# Scalable Blockchain-based Data Storage in Internet of Things

Wei Liu, Haojun Huang, Hao Yin, Geyong Min, Yunhao Yuan, and Dapeng Wu

***Abstract*—Internet of Things (IoT) as a ubiquitous networking paradigm has been experiencing serious security and privacy challenges with the increasing data in diversified applications. Fortunately, this will be, to a great extent, alleviated with the emerging blockchain, which is a decentralized digital ledger based on cryptography and has offered potential benefits for IoT. Currently, the resource limitations of IoT devices have prevented blockchain from flexibly storing the ever-increasing IoT data. To address this challenge, in this article, we introduce a scalable blockchain paradigm with cloud/fog/edge services and virtualization technology, and develop an innovative scalable blockchain-based architecture of IoT data storage (SBIT) to tackle its security and scalability concerns, through on-chain block validation in IoT and off-chain data storage in cloud/fog/edge servers. We start by investigating the traditional IoT and identifying the existing issues related to its security and scalability. Then, we explicitly present the details of the scalable blockchain and SBIT, along with a case study. Finally, we summarize the emerging challenges and discuss the future directions for further research on blockchain-based IoT.**

***Index Terms*—Internet of Things, blockchain, data storage, scalability, security.**

## I. Introduction

INTERNET of Things (IoT) is composed of diversified smart devices connected with embedded software and protocols to collect and exchange data in networks. Generally, most of these devices are heavily constrained by computing, storage, and bandwidth resources, and not capable of storing ever-increasing data, which often contains critical security and privacy-sensitive information [1], [2]. As a result, IoT cannot largely fulfill the Quality-of-Service (QoS) requirements of real-world applications and is vulnerable to a variety of cyber attacks. The typical examples of attacks include black hole, information injection, Denial of Service (DoS), and Distributed DoS (DDoS) [1]. There are a large number of solutions proposed to alleviate these problems [3], [4], [5]. However, despite their great benefits, it is practically impossible for them to fully achieve the desired targets due to the nature of the centralized architecture of IoT and the lack of trust between the resource-limited entities. This necessitates us fundamentally to rethink how IoT should be structured and innovated especially for its data storage.

TABLE I: The typical blockchain-based initiatives in IoT

| Years | Solutions | Main focuses/contributions |
|---|---|---|
| 2019 | [6] | The security of data trading ecosystems. |
| 2019 | [7] | The blockchain-based framework for IoT security. |
| 2020 | [5] | The scalability and security of IoT. |
| 2020 | [8] | The authentication management of IoT. |
| 2021 | [9] | The scalability and security of IIoT. |
| 2022 | [4] | The flexible data sharing in future networks. |
| 2022 | [10] | The secure and low-latency computation offloading of PIoT with blockchain and DRL. |
| 2022 | [11] | The secure data storage and sharing in IToT. |
| 2023 | [12] | The decentralized, fair and authenticated information sharing in IoT. |
| 2023 | [13] | The blockchain virtualization for interoperable computations in IIoT. |
| - | - | The scalable blockchain-based data storage with cloud/fog/edge services and technology. |

Nowadays, the emerging blockchain, which has possessed innovative features like decentralization, trustless and tamper-resistance, has been regarded as a disruptive paradigm to tackle the above-mentioned challenges [1], [6]. It is becoming an important essential of IoT, where the data generated in IoT is distributedly stored in the form of blocks. In reality, there exist many blockchain-based initiatives from academia and industry [10], [11], [9], [8], [6], [7], [13], [12], illustrated in Table I, to promote diversified IoT applications from network security, scalability, computation offloading, blockchain virtualization, data sharing, etc. Unfortunately, among them, the resource limitations of smart devices, which always are responsible for block establishment known as block creators, have not been well mitigated or taken into account [1]. The ever-growing IoT data stored in the selected block creators, each of which maintain and store one copy of blockchain, will result in rapid resource exhaustion and failure of block establishment. Furthermore, most of these blockchain-based initiatives often leverage the popular consensus protocols, for example, Proof of Work (PoW), Proof of Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT) [1], [7], which require heavy computation and communications in operations, to coordinate IoT devices in network interactions and block establishment. These will weaken the security of decentralized architecture of blockchain-based IoT, and hinder its scalability with the increasing number of the collected data and devices [2], [11]. So far, the benefits of blockchain-based IoT have not been fully excavated and employed for data storage, due to the resource-constrained smart devices. It is required to introduce additional storages and a set of resource-constrained devices

Liu Wei and H. Huang (corresponding author) are with Hubei Key laboratory of Smart Internet, Huazhong University of Science and Technology, Wuhan 430072, China. H. Huang is also with the Department of Computer Science, University of Exeter, Exeter, EX4 4QF, UK (E-mail: liuwei@hust.edu.cn; hjhuang@hust.edu.cn).

H. Yin is with Tsinghua University, Beijing 100084, China (E-mail:h-yin@mail.tsinghua.edu.cn).

G. Min is with the University of Exeter, Exeter EX4 4QF, UK (E-mail: g.min@exeter.ac.uk).

Y. Yuan is with Aalto Univeristy, Espoo 02150, Finland (E-mail: yunhao.yuan@aalto.fi).

D. Wu is with the City University of Hong Kong, Hong Kong (E-mail: dapengwu@cityu.edu.hk).

instead of individual entities to jointly establish and maintain blocks, enabling IoT data to be distributively and securely stored in networks.

Motivated by this observation, in this article, we present a scalable blockchain paradigm with cloud/fog/edge services and virtualization technology and propose an innovative scalable blockchain-based architecture of IoT data storage (SBIT) to resolve these challenges. Distinguished from the previous initiatives, each data in SBIT is on-block verified by the selected virtualized super-devices in IoT and distributively off-block stored in the collaborative servers, enabling secure and scalable IoT data storage. The third-party storages instead of individual resource-constrained IoT entities are introduced to jointly establish and maintain each block. The data included in the created blocks is presented with the hash value of its raw data, with a fixed length, resulting in significant consumption reductions of IoT resources. Under the proposed architecture, a case study with the ever-increasing data, along with the popular IoT attacks, has been implemented to demonstrate how the scalable blockchain can benefit IoT from scalability and security. Besides, we discuss the existing challenges and the future directions on scalable blockchain-based IoT.

The remainder of this article is organized as follows. In the following section, we mainly illustrate the existing issues in IoT and potential solutions triggered by blockchain. Then we introduce a scalable blockchain paradigm. Following that, we present the detailed design of SBIT, along with a case study. Finally, we outline discuss the emerging challenges and the future directions for further research, followed by the conclusion of this article.

## II. Challenges in IoT and Blockchain-based Solutions

### A. Existing Challenges in IoT

**Device security.** Numerous IoT devices, ranging from low-power facilities to high-performance servers, are allowed to access the Internet while without device security in mind, thereby making them easy targets of malicious attacks. Today, the new botnets, which control IoT devices to mine blocks, are appearing. All these indicate that many IoT devices suffer from security issues.

**Privacy leakage.** IoT data is originated from almost all aspects of human activities and often includes sensitive information, referring to personal locations, health conditions, financial situations, etc. Thus, it is easy to infer personal habits, behaviors and preferences from such data. Currently, most mobile servers and network providers are collecting such sensitive data, which raises severe privacy concerns. Furthermore, it might be manipulated and shared to interested parties while without their legal permissions, leading to privacy leakage.

**Centralization management.** IoT is heavily dependent on centralized communication model to identify, authenticate and connect devices, which makes it difficult to manage and maintain the ever-growing devices in a centralized manner. Besides, it will encounter intermittent communication barrier even if the economic and engineering factors are not considered, since large traffic would disrupt the critical network exchanges.

**Network heterogeneity.** IoT is characterized by heterogeneity and usually operates with the tight-coupling hardware and software [1]. Different devices and platforms installed a variety of long/short-range communication protocols like Zigbee, NB-IoT and LoRa will work together. As a result, it is difficult for IoT to recognize the emerging devices and interact with other components in an efficient manner.

**Trustless cooperation.** Due to the limited computing and network resources, numerous IoT devices need to perform the desired tasks together. Thus, each device ought to connect and communicate with others via wireless communications. However, there is no built-in trust mechanisms among different IoT devices to enable secure environments. It is impractical for non-confident devices to work closely and prevent their further inter-corporations.

### B. Rethinking IoT Triggered by Blockchain

The above-mentioned challenges congenitally exist in IoT associated with its highly centralized architecture, and necessitate fundamentally rethinking how IoT should be structured. Fortunately, this will be, to a great extent, alleviated with the emerging blockchain, which represents one of the most promising candidate technologies to establish a secure and distributed ecosystem for IoT.

Essentially, blockchain is a Peer-to-Peer (P2P) distributed ledger that includes an even-growing list of blocks to enable non-confident parties to maintain a set of global identical states. Each block is generally composed of two parts: block header and block body. The block header contains an identifier of the previous block, Merkle root, timestamp, etc. The block body stores a set of encrypted data, often called as transactions broadcast in networks, through the signature of senders in a decentralized network and combines the records in the form of a Merkle tree. All data is spread and verified across the networks in a P2P manner. The valid data will be added into blocks and attached to the blockchain with the distributive consensuses like PoW, PoS and PBFT [1], [7], which exploit the whole storage/computing power of networks to guarantee the immutability of this data. The salient features which turn blockchain into something with the potential of fundamentally innovating IoT include: security, privacy, decentralization management and control, adaptability and trust.

With these prominent characters, blockchain-based IoT will to a large extent overcome the limitations of traditional IoT. One example for applying blockchain into IoT is smart grid [14]. The inherent decentralized blockchain makes it a natural fit to overcome the single-point-of-failure problem, enhancing security and flexibility of smart grid systems. With the distributed consensus [15], blockchain enables heterogeneous IoT devices to establish trust without a trusted third party, which could significantly reduce the dedicated server costs of maintenance and operation. Furthermore, the smart contracts, referring to user-defined program codes, can be used for negotiation between service providers and users, facilitate energy trading among them. All participants will benefit from the adopted blockchain, while suffering from the scalability issue with the ever-increasing data due to the resource limitations of smart devices.

## III. Scalable Blockchain

Based on the abovementioned observations, we argue that exploiting blockchain can embrace IoT, by establishing a scalable blockchain-based decentralized IoT system for its data storage. Therefore, we explicitly present a scalable blockchain paradigm, which emphasizes the scalability of blockchain, including three kinds of public, private and federated blockchains, for IoT data storage, in consideration of the resource limitations of IoT devices. It establishes a distributed reference system for network architects, network operators, application designers, and customers to store, share and utilize IoT data.

The scalable blockchain is built on the IoT devices, cloud/fog/edge servers and virtualization techniques. The scalability of it is achieved by extending the storage space of IoT into cloud/fog/edge services and off-chain storing each IoT data in multiple cloud/fog/edge servers, which interact with IoT via WiFi, 5G and beyond, as well as Internet. The proposed blockchain, compatible with different types of blockchains, provides SBIT with not only secure and privacy-preserving network environments and the extended storage space beyond IoT, but also decentralized network control and management. To enable normal blockchain establishment, a set of resource-limited devices in IoT will be virtualized and integrated into super-devices to act as the block creators. All collected data in IoT will be encrypted and sent to cloud/fog/edge servers, rather than being stored in block creators or IoT, resulting in significant storage and network resources reduction for IoT. The data transactions in this process will be recorded by the super-devices and encrypted with hash function, computed with the fixed number of words, and then included into the created blocks.

The framework of the scalable blockchain is illustrated in Fig. 1, which include data layer, consensus layer, incentive layer and contract layer. The data layer aims to design blockchain, referring to block structure, chain structure, hash algorithm, tree, timestamp, etc. The consensus layer, running on top of the network layer of IoT, is used for all participants to reach consensuses in block creation and data exchange between IoT and cloud/fog/edge servers. The incentive layer is to incentivize participants to devote to the blockchain creation in an economic manner, referring to the issuance and distribution mechanisms of economic incentives for IoT and cloud/fog/edge facilities. The contract layer is for all devices to intelligently execute instructions ordered by applications, mainly in the form of smart contracts.

The scalable blockchain works as follows. Firstly, it will arrange a set of super-devices to record all data transactions occurring in networks, referring to data exchange between different parities and data storage in cloud/fog/edge servers, and then distributively stores such records in these super-devices in the form of hash function. After that, it adopts appropriate distributive consensuses like PoS, DPoS and PBFT to reach agreements in block creation in IoT. In this process, different economic incentives will be executed at the incentive layer to incentivize participants who devote to the blockchain creation. To adaptively control the data storage, the smart contracts,

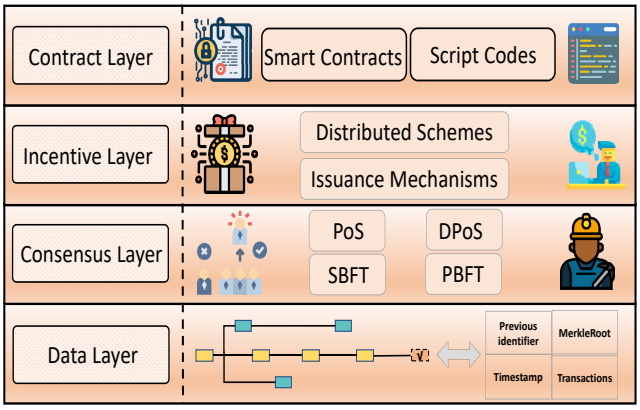


Fig. 1: The framework of the scalable blockchain in IoT.

which essentially are flexible programming applications, will be used to specify any functionality automatically executed on super-devices under certain conditions.

## IV. SBIT: Framework and Components

Fig 2 illustrates SBIT, a scalable blockchain-based IoT architecture of data storage, which includes device layer, network layer, application layer, clould-fog-edge layer, and blockchain layer. The high-volume data collected in IoT will be encrypted and on-chain verified by a set of selected block creators, each of which is an IoT super-device built on a number of virtualized resource-limited smart devices, and distributively off-chain stored in the collaborative cloud/fog/edge servers beyond IoT, which are the extensive services of tradition IoT. Each data will be stored in multiple cloud/fog/edge servers, rather than only one, avoiding the risk of single-point-of-failure in data utilization. The amount of backups of such data depends on their residual resources and the desired trade-off between data storage expenditure and performance. Each backup of session flow, which includes much data collected from a same device, will be stored in the same or adjacent cloud/fog/edge servers, and its data transactions will be sent to the block creators and stored in blockchain in the form of hash function. All data transactions between IoT devices and cloud/fog/edge services will be proportional to the size of IoT data but smaller than it, and sent to the selected block creators. This means that the number of data transactions is fewer than the overall workflow of the system, referring to the IoT data sent to cloud/fog/edge servers for storage, and have little lightweight impacts on the overall workflow of the system. The smart contracts included in SBIT will automatically execute instructions for block establishment in IoT and data storage in cloud/fog/edge servers. The choice of cloud/fog/edge storage is mainly dependent on their storage expenditure and QoS as well as the performance requirements of such data. For example, the edge services would be utilized if the real-time feedback from the storage devices is required or it is too far from the cloud/fog servers. These bring SBIT capacity of scalable, secure and privacy-preserving data storage.

The blockchain layer is built on the proposed scalable blockchain, and closely interacts with other four function layers. The main function of it is to process and store

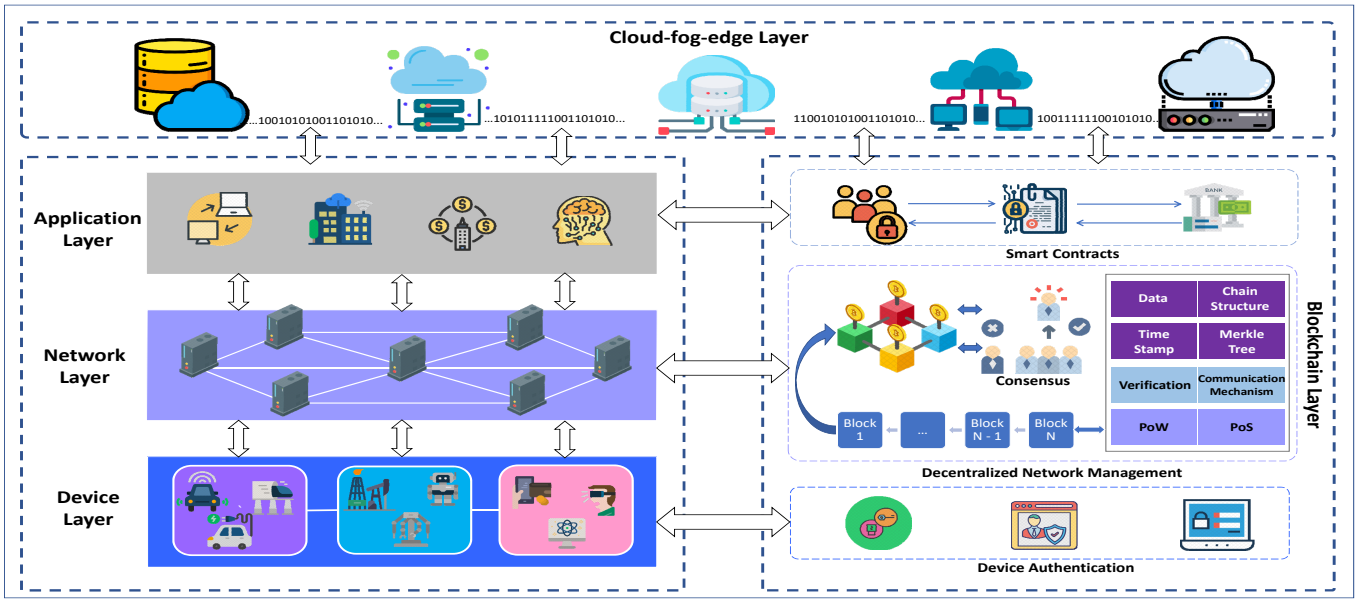


Fig. 2: The architecture of SBIT, which includes device layer, network layer, blockchain layer, application layer, and clould-fog-edge layer for scalable blockchain-based data storage.

all encrypted data transactions, verify data storage, execute blockchain establishment, and conform the created blocks to ensure data security. The blockchain layer can introduce security and scalability features of the scalable blockchain into the device, network, application, and clould-fog-edge layers of SBIT for off-chain data storage, including identity authorization at the device layer, decentralized network management at the network layer, smart contact at the application layer, and distributively data storing at the clould-fog-edge layer.

The device, network and application layers posses almost the same functions of the traditional IoT but in decentralized and secure manners, and closely interact with the blockchain layer to distributively collect, process, exchange, store and exploit IoT data. The device layer, consisting of a large number of smart devices equipped with sensors and actuators, takes charge of data sensing, data collection, local data processing and offloading. A smart device can either process the collected IoT data locally, or offload it to the clould-fog-edge layer for its off-chain processing and storage. The network layer is mainly responsible for the reliable data transmission back and forth over the network and data sharing with the upper layers. The application layer that interacts with IoT devices provides the personalized or industrialized services through smart contracts, which links the gap between users and applications. The clould-fog-edge layer mainly devotes to efficient data processing, analysis and storage in cloud/fog/edge servers.

The data storage of SBIT includes five steps: block creator election, data transmission, transaction record, data storage, and block establishment. In step 1, a set of super-devices built on the virtualized resource-limited devices have been selected as the block verifiers and creators at the blockchain layer, initiated by the smart contracts of the blokchain layer. In step 2, the IoT data collected from different smart devices will be local processed and encrypted at the device layer, and sent to cloud/fog/edge servers over the network layer. Step 3 is responsible for keeping a record of all such encrypted data delivered to cloud/fog/edge servers in the form of candidate blocks at the blockchain layer. Step 4 takes charge of data storage in cloud/fog/edge servers at the clould-fog-edge layer, along with a number of feedbacks regarding the storage information to super-devices. On this basis, the selected super-devices devote to the block creation at the blockchain layer with the receiving records marked with different timestamps and the data storage information in step 5.

In addition to execution IoT data storage in cloud/fog/edge servers, the functions of SBIT by combing blockchain layer with three layers of IoT also include:

**Secure device management at the device layer.** The scalable blockchain, seamlessly integrating with the device layer, is mainly responsible for authenticating the devices as legal users to access and communicate with others and preventing themselves from malicious attacks, using asymmetric cryptography, timestamped records, pseudo-anonymous and distributed consensus. This enables users to interact with others in a trustless environment, mitigating the risk of the remote control, thereby intensifying the security and privacy of IoT.

**Decentralized network control and management at the network layer.** Without relying on a trusted intermediary, the scalable blockchain is mainly responsible for secure data confirmation and information exchanges back and forth over the networks. It can distributively manage and control networks by introducing a set of P2P devices, which do not fully trust each other, through consensus mechanisms, enabling credible and available network resources open to massive non-confident users and avoiding the risk of single-point-of-failure.

**Automatic commitment execution at the application layer.** SBIT will allow many event-driven applications designed for identity management, mobile-crowd sensing, Industry 4.0 and Internet of Energy to be execute at the application

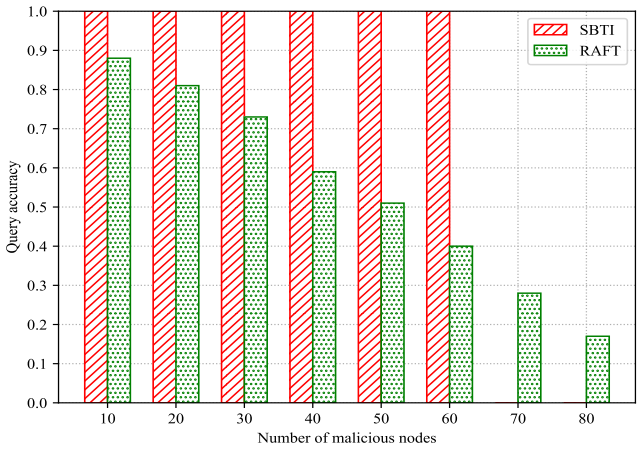


Fig. 3: Query accuracy with changed malicious nodes.

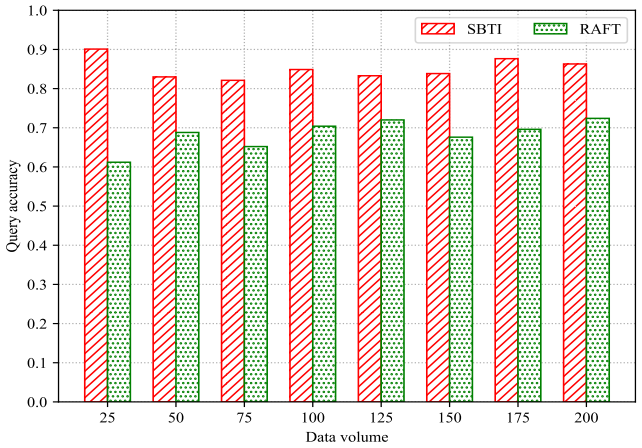


Fig. 4: Query accuracy with increasing IoT data transactions.

layer. With smart contracts, the actions taken by the scalable blockchain can be automatically executed on Virtual Machine (VM) or container when predefined state, transition rules, executed situation, or corresponding actions have appeared, enabling SBIT to fulfill the requirements of event-driven applications intellectively.

To estimate the performance of SBIT, we have conducted a case study via extensive simulations. A scalable blockchain-based IoT integrated with cloud/fog/edge servers has been built, which consists of 200 ordinary nodes and 100 critical nodes acting as block validators and creators with the memory of 97.6KB. The simulations last for about 60 minutes. The size of block is set to be 4.375KB. A number of DoS attacks has been considered in IoT data storage. The query accuracy with the changed malicious nodes and increasing IoT data transactions, in the ranges of [10, 80] and [25, 200], respectively, is illustrated in Figs. 3 and 4. Such results illustrate that SBIT can efficiently store ever-increasing IoT data when the scalable blockchain works correctly (The percentage of reliable nodes is more than 66.7% for all current blockchain with PBFT consensus) compared to RAFT, which is a typical traditional distributed data storage approach.

## V. Emerging Challenges and Future Directions

The current applications and our investigation have identified the promising benefits and brilliant future of the scalable blockchain brought to IoT, however, there still exist formidable challenges to be addressed. In this section, we highlight these challenges and the potential directions for further research.

**Blockchain privacy protection.** IoT data has become related to almost all aspects of human activities from personal medical recording to industrial smart grids, and thus its privacy receives considerable attention. In reality, blockchain exploits the strategy of minimising the association between the user identity and the block addresses to achieve the high degree of information anonymity. But, it is still easy to derive sensitive information, for example, usage patterns and time schedules, from the data included in blockchain, because all such data is designed to be visible to all participants. An emerging solution to mitigate this issue is to create completely anonymous transactions, while consuming additional storage resources and spending more verification time. Therefore, how to guarantee the privacy of blockchain still is a challenge to be solved to enable privacy-preserving blockchain-based IoT in future.

**Blockchain security.** The existing blockchain, including our proposed scalable blockchain, can partially but not fully resolve the IoT security, thereby hindering the development of diversified blockchain-based IoT applications. Currently, blockchain security mainly refers to 51% attack, double spending, consensus threat, and private key security, which always work together to threat blockchain [1]. For instance, PoW, as the fundamental component of blockchain, faces serious challenge of the "51% attack", which could forge blockchain data or prevent any new transaction with more than 50% of computation power of the entire network. There are some variants proposed to partially prevent "51% attack", while consuming high computing power and heavy storage resources. In the future, it is required to focus on the blockchain security of SBIT.

**Standardized smart contracts.** Smart contracts are becoming a promising commercial paradigm in blockchain with innovative features such as self-verifiable, automatic execution and tamper proof. There are different smart contracts developed for various applications, including wallet commercial contracts, notary, gambling, and supplychain. However, due to the unique execution environments and languages, most of them cannot be compatible with each other or work in different platforms, which may become an obstacle to on/off-chain collaboration among them. So far, these smart contracts still lack scalability, auditability, manageability and verifiability at a technical level. Therefore, there is a strong need for further research to establish uniform standards for SBIT to write and execute the available smart contracts for various blockchain-based applications.

**Constricted resources for blockchain establishment and data exchange.** To provide security and privacy supports for blockchain-based SBIT, it is quite crucial for the blockchain participants to execute the consensus mechanisms and store all received data in cloud/fog/edge servers. As a result, there are abundant resource expenditures in block establishment and

data exchange between IoT and cloud/fog/edge servers. For example, applying the available consensus protocols like PoW, PoS and PBFT to establish blocks will consume much more computing and network resources. Due to the limited storage and restrained processing capacity, it is infeasible for IoT to establish more blockchains to include the high-volume data. Therefore, the resources limitation for blockchain computing and storage ought to be fully taken into consideration in SBIT in the future.

**AI-enabled blockchain.** Blockchain is being used in a variety of IoT applications, including data storage, spectrum sharing, and energy exchange, etc. However, in reality, blockchain often suffers from security, scalability, and efficiency problems, due to the lack of global network view derived from IoT data. A potential solution to address this problem is to introduce Artificial Intelligence (AI) [1], [4], which can efficiently characterize the features and the hidden rules behind blockchain establishment, into SBIT. With the powerful learning capacity, the AI-based blcokchain can greatly improve the network intelligence of SBIT and reshape its network architecture. For example, it can help service providers make decisions on issues, such as which cloud/fog/edge server is used to store IoT data built on its predicated remaining resources and when the on-chain block validation is conducted, which may greatly improve the intelligence and the scalability of SBIT. In the future, AI should be integrated with SBIT to figure out the global view behind IoT data for efficient blockchain-enabled data storage and sharing.

## VI. Conclusions

Blockchain has been considered as a promising paradigm for IoT to mitigate its security and privacy challenges, which brings an extraordinary opportunity to rethink IoT design and revolution. Motivated by the fact that the smart devices are heavily constrained by storage resources and not capable of storing ever-increasing IoT data, we have proposed a scalable blockchain paradigm with cloud/fog/edge services and virtualization technology, and developed an innovative scalable blockchain-based architecture of data storage for IoT, to resolve its security and scalability concerns, through on-chain block validation in IoT and off-chain data storage in cloud/fog/edge servers. Under this architecture, a case study with the ever-increasing data has been implemented to demonstrate the benefits of our initiative from security and scalability. Furthermore, we have outlined the potential issues and future research directions.

## Acknowledgment

This work is partially supported by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant Agreement (No.101030505), the Natural Science Foundation of China (No.62372192, No.92067206, and No.61977064), and the National Key Research and Development Program of China (No.2022YFB2702801 and No.2020YFB1806904). This article reflects only the authors' view. The European Union Commission is not responsible for any use that may be made of the information it contains.

## References

[1] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2018.

[2] T. Cai, W. Chen, K. E. Psannis, S. K. Goudos, Y. Yu, Z. Zheng, and S. Wan, "Scalable On-chain and Off-chain Blockchain for Sharing Economy in Large-scale Wireless Networks," *IEEE Wireless Communications*, vol. 29, no. 3, pp. 32–38, 2022.

[3] T. Xu, T. Qiu, D. Hu, C. Mu, Z. Wan, and W. Liu, "A Scalable Two-Layer Blockchain System for Distributed Multicloud Storage in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 9173–9183, 2022.

[4] L. Xue, D. Liu, C. Huang, X. Shen, W. Zhuang, R. Sun, and B. Ying, "Blockchain-based Data Sharing with Key Update for Future Networks," *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 12, pp. 3437–3451, 2022.

[5] C. Qiu, H. Yao, F. R. Yu, C. Jiang, and S. Guo, "A Service-oriented Permissioned Blockchain for the Internet of Things," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 203–215, 2020.

[6] W. Dai, C. Dai, K.-K. R. Choo, C. Cui, D. Zou, and H. Jin, "SDTE: A Secure Blockchain-based Data Trading Ecosystem," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 725–737, 2019.

[7] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based Solutions to Security and Privacy Issues in the Internet of Things," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 12–18, 2018.

[8] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A Hybrid Blockchain-based Identity Authentication Scheme for Multi-WSN," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241–251, 2020.

[9] U. Javaid and B. Sikdar, "A Checkpoint Enabled Scalable Blockchain Architecture for Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7679–7687, 2021.

[10] S. Zhang, Z. Wang, Z. Zhou, Y. Wang, H. Zhang, G. Zhang, H. Ding, S. Mumtaz, and M. Guizani, "Blockchain and Federated Deep Reinforcement Learning Based Secure Cloud-Edge-End Collaboration in Power IoT," *IEEE Wireless Communications*, vol. 29, no. 2, pp. 84–91, 2022.

[11] J. Lu, J. Shen, P. Vijayakumar, and B. B. Gupta, "Blockchain-based Secure Data Storage Protocol for Sensors in the Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 8, pp. 5422–5431, 2022.

[12] Y. Liu, X. Hao, W. Ren, R. Xiong, T. Zhu, K. R. Choo, and G. Min, "A Blockchain-Based Decentralized, Fair and Authenticated Information Sharing Scheme in Zero Trust Internet-of-Things," *IEEE Transactions on Computers*, vol. 72, no. 2, pp. 501–512, 2023.

[13] R. Tapwal, P. K. Deb, S. Misra, and S. K. Pal, "Shadows: Blockchain Virtualization for Interoperable Computations in IIoT Environments," *IEEE Transactions on Computers*, vol. 72, no. 3, pp. 868–879, 2023.

[14] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Cmmunities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.

[15] B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, and M. Peng, "When Internet of Things Meets Blockchain: Challenges in Distributed Consensus," *IEEE Network*, vol. 33, no. 6, pp. 133–139, 2019.

**Wei Liu** is a professor in the School of Electrical Information and Communications Engineering, Huazhong University of Science and Technology. He received the Ph.D. degree in electronics and information engineering from the Huazhong University of Science and Technology in 2004. His research interests include wireless networking, Internet of Things, and learning evaluation.

**Haojun Huang** currently is an associate professor in the School of Electrical Information and Communications Engineering, Huazhong University of Science and Technology. He received his Ph.D. Degree in Information and Communication Engineering from the University of Electronic Science and Technology of China in 2012. His research interests include Artificial Intelligence, Network Function Virtualization, Internet of Things, and Software-Defined Networking.

**Hao Yin** is a professor with the Research Institute of Information Technology, Tsinghua University, Beijing, China. He received the PhD degree in Electrical Engineering from the Huazhong University of Science and Technology, Wuhan, China 2002. His research interests span broad aspects of Multimedia Communication and Computer Networks.

**Geyong Min** is a Professor of High Performance Computing and Networking in the College of Engineering, Mathematics and Physical Sciences, University of Exeter, United Kingdom. He received the PhD degree in Computing Science from the University of Glasgow, United Kingdom, in 2003. His research interests include Future Internet, Computer Networks, and Wireless Communications.

**Yunhao Yuan** received the BS degree in Networking Engineering from China University of Geosciences in 2020. He is currently pursuing the PhD degree in Computer Science at the Aalto University, Espoo, Finland. His research interests include Computational Social Science and Natural Language Processing.

**Dapeng Oliver Wu** (IEEE Fellow) currently is a Chair Professor at the Department of Computer Science, City University of Hong Kong. He received his Ph.D. in Electrical and Computer Engineering from Carnegie Mellon University, Pittsburgh, USA, in 2003. His research interests include networking, communications, signal processing, computer vision, and machine learning.