IoT Privacy Preservation Using Blockchain

Subjects: Computer Science, Interdisciplinary Applications
Contributor: Zainab Iftikhar

IoT uses a large number of devices and most of these devices are resource-constrained. Blockchain being light-weighted is a great solution for privacy preservation in resource-constrained devices. The privacy aspect of blockchain comes from its ability to provide transparency in a distributed network.

Keywords: blockchain ; consensus ; IoT ; smart contracts ; bitcoin

1. Introduction

IoT ’s privacy and security with interconnected devices causes security challenges in the area of network computing. It means at any moment from anywhere, an attack can be launched on these devices that includes threats like denial of service, fabrication of identity, physical threats, communication channel targeting and many more. One of the biggest challenges in this research field is consumption of power resources and computational overheads on IoT devices. Many solutions have been proposed by the researchers in which strategies based on blockchain, homomorphic encryption, and attribute-based encryption are provided.

The exchange of data among physically connected devices related to their infrastructure and behaviors in the form of groups is known as IoT. From the Gartner report shown in **Table 1** , it was expected that almost 5.8 Billion interconnected devices would be having a vast share in market of $3 trillion in 2020 [1], while the forecasts of international data co-operation report that the expected market value of IoT devices is $1.1 trillion for 2023—the market of full stack systems, like RIOT [2] and Contiki [3] that enabled IoT devices functionality, is also expected to expand.

Table 1. IoT endpoint market by segment, 2018–2020, worldwide (in billions) [1].

Segment	2018	2019	2020
Utilities	**0.98**	**1.17**	**1.37**
Govt	**0.40**	**0.53**	**0.70**
Building automation	**0.23**	**0.31**	**0.44**
Physical security	**0.83**	**0.95**	**1.09**
Manufacturing and natural resources	**0.33**	**0.40**	**0.49**
Automotive	**0.27**	**0.36**	**0.47**
Healthcare providers	**0.21**	**0.28**	**0.36**
Retail and wholesale trade	**0.29**	**0.36**	**0.44**
Information	**0.37**	**0.37**	**0.37**
Transportation	**0.06**	**0.07**	**0.08**
Total	**3.96**	**4.81**	**5.81**

IoT brings improvement in quality of life in various domains. IoT devices play a huge role in different aspects of life, for example security, energy, safety, healthcare, smart grid, VANETs, industry and entertainment, but in terms of battery power, network protocol, complex computation and infrequent connectivity, these devices are fundamentally constrained in resources.

One of the most important features of blockchain is decentralization. It is also used as a consensus mechanism to enable trust between all parties involved in decentralized networks, one example is cryptocurrency—for example, Bitcoin and Ethereum. IoT devices are decentralized and hence can be benefited by the blockchain.

2. Blockchain

Blockchain is divided into three categories, public blockchain, which is permissionless, private blockchain, which is permissioned and consortium blockchain, which is a combination of both. All types provide immunity against malicious and faulty ledger users. **Table 2** shows properties of all four types of blockchain. Their detailed example is presented in [4] by T. M. Fernández et al. Strengths of blockchain include accuracy, cost reduction, decentralization, efficiency, immutability, transparency and privacy.

Table 2. Types of blockchain and their properties.

Properties	Public Blockchain	Private Blockchain	Consortium Blockchain	Hybrid Blockchain
Access Restrictions	**Permissioned for public**	**Permission needed to join the network**	**Permissioned**	**Permissioned**
Transaction Restrictions	**Permissioned for public**	**Restricted**	**Customized**	**Customized**
Mining	**Permissioned for public**	**Restricted**	**Customized**	**Customized**
Decentralization	**Fully decentralized**	**Centralized**	**Less centralized than private, and less decentralized than public blockchain.**	**Decentralized**
Need for a Controlling Entity	**None**	**Managed by a single organization**	**Managed by multiple organizations**	**Public and private module**
Transparency	**Yes**	**No**	**Little transparency**	**Little transparency**
Incentive for mining	**Yes**	**No**	**No**	**No**
Examples	**Bitcoin, Ethereum, Litecoin, NEO**	**Hyperledger and R3 Corda, Multichain, Hyperledger Sawtooth**	**Marco Polo, Energy Web Foundation, IBM Food Trust**	**Dragonchain, XinFin's Hybrid blockchain**
Uses	**Voting, fund raising**	**Supply chain management**	**Banking, Research**	**Retail, Real estate**

Figure 1 shows some applications of blockchain in different fields, including IoT, healthcare, finance, agriculture and cryptocurrency.

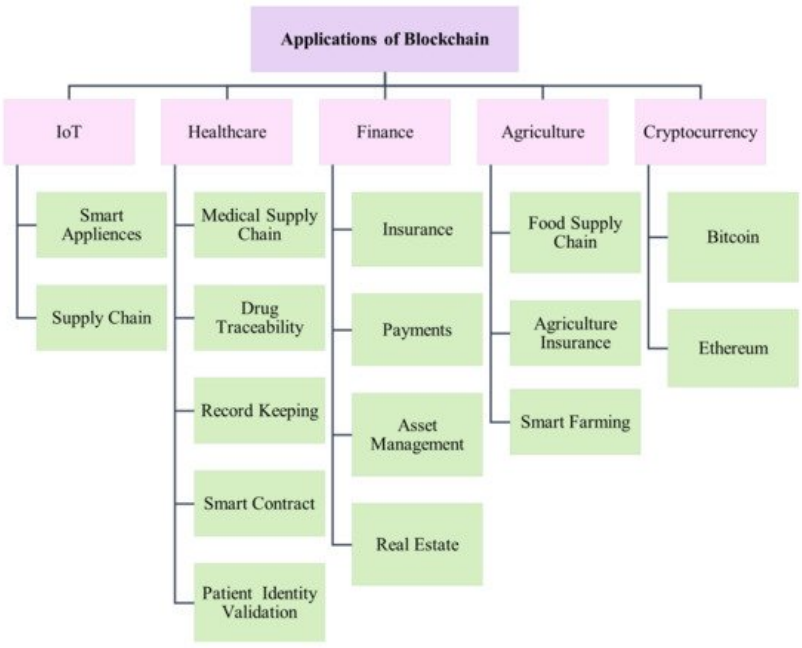

Figure 1. Applications of Blockchain.

Although it is infeasible to discuss all applications, we describe some of the most important applications of blockchain in the following subsections.

As blockchain ensures secure storage and immutability, it makes exchanging of funds more secure. Transactions, using blockchain, become transparent and private.

3. Integration of Blockchain and IoT

Many researches integrate blockchain in IoT to enhance security and provide an efficient data storage system. In [5], authors review the recent literature on blockchain's integration with IoT. It is pointed out that blockchain helps to improve security and scalability in IoT scenarios. In [6], authors highlight some attacks that IoT systems are prone to, and review the researches that use blockchain to mitigate privacy-related issues in IoT.

A blockchain-based architecture for IoT privacy preservation is proposed by Rahulamathavan et al. [7], in which an attribute-based encryption has been used with Testbed platform to achieve data privacy and confidentiality, but there is a slight time increase due to involvement of multiple attribute authorities and using PoW consensus mechanism.

As IoT consists of billions of devices accross the world, it poses serious threats to the privacy of the users. Other than providing decentralization, consensus and smart contracts for IoT, blockchain is being used at a large scale to assure privacy preservation in IoT. **Table 3** presents a summary of recent researches based on the scheme utilizing blockchain for privacy preservation in IoT.

Table 3. Recent research on blockchain-based privacy preservation in IoT.

Ref#	Model	Limitations	Parameters	Strengths	Tools-Technology
[8]	Software defined networking for IoT	Lack of location privacy	Distributed blockchain cloud architecture	Dos/Dos attacks, Data protection, Access control, reduced end to end delay between IoT devices	SDN controller, 6 desktops, 64 Gb DDR3 ram, intel i7
[9]	Collaborative video delivery	Lack of privacy and anonymity	Smart contracts	Provide requested service through network service chains	Hyperledger fabric, pbft consensus, CLCs
[10]	Crowd sensing app	Collusion attacks	whitewashing attack, QAIM	privacy preserving, impersonation attacks	K anonymity, server with k nodes, EM algo in Ubuntu 16.04 environment
[11]	Scalable access management	Cryptocurrency fees, processing time	Mobility, accessibility, concurrency, lightweight, scalability, transparency	Access control	Ubuntu 16.04 desktop, intel core i7 -950, 3.07 !GHz
[12]	Secured Grid monitoring	Lack of location privacy	Sovereign blockchain network, cryptographic keys	Data integrity, data confidentiality, data provenance and auditing	Smart contracts, sha256, smart meters
[13]	Internet of Energy	data provenance and auditing	SCADA network, data encryption and broadcast	False data injection attacks	54 generators, 118 nodes, 186 branches, 676 communication channels, 676 sensors.
[14]	Consortium blockhain in industrial IoT	Lack of privacy and anonymity, optimal energy aggregator selection	Optimal pricing, credit-based payment	Secure energy trading	50 pairs if IIoT nodes, Traditional blockchain, EAGs
[15]	Decentralized energy trading through multisig and BC	Collusion attacks	Anonymous encrypted message streams,	Privacy, double spending attacks	Python 2.7 with bitcoinlib, libbitcoin toolkit, PYBitmessage API, pysolar
[16]	Consortium BC in Mobile devices	Lack of privacy and anonymity	Fuzzy comparison method, MFM	Malware detection	Intel core i7-3770, 16 GB, Ubuntu 15.10, DREbin dataset
[14]	Secure firmware in IoT environment	Data credibility assessment	Remote firmware updates, p2p sharing	Firmware verification and update	BAN logic, Scyther tool, merkle tree

Ref#	Model	Limitations	Parameters	Strengths	Tools-Technology
[17]	Bitcoin	Public key privacy	Paillier cryptosystem, Overlay attack, Double-spending attack	Provably Secure	Multi-layered Linkable Spontaneous Anonymous Group signature (MLSAG), ring signature

4. Future Research Directions and Challenges

Privacy preservation is important because users' data is collected by almost all IoT devices. We present some future research directions in terms of privacy preservation.

In order to provide security and privacy, integration of the Tangle in IoT can be very useful. Tangle is a data structure that IOTA is based on. It utilizes a directed acyclic graph and utilizes less energy as compared to a blockchain network. IOTA is light-weighted and quantum resistant. Another important advantage is that IOTA does not need miners. The network participants issue new transactions without having to involve another node that has better computing resources. Having no miners makes IOTA fee-less.

Strong privacy preservation is still a challenge when using blockchain. For example, in order to resist Sybil attack, a certain amount of honest participants are required in decentralized mixing protocol. Hawk reinitializes and creates a different trusted process for every smart contract, so privacy preservation having few trust assumptions needs to be enhanced.

A single security solution for all blockchain-based IoT devices cannot fulfill security requirement due to resources-constrained nature of devices. The designs of such kinds of frameworks are required to provide dynamic and adaptable security. Implementation of other privacy preserving solutions, such as data anonymization and differential privacy along with blockchain, can provide better privacy. A framework is needed that can preserve privacy using both the techniques, keeping resource-constrained nature of IoT devices in mind.

References

1. Gartner, R. Forecast: The Internet of Things, Worldwide, The Internet of Things; Forecast: Egham, UK, 2017.
2. Baccelli, E.; Hahm, O.; Günes, M.; Wählisch, M.; Schmidt, T. RIOT OS: Towards an OS for the Internet of Things. In Proceedings of the 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Turin, Italy, 14–19 April 2013; pp. 79–80.
3. Dunkels, A.; Gronvall, B.; Voigt, T. Contiki-a lightweight and flexible operating system for tiny networked sensors. In Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, Tampa, FL, USA, 16–18 November 2004; pp. 455–462.
4. Fernández-Caramés, T.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. IEEE Access 2018, 6, 32979–33001.
5. Wang, X.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Niu, X.; Zheng, K. Survey on blockchain for Internet of Things. Comput. Commun. 2019, 136, 10–29.
6. Hassan, M.; Rehmani, M.; Chen, J. Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Gener. Comput. Syst. 2019, 97, 512–529.
7. Rahulamathavan, Y.; Phan, R.W.; Rajarajan, M.; Misra, S.; Kondoz, A. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In Proceedings of the 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bhubaneswar, India, 17–20 December 2017; pp. 1–6.
8. Sharma, P.; Chen, M.Y.; Park, J. A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. IEEE Access 2018, 6, 115–124.
9. Herbaut, N.; Negru, N. A Model for Collaborative Blockchain-Based Video Delivery Relying on Advanced Network Services Chains. IEEE Commun. Mag. 2017, 55, 70–76.
10. 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, 17545–17556.
11. Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. IEEE Internet Things J. 2018, 5, 1184–1195.

12. Gao, J.; Asamoah, K.; Sifah, E.; Smahi, A.; Xia, Q.; Xia, H.; Dong, G. Gridmonitoring: Secured sovereign blockchain-based monitoring on smart grid. IEEE Access 2018, 6, 9917–9925.
13. Liang, G.; Weller, S.; Luo, F.; Zhao, J.; Dong, Z. Distributed blockchain-based data protection framework for modern power systems against cyber attacks. IEEE Trans. Smart Grid 2018, 10, 3162–3173.
14. Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium blockchain for secure energy trading in industrial Internet of things. IEEE Trans. Ind. Inform. 2017, 14, 3690–3700.
15. Aitzhan, N.; Svetinovic, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans. Dependable Secur. Comput. 2016, 15, 840–852.
16. Gu, J.; Sun, B.; Du, X.; Wang, J.; Zhuang, Y.; Wang, Z. Consortium blockchain-based malware detection in mobile devices. IEEE Access 2018, 6, 12118–12128.
17. Wang, F.; Hu, L.; Hu, J.; Zhou, J.; Zhao, K. Recent advances in the Internet of things: Multiple perspectives. IETE Tech. Rev. 2017, 34, 122–132.
