Privacy Preservation in IoT systems via Blockchains: A Brief Review

Naqqash Dilshad, Kelvin Dushime, JaeSeung Song*
Sejong University, Seoul, South Korea
{dilshadnaqqash, dushimekelvin}@sju.ac.kr, jssong@sejong.ac.kr

Abstract—Modern-day Internet of Things (IoT) techniques are paving their path for a revolutionized world in which most of the everyday items that we use will be interconnected. These entities will be able to connect and share information to mechanize the majority of our tasks. This interconnection of edge devices needs security, impeccable authentication, robustness, and effortless maintenance services. To provide such relevant features, blockchain appears as a sustainable solution. The decentralized nature of blockchain has solved numerous security, maintenance, and authentication issues of IoT systems. Consequently, enormous growth in applications of blockchain-based IoT systems can be witnessed in recent years. However, a blockchain-based IoT network is public, so transactional details and encrypted keys are open and visible to everyone in that network. Thus, any foe can infer critical information of users from this public infrastructure. In this study, we discuss the privacy issues caused due to the integration of blockchain in IoT applications by focusing on the applications of our daily use. Furthermore, we highlighted the implementation of privacy preservation strategies in blockchain-based IoT systems.

Index Terms—Blockchain, Privacy Preservation, Blockchain Applications, Trust Model

I. INTRODUCTION

The exponential increase of digital gadgets and devices using IoT technology has drawn the attention of academia and the industrial sector. IoT technology is performing an effective role in the development of numerous fields of our daily life involving energy systems, transportation, and industrial automation. It is expected that there will be roughly 18 billion IoT devices by the year 2022. These IoT devices collect data from surroundings and also interchange data with other IoT devices and platforms. Conventionally for future use IoT systems collected data is stored in a specific centralized server (especially cloud servers). Therefore, IoT users have to develop trust for the centralized servers that their sensitive and personal data is safe in these servers [1].

Regardless of the undeniable advantages offered by these service providers, centralized IoT systems may cope with many challenges. For example, unencrypted server data can be hacked and may trigger the leakage of sensitive information. Furthermore, a few IoT devices need management by more than one supervisor at the same time. Keeping in view all mentioned points, scholars are thinking to move towards a decentralized architecture for the management and storage of IoT devices and data correspondingly. Blockchain is a new concept towards decentralized storage and data management, as it functions over the notion of a shared, secured, and distributed ledger that keeps and stores records without any centralized authority or trusted third party.

In the context of IoT, blockchain authorizes two devices to communicate and exchange, resources, information, and data in a decentralized peer-to-peer (P2P) network. Blockchain delivers a transparent architecture in which the odds of any fraudulent access is the least possible because the decision to add any data is broadcast to the entire network, and any critical decision is taken with the agreement of a majority of users instead of a solo centralized administrator/server. In Fig. 1, some of the most common advantages that blockchain technology provides in IoT systems are presented. Moreover, this study briefly introduces related literature in Section II, while the last section provides a conclusion and offers a viewpoint of future research direction.

II. LITERATURE REVIEW

Our study offers a summary of privacy issues in blockchain-based IoT systems and is different from previous studies, as we notably cover the particular area of privacy issues in applications of blockchain-based IoT systems. Brief literature of past survey articles concentrating on blockchain and its assimilation with IoT is present, and only some of them aimed over security and privacy concerns of blockchain. Neverthe-
less, as per our knowledge, there is no previous article that refers to privacy preservation techniques in a blockchain-based IoT environment from an application perspective. We classify the previous work of literature over blockchain into three major categories named blockchain applications, blockchain as trust model, and blockchain-based security services. We categorized recent survey articles in Table I along with key scientific contributions, and several deemed factors. An insightful work on applications of blockchain is introduced in [2] [3], in the aforementioned studies the authors presented a substantial overview of direct and smart contract-based transactions in blockchain-based banking ledgers. Additionally, the functioning and implementation of the practical framework of the blockchain system is outlined and provided discussion about the applications of blockchain in a comprehensive and detailed manner. They extensively discussed two state-of-the-art models called "Internet of money” and "second-generation blockchain”. Additionally, in use cases of blockchain, the authors in [4] used blockchain as a trust model because of its significant properties. The authors presented an organized survey article on the practical implementation of blockchain in various smart applications. A different survey overusing blockchain as a security service is performed in [5]. This survey aimed at abusing blockchain for various security services such as authentication, access control, confidentiality, and privacy control.

Based on the literature [6] [7], anonymization is the most common approach used to preserve privacy in IoT-based systems. Several studies have included anonymization techniques to protect the privacy of blockchain-based IoT applications. Some common applications include electronic health records, finances, vehicular networks, and energy systems. There are numerous anonymization policies such as k-anonymity, t-closeness, and l-diversity to make anonymization stronger. A comprehensive analysis of the aforementioned policies of anonymization is out of the scope of this article, and interested readers can read work presented in [7].

### III. Conclusion

The tendency of combining IoT systems in our day-to-day tasks is growing dramatically, and it has aided our lives in several aspects. This innovation has raised a number of security and authentication challenges such as mining, hacking, and service denial attacks due to a centralized setup, but blockchain technology came up as the best possible way to overwhelm these challenges. Nevertheless, blockchain-based IoT systems are also susceptible to numerous privacy hazards that require to be solved before their practical implementation. In this study, we have presented a summary of the significance of privacy preservation in blockchain-based IoT systems. Finally, we concluded the article by mentioning and highlighting certain challenges and future research directions in blockchain-based IoT systems.

### ACKNOWLEDGMENT

This work was supported by IITP grant funded by the Korean government (MSIT) (No.2020-0-00959, Fast Intelligence Analysis HW/SW Engine Exploiting IoT Platform for Boosting On-device AI in 5G Environment). Corresponding author: Prof. Song JaeSeung.

### REFERENCES


