A Dynamic Scalable Blockchain Based Communication Architecture for IoT

Han Qiu[1], Meikang Qiu[2(✉)], Gerard Memmi[1], Zhong Ming[2], and Meiqin Liu[3]

[1] Telecom-ParisTech, Paris, France
{han.qiu,gerard.memmi}@telecom-paristeh.fr
[2] College of Computer Science, Shenzhen University, Shenzhen, China
{mqiu,mingz}@szu.edu.cn
[3] College of Electrical Engineering, Zhejiang University, Hangzhou, China
liumeiqin@zju.edu.cn

Abstract. The recent development of Blockchain based cryptocurrency technology has enabled a high level of trust and security for many applications in people's daily life. Traditional Blockchain architecture can provide decentralized and trustworthy systems for financial services with persistency, anonymity, and auditability guaranteed. Internet of Things (IoT), as the next promising smart system, has the similar decentralized topology with Blockchain. However, deploying Blockchain in IoT system is still unpractical in many aspects. In this paper, we first point out the practical obstacles to deploy Blockchain topology in IoT system. Then a dynamic Blockchain based trust system is proposed to provide a dynamic and scalable communication architecture for IoT networks. We also present a case study to further discuss the security issues and provide future research directions.

Keywords: Blockchain · IoT · Trust · Security · Bitcoin · Privacy

1 Introduction

Blockchain has been an important technology for building trust architecture in many aspects. Blockchain was first introduced in 2008 as the technical foundation for a cryptocurrency known as Bitcoin [10] and since then has been widely used in other cryptocurrencies [11]. As a core technique for all kinds of cryptocurrencies, blockchain is built on a distributed digital ledger of transactions that is owned across all participating entities in a peer-to-peer network. Decentralization is implemented by deploying all participating entities to verify and confirm the new transactions. Once verified, confirmed, and recorded, the transaction data cannot be altered retroactively without alteration of all subsequent blocks, which requires a consensus of the network majority. In the implementation of Bitcoin, all valid transactions records are hashed and encoded into a Merkle tree [10]. Then batches of valid transactions are formed into blocks. Each block includes the hash results of the prior block which links the two adjacent blocks. Then the

M. Qiu (Ed.): SmartBlock 2018, LNCS 11373, pp. 159–166, 2018.
https://doi.org/10.1007/978-3-030-05764-0_17

linked blocks form a chain which is called blockchain [10]. The process of building blockchain is to continuously append new blocks to the existing blockchain which is also referred to mining [11]. The basic operation of mining is to solve a math puzzle (usually *Proof of Work* (PoW) [14]) which is hard-to-solve but easy-to-verify. In order to solve this puzzle, the participating entities must provide huge computation resources which restrict the number of blocks that can be mined. Also, malicious mining of blocks can be further avoided with this mechanism. The popular puzzle used in blockchain is usually or *Proof of Stake* (PoS) [7]. POW demands high computational resources which are deployed in Bitcoin protocol as finding the specific value with specific Hash results [10]. POS will consume both computational and memory resources [7]. All message exchanged between entities are encrypted with deploying changeable Public Keys which can avoid eavesdropping.

Although blockchain can be used into many famous cryptocurrencies such as Bitcoin, there are other potential applications that can deploy blockchain as a fundamental technology. As building blockchain can allow payment done without any trusted intermediary, many financial services such as digital assets, remittance, and smart contracts are developed [17]. In fact, blockchain is becoming one of the most promising techniques for designing the next generation of communication and interaction systems such as *Internet of Things* (IoT) [3].

With the rapid growth of smart devices and bandwidth of wireless networks, the concept of IoT is becoming realized with wide acceptance and popularity [16]. Nowadays, it represents a network where smart "things" having sensors and antennas are connected. As a highly dynamic network, IoT always has the scalability to allow nodes to join and leave the network. In fact, as the IoT paradigm represents a collection of connected devices and heterogeneous networks, it also inherits the traditional security and privacy issues from the computer networks [8]. However, on the other hand, different from traditional computers, IoT devices are usually equipped with constrained resources such as limited power supply, calculation capacity, and storage space [13]. This leads to the issue that the traditional security schemes used in computer networks based blockchain are difficult to be implemented in IoT networks.

One problem in IoT networks is the identity management for the devices. As the very different connection properties of IoT devices such as connection lifetime, service requirement, and trust levels, it is difficult to assign an ID that can universally identify the "things" and to maintain this identification scheme. In fact, blockchain architecture can be deployed as the foundation for further building security and privacy in IoT. The very basic design could be to deploy every IoT node as a participating entity of blockchain which can further build a trusted digital ledger for IoT applications.

In this paper, we first point out the obstacles of building blockchain in IoT networks. Then a system design with a labeled network topology for the IoT ID management is presented to indicate one solution to use a blockchain based protocol in IoT networks.

The roadmap of this paper is given as follows. In Sect. 2, we illustrate the practical problems for using blockchain design in IoT networks. In Sect. 3, we propose the layered network design to deploy blockchain as a foundation for IoT security. In Sect. 5, a brief system evaluation is given and we discuss the future work. We conclude our work in Sect. 6.

2 Research Background

In this section, we first point out the practical obstacle of building a secure IoT system. The conflict between security schemes cost and the practical low overhead requirement for deploying IoT network is discussed. Then the new architecture of blockchain with full nodes and lightweight nodes is introduced.

2.1 One Example of IoT Security Issues

As shown in Fig. 1, the IoT networks are built up by many heterogeneous digital devices with very different hardware configurations which all rely on the communication middle layer to make them connected. Many IoT devices are equipped with two basic elements for data collection and transmission. Some devices such as smartphones are also equipped with powerful calculation chips which can also process collected data.

As pointed out in Sect. 1, although IoT is inherited from the traditional computer networks which also inherit the security and privacy issues, the traditional countermeasures are difficult to inherit. The main reason is not only due to the heterogeneous devices with totally different hardware configurations, but also due to the dynamic communications in IoT concept. One example is given in Fig. 1 that there are devices with constant and dynamic links, and also devices that are always offline or frequently join and leave the networks. In such cases, it is much easier for an attacker to manipulate a compromised node with fake ids to join the communication environment. It is more difficult to manage the id in IoT than in traditional computer networks with such dynamic networks.

A review of security threats is listed in [6]. One of the threats is about the authentication and secure communications in IoT. As shown in Fig. 1, any devices in an IoT network must be authenticated first before they can communicate. However, in practical implementations, due to constrained hardware resources, the overhead of security mechanisms must be minimized to consider the efficiency problems which will further lead to security breaches [9].

2.2 Scalable Blockchain Nodes

As explained in Sect. 1, the foundation of blockchain is that all the transaction records are verified and confirmed in previous blocks which can avoid the deniable operations. This mechanism will require all participating entities in a blockchain network to maintain and more importantly, to store the verified and confirmed transaction records. In fact, once a new entity joins the blockchain network, the

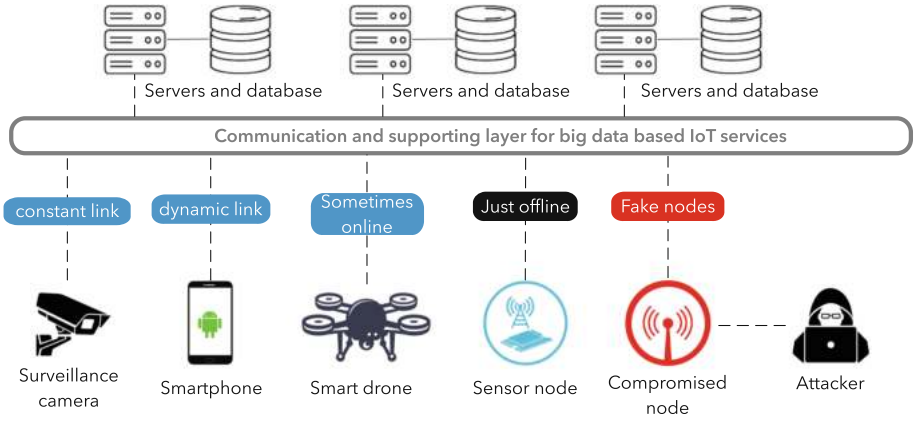

Fig. 1. IoT network with heterogeneous devices and dynamic connections.

download for all history blocks are necessary. However, this feature became the obstacle for deploying blockchain architecture in IoT network. Most devices are calculation and storage limited and the connection links between the IoT nodes are always dynamic which means either maintaining or downloading the history blocks are not practical.

Fortunately, there are new designs for blockchain nodes called full nodes and lightweight nodes in Bitcoin protocols [1]. A lightweight node only downloads the block headers to validate the authenticity of the transactions instead of all the history blocks. Then lightweight nodes are served by full nodes to connect to the blockchain network, they are easy to maintain and run without a heavy overhead.

However, the large deployment of lightweight nodes may lead to privacy issues in IoT. As lightweight nodes are served by full nodes, the malicious users hold the full node will compromise the privacy of transactions from lightweight nodes. Moreover, as the dynamic connections of IoT, once a full node leaves the network, the corresponding lightweight nodes will have problems to enjoy the blockchain network. One work proposed an IoT architecture with smart home settings shown in [4] which uses the devices such as computers in the home as full nodes to serve the lightweight nodes. However, this design fits the topology of smart home scenario which every home is assumed to have personal computers and can be seen as the connection cores for the IoT sub-networks in each smart home.

3 System Designs

In this section, we present a multi-layered blockchain based ID management topology to fit the dynamic IoT network. Different roles for nodes are defined and coordinated to maintain the whole blockchain network. More particularly,

the different devices in IoT network will be assigned with different roles according to the connection life and hardware. Coordination methods are also necessary to guarantee the backup full nodes to serve the lightweight nodes when their full nodes are offline.

First, we see all IoT devices as nodes in a blockchain network. Then an unique ID will be assigned for each IoT device which will be also associated with the blockchain wallet ID. With this design, all valid IDs will be easily verified in IoT network while fake IDs are difficult to be found and refused. Moreover, any malicious actions from IoT devices will be recorded with the ID to defend attackers in the future.

In order to avoid the heavy computation or storage with existing blockchain topology, different nodes should be defined with different IoT device configurations. In this paper, we define three blockchain labels for devices in IoT: lightweight node, full node, and coordination node. Then we classified all devices by assigning different labels according to connection lifetime and hardware configurations. Lightweight node labels are corresponding to the IoT devices that have low computing capacity or have short connection lifetime. Full node labels will require the IoT devices always maintain connecting to the IoT network and have enough calculation capacity and storage space. Coordination node labels are assigned to the devices with long connection lifetime and low calculation capacity.

For example, a surveillance camera as shown in Fig. 2 is the device that has a long connection lifetime and low hardware capacity will be assigned with a coordination node. The computers which are used as the overlay layer in [4] are assigned with full node labels and the blockchain is maintained mainly on them. Then the devices which are dynamic join and leave this IoT network are assigned with lightweight node labels to allow them to participate in this blockchain system while do not need the overhead of full nodes.

By combining the decentralized blockchain topology with identity verification and recording, an IoT ID management system can be created. This system could improve security and reduce malicious behaviors in IoT networks. For any attackers with faked IDs, it will be more and more difficult to continuously maintain the connection to the IoT network as frequently faking different IDs are more difficult and costly. Moreover, considering difficult hardware configurations of the IoT devices, on one hand, the practical implementation is possible while on the othe hand, the trust system with different levels can be built further to manage the connections for different devices. One example would be there are different devices associated with different roles in IoT networks [15] such as center connection nodes or edge nodes.

4 A Brief Case Study

Once a new sensor node wants to join this blockchain network, the first thing is to send a request to the coordination nodes with its label. If it is a full node, then a high level security verification will be required until it gets permission to

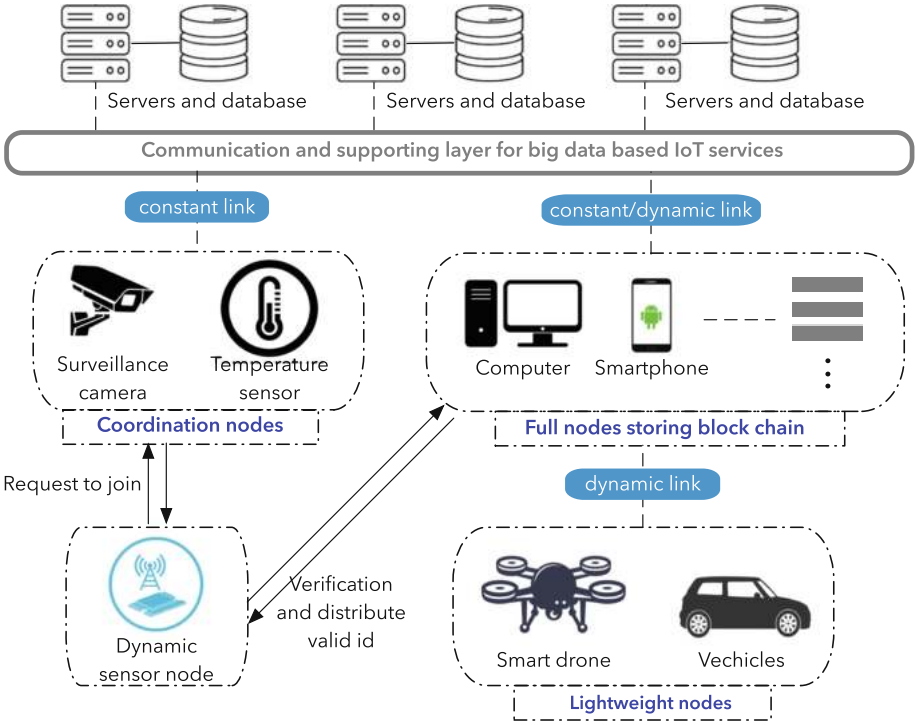

Fig. 2. IoT network with labeled devices and dynamic connections.

join the full node group. If it is a lightweight node, the coordination nodes will distribute a full node that can serve this newcomer. However, the newcomer will not get a valid id to communicate until the verification for the real id. Once a full node goes offline, the coordination nodes will then distribute new full nodes to the lightweight nodes to maintain the connections.

In this section, we assume a threat mode with a malicious user in the IoT network that may manipulate one IoT node by cracking or to fake a node ID to try to access to the IoT network. For the first case, an attacker may be able to compromise and control one IoT node in the network. Many malicious actions may be then reported by other nodes in the IoT network. In such case, the ID of the compromised node will be marked and recorded in the following blocks in the blockchain system. In the following time slots, higher security verification requirements and the lower level of trust will be modified accordingly. Thus, it will be more difficult for the attacker to compromise the same node again in future.

In the other scenario that the attacker connect into the IoT network with a faked ID. If the faked ID is owned by an IoT node that is still active, the verification process on the controller node will refuse the connection to block the attacker out. Even if the attacker manage to connect the IoT network, the report

for the malicious behaviors will let this faked ID be marked as vulnerable and blocked out from this IoT network. If the ID management system is efficient, the attacker will have to frequently change the faked ID to maintain the connection. Thus higher security level will be achieved as the cost for faking IDs will be increasing.

5 Discussions and Future Work

With a blockchain based IoT network, we can record all transactions pertaining to devices in this IoT and stored locally. This information can be very useful for security purpose. For instance, once the attacker wants to fake an id to join the IoT network, the label must be assigned first. If the attacker pretends to be a full node, the high level security verification will find him or make the attack really expensive. Or if the attacker just wants to pretend as a lightweight node, it is also hard because all history is recorded and the attacker must fake everything again for each time trying to attack. However, there are still future works to do which is to define the coordination and switching protocols for lightweight nodes. Also, other situations like when full nodes cannot be trusted must be considered [5].

One further design in IoT with blockchain topology should be not only managing the ID but also protecting the information exchanged in the IoT network. For example, data sharing and verification protocols must be designed to further guarantee the IoT network security. As IoT devices have very different hardware configuration that uniform simple encryption algorithm is difficult to implement, authentication and verification are important to guanratee the security of data sharing. Lightweight encryption methods [12] should also be introduced as supplementary methods for security for some specific use cases [2]. Also, more work in future need to be done for test the system performance and practical possibility to deploy such architecture in real IoT environment.

6 Conclusion

In this paper, we presented the obstacle of deploying blockchain technology into IoT networks. We proposed an IoT system architecture with practically labeling all IoT devices which can map them to the full nodes and lightweight nodes concepts in blockchain protocol. Then we evaluated that this design could enhance the security level by managing the IDs of IoT devices while increases the difficulty for attackers to fake IoT nodes.

Acknowledgement. Dr. H. Qiu and Prof. G. Memmi are supported by BART: Blockchain Advanced Research & Technologies teamed up by Telecom-ParisTech, Inria, IRT SystemX and Telecom-SudParis. This work is also partially supported by China NSFC 61836005 and 61672358; China NSFC 61728303 and the Open Research Project of the State Key Laboratory of Industrial Control Technology, Zhejiang University, China (ICT1800417). Prof. M. Qiu is the corresponding author.

References

1. Antonopoulos, A.M.: Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media Inc., Newton (2014)
2. Dai, W., Qiu, L., Wu, A., Qiu, M.: Cloud infrastructure resource allocation for big data applications. IEEE Trans. Big Data **4**(3), 313–324 (2018)
3. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: 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), pp. 618–623. IEEE (2017)
4. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: LSB: a lightweight scalable blockchain for IoT security and privacy. arXiv preprint arXiv:1712.02969 (2017)
5. Gai, K., Qiu, M.: Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers. IEEE Trans. Ind. Inform. **14**(8), 3590–3598 (2018)
6. Khan, M.A., Salah, K.: IoT security: review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. **82**, 395–411 (2018)
7. Kiayias, A., Russell, A., David, B., Oliynykov, R.: Ouroboros: a provably secure proof-of-stake blockchain protocol. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10401, pp. 357–388. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63688-7_12
8. Li, C., Qiu, M.: Reinforcement Learning for Cyber Physical Systems with Cybersecurity Case Studies. Chapman & Hall/CRC, Boca Raton (2018)
9. Mahalle, P.N., Anggorojati, B., Prasad, N.R., Prasad, R., et al.: Identity authentication and capability based access control (IACAC) for the Internet of Things. J. Cyber Secur. Mobil. **1**(4), 309–348 (2013)
10. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008)
11. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S.: Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, Princeton (2016)
12. Qiu, H., Memmi, G., Noura, H.: An efficient secure storage scheme based on information fragmentation. In: 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 108–113. IEEE (2017)
13. Qiu, M., Gai, K., Thuraisingham, B., Tao, L., Zhao, H.: Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry. Future Gener. Comput. Syst. **80**, 421–429 (2018)
14. Vukolić, M.: The quest for scalable blockchain fabric: proof-of-work vs. BFT replication. In: Camenisch, J., Kesdoğan, D. (eds.) iNetSec 2015. LNCS, vol. 9591, pp. 112–125. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-39028-4_9
15. Wu, D., Arkhipov, D.I., Asmare, E., Qin, Z., McCann, J.A.: UbiFlow: mobility management in urban-scale software defined IoT. In: 2015 IEEE Conference on Computer Communications (INFOCOM), pp. 208–216. IEEE (2015)
16. Zhang, Y., Qiu, M., Tsai, C.W., Hassan, M.M., Alamri, A.: Health-CPS: healthcare cyber-physical system assisted by cloud and big data. IEEE Syst. J. **11**(1), 88–95 (2017)
17. Zheng, Z., Xie, S., Dai, H.N., Wang, H.: Blockchain challenges and opportunities: a survey. Work Pap.-2016 (2016)