Asian Journal of Multi-Disciplinary Research

ISSN (Online): 2395-1710, ISSN (Print): 2395-1729
Volume: 5, Issue: 1 March 2019
DOI: http://dx.doi.org/10.20468/ajmdr.2019.5.1.05

Research Article

Security and Privacy Issues Based on Blockchain for the Internet of Things

P. V. Kumaraguru, V. J. Chakravarthy

Department of Computer Applications, Guru Nanak College, Chennai, Tamil Nadu, India

ABSTRACT

To resolve the privacy, consistency, and scalability based on missing link, blockchain technology is an involvement in the Internet of Things (IoT). It can be used in tracking billions of connected devices, enable the processing of transactions and coordination between devices that allow for significant savings to IoT industry manufacturers. Blockchain technique has provided with decentralized security and privacy and also accomplished essential energy, computational overhead, and delay. These are not a suitable for most resource-constrict IoT devices. This approach of decentralization would create an additional network for devices to run on and eliminate the single points of breakdown. This study describes block chain technology using cryptographic algorithm based on encryption and decryption has built a user database with highly secure and privacy and this paper illustrate about the security and privacy preserving based on block chain in IoT.

Address for correspondence:
Dr. V. J. Chakravarthy, Assistant Professor, Department of MCA, Guru Nanak College, Chennai.

Keywords:
Blockchain, Internet of things, Privacy, Security

Received: 18th February 2019
Accepted: 03rd March 2019
Published: 21rd March 2019

INTRODUCTION

Blockchain is a database that maintains a continuously growing set of data records. It is distributed in nature, meaning that there is no master computer holding the entire chain. Rather, the participating nodes have a copy of the chain. It added only the ever-growing data records to the chain. The combination of Internet of Things (IoT) system with the blockchain has the benefit of robustness against attacks and threats, low cost of operation, resources based on decentralized management, and so on. To overcome the major challenges, the merging of IoT and blockchain aims to realize the IoT platform in the near future. Blockchain is the developed dispersed ledger technology that supports bitcoins in the industry as an object of penetrating attention and beyond. Blockchain technology is designed to be secured, clear, efficient, auditable and highly challenging to outages in a way that offers any digital interaction or recording transactions. It carries with enabling novel business models and probability of disrupting industries. The technology is young and changing very rapidly; widespread commercialization is still a few years off. However, to avoid the missed opportunities, planners, decision-makers, strategists, and disruptive surprises across the business functions and industries should pay attention to discover requests of the technology. The blockchain organization is self-possessed of an order of blocks, which are connected together by their hash values.

In the network of blockchain as shown in Figure 1, digital signed transactions of users were maintained by public ledger in a P2P network. There are two keys for user: (i) Public key is used for encryption and (ii) private key is to read an encrypted message as shown in Figure 2, and also, it is used for signing the perspective of blockchain that signifies the unique address. Asymmetric cryptography is used to decrypt the message encrypted by the corresponding public key.

At the beginning stage, user ciphers a transaction and broadcast to its peers using its private key. The cipher transaction is received by the peers and then will validate the transaction and broadcast over the network. All the entire parties have mutually validated who involved in the transaction to meet the consent agreement. Once a distributed consensus is reached, the special node called as miners, includes the valid transaction into a timestamped block. The block which is included by the miner, is broadcast back into the network.[1] After validating the broadcast block, which contain the transaction, as well as hash-matching it with the previous block in the block chain, the broadcast block is appended to the blockchain..

BLOCKCHAIN-BASED IOT SECURITY AND PRIVACY ISSUES

Authentication

The proposed novel scheme of closed undirected graph authentication supports blockchain based on system identity management.[2] In comparison to other competing authentication schemes, their proposal provides an additional capability of dynamically adding or deleting nodes and edges. In addition, this proposed scheme solves the authentication

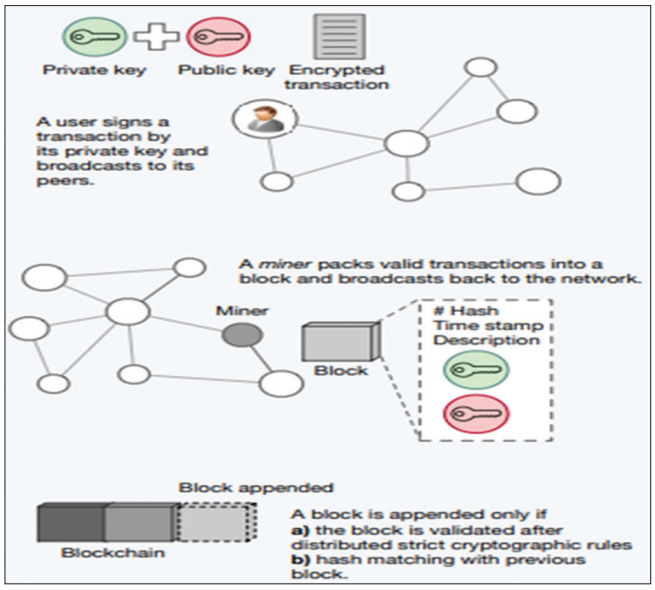

Figure 1: Blockchain working methodology

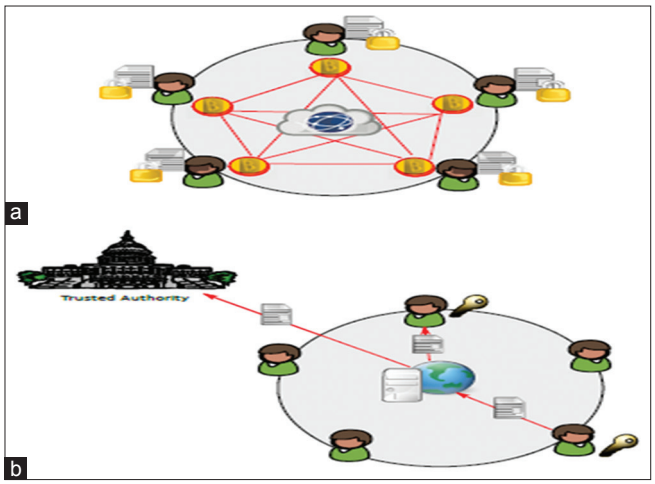

Figure 2: (a) Public blockchain system (b) Private blockchain system

problem that was constructed on Ethereum of non-existent edges, and this will be challenging in transitive signature system. The framework of the blockchain based framework that can ensure a secure remote user authentication. The proposed framework combines attribute-based signatures, multi-receivers encryption Message Authentication Code.[5] The proposed echo announcement is based on a threshold authentication protocol, for novel privacy preserving on announcement network of Vehicular Ad-Hoc Networks.[4] In blockchain, linear identity-based homomorphic signature system can be used for recognizing the authentication. This method would produce a linear homomorphic signature that permits ciphers to avoid the inadequate public key certificates and also it is robust against several attacks.[5,6]

Privacy preserving

In the core of blockchain philosophy lies the private key that can unlock the cryptographic protection of the digital assets. The private key stored on a piece of paper, disk, screen, and local memory in the cloud. Digital wallets can be either hardware or software; for example, keep key or trezor is used by the consumer which are vulnerable to some attacks like error injections.[7] Nowadays, another solution for gaining the ground is the use of cryptoprocessor and hardware security modules (HSMs) that securely protect, store, and create keys. The entire cryptographic key lifecycle happens inside the HSM. HSM operates offline, and also, it can be a standalone device and embedded in a server which has tough against damage or impairment and is usually located in a physically secure area to prevent unauthorized access.[8] To achieve k-anonymity privacy protection, Wang *et al*.[9] use a node cooperation verification approach, in which each group contains K nodes to meet the objective of K-anonymity protection. Aitzhan *et al*[12] proposed a technique for hiding non-content data and protecting the parties from inactive snooping in order to accomplish the transaction in bitcoin withinvolvement of the private key system advancement.[13] Using elliptic curve digital signature algorithm, unforgeability and standard ring signature has an idea to attain the anonymity.[12] In blockchain, the other feature of privacy system is anonymity. The potential network of block chain has utilized for planning a virtually indisputable and tamper-resistant transaction can be viewed with assist of all the nodes.[15]

Trust

Trust-based blockchain payment system is setting in remote region.[14] The proposed scheme is assumed to have an intermittent connectivity to a bank's central system. There is a two-layer architecture which is accomplished by distributed trust. The bank approves a group of selected villagers to act as miners which in turn to approve the transactions among the villagers and the bank. These trust mechanism presents and maintains his own chain of transactions and grows it every participant.[15] The proposed approach provides distributed trust, without the need of any gatekeeper, while being robust against Sybil attacks.

CONCLUSION

This paper has illustrated the blockchain efficiency in terms of high decentralized security and privacy for IoT which is one of the challenging factors to meet a wide expectation of technology for transforming several features of this society economy. This proposed scheme switches the security and privacy intimidations for several IoT devices while seeing the resource constraints. Hence, IoT system moving into decentralized pathway is the right decision. The popular decentralization system of blockchain technology is powerful management process and computation. This can be used to solve many of IoT issues and particularly in security.

REFERENCES

1. Ferrag MA, Derdour M, Mukherjee M. Blockchain technologies for the internet of things: Research issues and challenges. IEEE Internet Things J 2018;2018:1.
2. Lin C, He D, Huang X, Khan MK, Choo KK. A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems. IEEE Access 2018;6:1.
3. Lin C, He D, Huang X, Choo KK, Vasilakos AV. Bsein: A blockchain-based secure mutual authentication with fine-grained

access control system for industry 4.0. J Netw Comput Appl 2018;116:42-52.
4. Li L, Liu J, Cheng L, Qiu S, Wang W, Zhang X, Zhang Z. CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Trans Intell Transp Syst 2018;19:1-17.
5. Lee JH. BIDaaS: Blockchain based ID as a service. IEEE Access 2018;6:2274-8.
6. Lin Q, Yan H, Huang Z, Chen W, Shen J, Tang Y. An ID based linearly homomorphic signature scheme and its application in blockchain. IEEE Access 2018;6:1.
7. Boireau O. Securing the blockchain against hackers. Netw Secur 2018;2018:8-11.
8. This Ultra-Secure pc Self Destructs if Someone Messes with it. Available from: https://www.wired.com/2017/06/orwl-secure-desktop-computer. [Last accessed on 2018 Jun 01].
9. Wang J, Li M, He Y, Li H, Xiao K, Wang C. A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. IEEE Access 2018;6:17545-56.
10. Aitzhan NZ, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans Dependable Secur Comput 2016;15:1.
11. Wang Q, Qin B, Hu J, Xiao F. Preserving transaction privacy in bitcoin. Future Gener Comput Syst 2017;4:14-17.
12. Liu Y, Liu X, Tang C, Wang J, Zhang L. Unlinkable coin mixing scheme for transaction privacy enhancement of bitcoin. IEEE Access 2018;6:23261-70.
13. Fan K, Ren Y, Wang Y, Li H, Yang Y. Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G. IET Commun 2018;12:527-32.
14. Hu Y, Manzoor A, Ekparinya P, Liyanage M, Thilakarathna K, Jourjon G, *et al*. A Delay-Tolerant Payment Scheme Based on the Ethereum Blockchain; 2018. Available from: http://www.arxiv.org/abs/1801.10295.
15. Otte P, de Vos M, Pouwelse J. TrustChain: A Sybil-Resistant Scalable Blockchain. Future Generation Computer System in Press; 2017.

Cite this article: Kumaraguru PV, Chakravarthy VJ, Security And Privacy Issues Based On Blockchain For The Internet Of Things. Asian J Mult-Disciplinary Res. 2019;5(1):17-19.

Source of Support: Nil, **Conflict of Interest:** None declared.