of transactions that have taken place within the system. Each new block stores reference of the previous transaction by including a SHA-256 hash of the previous transaction. In this way, it creates a 'chain' of blocks and hence the name. Blocks are

computationally difficult to create, and takes multiple specialised processors and significant amounts of time to generate.

Since generating a block is difficult and to tamper one block, one has to tamper the previous block and then has to follow the chain to change it completely, blockchain technology is considered to be tamper resistant.

Miners are the ones who run powerful computers to create blocks.

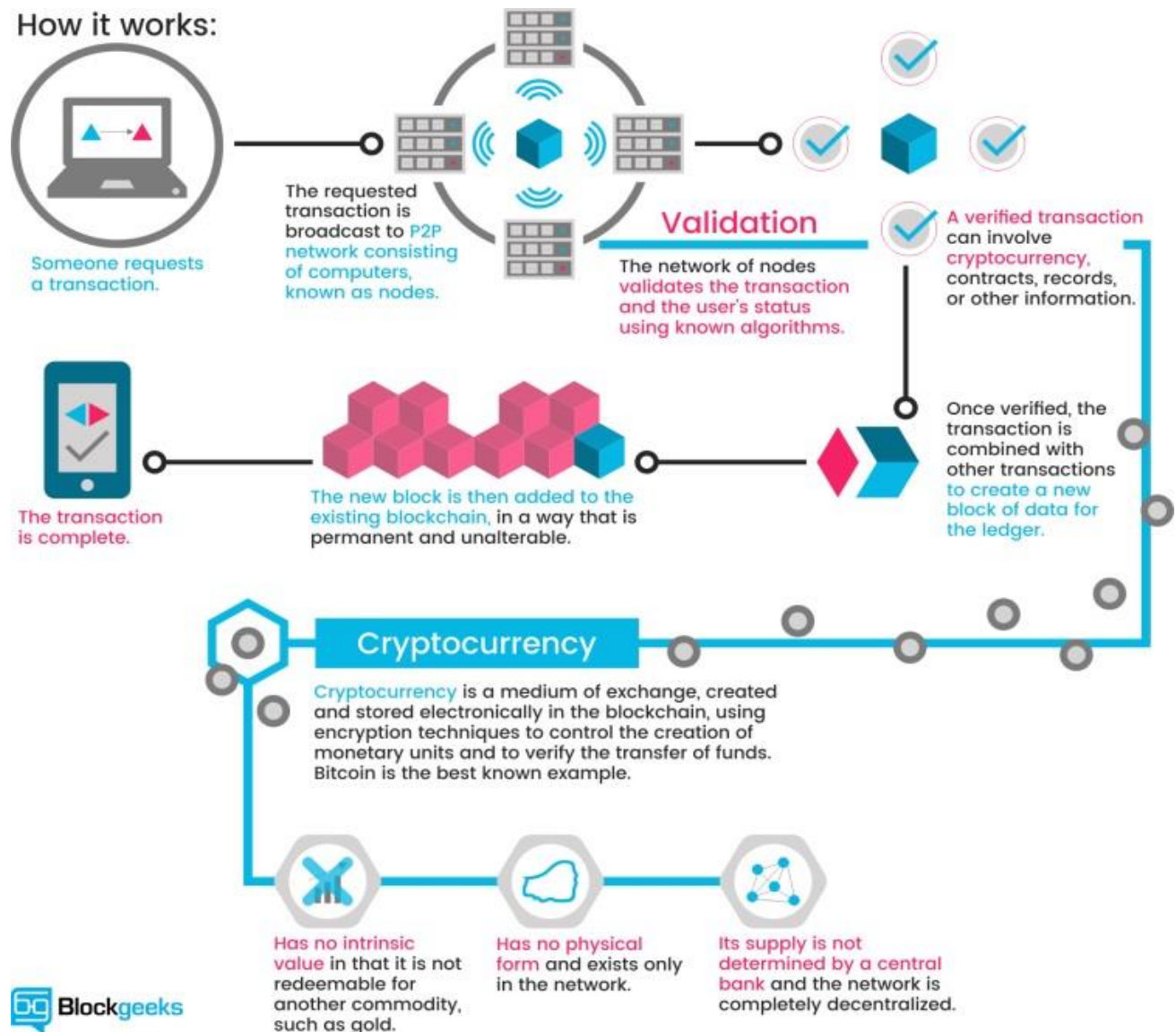


Figure 1.2 : The working process of Blockchain technology

Blockchain technology is the missing link to settle scalability, privacy, and reliability concerns in the Internet of Things.

This decentralized approach would eliminate single points of failure, creating a more resilient ecosystem for devices to run on. The cryptographic algorithms used by blockchains, would make consumer data more private.

In an IOT network, the blockchain can keep an immutable record of the history of smart devices. This feature enables the autonomous functioning of smart devices without the need for centralized authority. As a result, the blockchain opens the door to a series of IOT scenarios that were remarkably difficult, or even impossible to implement without it.

1.2 Problem Statements

We can secure smart home by using many ways like as using strong and unique password for wifi networks, by avoiding from using the public network, by giving a strong password for device account, by keeping your software up to date, by disabling features you may not need, change default usernames and passwords, check the setting for your devices. Although using all these techniques, we can not secure our smart home, because hackers are always update the technique to hack your privacy and use your devices.

As discussed in [1], IOT networks are vulnerable to external threats for a variety of reasons. It is easy to gain physical access to individual devices since they are often isolated and there is no administrator to manage them; They usually communicate with each other and with a gateway using different wireless communication protocols, making eavesdropping very easy; and finally, most devices have low processing capabilities and thus it is difficult to implement complex security schemes on a per device basis.

So, in this discussion we try to make the smart home more secure by using the blockchain technology and try to describe the way of working by which the blockchain is actually work more to enhance the security of smart home.

1.3 Objectives

The main objectives of this thesis are given below-

- i. To secure sensitive data in IOT
- ii. To add extra security layer in IOT devices.
- iii. To prevent data from external access from our IOT based smart home.
- iv. To enhance the security for IOT devices which are belongs in a smart home.
- v. To create a trustworthy IOT environment.

CHAPTER 2

LITERATURE REVIEWS

The use of Blockchain technology in the IOT domain to facilitate the sharing of services and resources, and automate in a secure manner several time-consuming workflows, is studied in [2]. The authors concluded that the Blockchain-IOT combination is powerful and can pave the way for novel business models and distributed applications. Moreover, relative literature and work designed for Blockchain use in IOT was studied in [3]. The paper identified different research efforts, [4, 5, 6], that utilize the Blockchain infrastructure as a data storage management solution. In all cases, data exchanged between IOT devices are stored as unique transactions within the Blockchain and are subsequently distributed among the nodes, ensuring the integrity and security of the communication between them.

A decentralized peer-to-peer platform based on Blockchain networks for Industrial IOT was proposed in [7]. Their use cases focus on industrial and manufacturing applications, where Smart Contracts act as intermediaries between the Blockchain ecosystem and outside stakeholders. Dorri et al. proposed a private Blockchain infrastructure for Smart homes, [8]. They focus on security issues with respect to confidentiality, integrity and availability, while simulation results indicate that the overheads imposed by the use of such technology remain at low levels. Additionally, [9] discusses the security enhancements with the use of Blockchain in IOT. The role of Blockchain is examined through four challenges, namely: Costs and capacity constraints, Architecture, Unavailability of services and Susceptibility to manipulation. They conclude that with the decentralized and consensus-driven structures of Blockchain, more secure

IoTecosystems can be provided as the network size increases. Recently, FairAccess, a token-based access control model with the use of Blockchain, has been proposed in [10], that provides an access control mechanism for the transactions realized within a Blockchain infrastructure.

IT companies have also shown a great interest in applying Blockchain architectures in IOT ecosystems. The IBM Watson IOT platform supports private Blockchain ledgers for sharing IOT data via transactions. ADEPT (Autonomous Decentralized Peer-To-Peer Telemetry), a research project for Blockchain in IOT that uses the technology of Ethereum, Telehash and BitTorrent, was also announced [11]. Targeting an economy of Things, ADEPT focuses on Distributed Transaction Processing and Applications, Robust Security and Privacy By Design and Default. There are also other companies and start-ups that focus on transaction integrity, trust and security in the IOT domain.

Almost all relevant research work utilize the Blockchain technology as a data storage management solution.

CHAPTER 3

METHODOLOGY

When running on the blockchain, smart home devices become immutable and therefore safe from cyber attacks. This means that hackers cannot access your home or the data collected by your IOT devices. Additionally, with a blockchain-powered smart home system, you can securely enable other parties to access specific areas and devices without giving them access to everything.

A good example of smart home tech using blockchain for this purpose is Comcast. Their blockchain technology utilizes a permission-based ledger, enabling the homeowner to grant access permissions remotely through a mobile application. The mobile app also enables them to revoke these permissions at the click of a button.

The blockchain-powered smart home technology can also enable homeowners to hire domestic workers for specific tasks and pay them through smart contracts which ensures that the specified conditions between the contractor and the contractee are met before executing the contract.

As technologies in IOT, blockchain continue to expand, there is no doubt that more advanced smart home solutions will come.



Figure 3.1 : Get a handle on Blockchain to solve IOT security problem

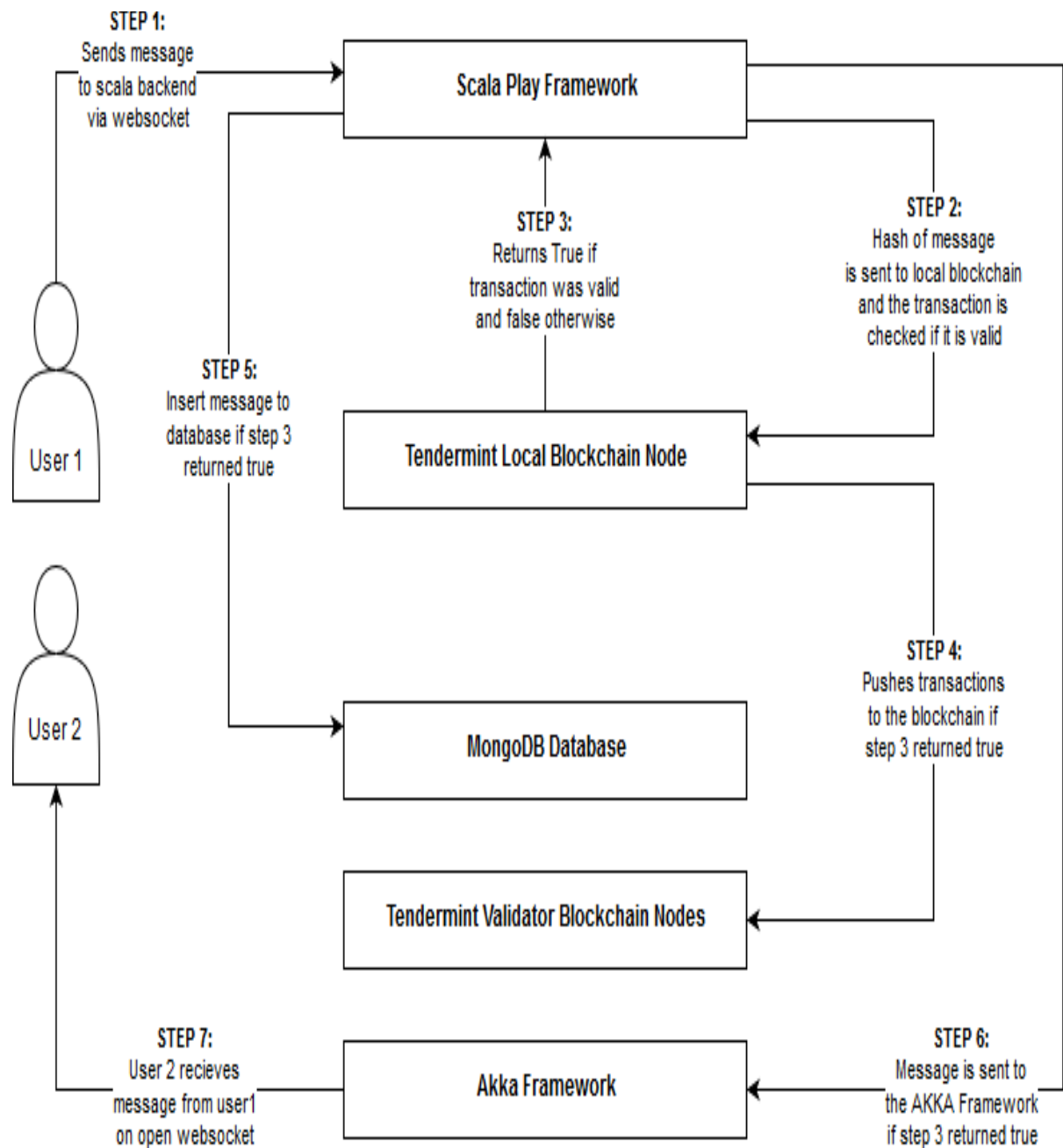


Figure 3.2 : Flow diagram of user-1 sending a message to user-2 with a Blockchain

CHAPTER-4

RESULT

4.1 EXPECTED OUTCOMES

Hope that, this thesis will help for develop to secure and stable IOT based smart home. This thesis will demonstrate the security vulnerability in IOT based smart home and show the technique how to secure those vulnerability.

CHAPTER-5

CONCLUSION

By implementing blockchain technology, the owner of the smart home can handle the automatic controllation of the home more securely than before.

The enhanced security environment that blockchain facilitates will massively help to overcome people apprehensions when it comes to using an increasing number of smart devices in their daily lives.

Knowing that using a smart lock for your home is safer than using a physical key, for example, will greatly speed up the transition we all make to using such smart technology.

REFERENCES

[1]. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: a survey. *Comput. Netw.* **54**(15), 2787–2805 (2010)

CrossRefGoogle Scholar

[2]. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things. *IEEE Access* **4**, 2292–2303 (2016).

CrossRefGoogle Scholar

[3]. Conoscenti, M., Vetró, A., Martín, J.C.D.: Blockchain for the Internet of Things: a systematic literature review. In: 2016

IEEE/ACS 13th International Conference on Computer Systems and Applications (AICCSA), pp. 1–6, November 2016

Google Scholar

[4]. Wörner, D., von Bomhard, T.: When your sensor earns money: exchanging data for cash with Bitcoin. In: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication, UbiComp 2014 Adjunct, pp. 295–298. ACM, New York (2014)

Google Scholar

- [5]. Zhang, Y., Wen, J.: The IOT electric business model: using blockchain technology for the Internet of Things. *Peer-to-Peer Netw.Appl.* **10**(4), 983–994 (2017)

CrossRefGoogle Scholar

- [6]. Zyskind, G., Nathan, O., Pentland, A.: Enigma: decentralized computation platform with guaranteed privacy. *arXiv preprint arXiv:1506.03471* (2015)

- [7].Bahga, A., Madiseti, V.K.: Blockchain platform for industrial Internet of Things. *J. Softw. Eng. Appl.* **9**(10), 533 (2016)

CrossRefGoogle Scholar

- [8]. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.:

Blockchain for IOT security and privacy: the case study of a smarthome. In: 2017 IEEE International Conference on Pervasive

Computing and Communications Workshops
(PerComWorkshops), pp. 618–623, March 2017

- [9]. Kshetri, N.: Can blockchain strengthen the Internet of Things? IT Prof. **19**(4), 68–72 (2017)

CrossRefGoogle Scholar

- [10]. Ouaddah, A., Elkalam, A.A., Ouahman, A.A.: Towards a novel privacy-preserving access control model based on blockchain technology in IOT. In: Rocha, Á., Serrhini, M., Felgueiras, C. (eds.) Europe and MENA Cooperation Advances in Information and Communication Technologies, pp. 523–533. Springer, Cham (2017).

https://doi.org/10.1007/978-3-319-46568-5_53 CrossRefGoogle Scholar

- [11]. Veena, P., Panikkar, S., Nair, S., Brody, P.: Empowering the edge-practical insights on a decentralized Internet of Things.

IBM Institute for Business Value 17 (2015)

Google Scholar

