Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things

Yong Yu, Yannan Li, Junfeng Tian, and Jianwei Liu

Abstract

IoT is leading a digital revolution in both academia and industry. It brings convenience to people's daily lives; however, the issues of security and privacy of IoT become challenges. Blockchain, a decentralized database based on cryptographic techniques, is promising for IoT security, which may influence a variety of areas including manufacture, finance, and trading. The blockchain framework in an IoT system is an intriguing alternative to the traditional centralized model, which is struggling to meet some specified demands in IoT. In this article, we investigate typical security and privacy issues in IoT and develop a framework to integrate blockchain with IoT, which can provide great assurance for IoT data and various functionalities and desirable scalability including authentication, decentralized payment, and so on. We also suggest some possible solutions to these security and privacy issues in IoT based on blockchain and Ethereum to show how blockchain contributes to IoT.

Introduction

The Internet of Things (IoT), one of the most disruptive technologies in this century, is an influx of smart physical devices connected via network with embedded sensors, software, applications, and so on to collect, provide, and exchange data [1]. Generally speaking, IoT encompasses everything that is connected to the Internet. The overview of an IoT infrastructure is depicted in Fig. 1. The devices are uniquely identified in an IoT system and always regarded as equipped with low power, limited storage, and restrained processing capacity. The gateways are employed to link IoT devices to the Internet and able to "talk" to each other. IoT makes the world more connected, smarter, and thus more efficient. Cheap sensors and the interconnection between "things" generate more data than ever, and the information contained in these data makes the environment more cognitive and smarter. For example, the data can be collected for analysis to provide customized services for individuals. The prevalent IoT is now experiencing exponential growth in both research and industry [2]. A number of well-known corporations have poured billions of dollars to build IoT platforms such as Amazon AWS IoT and Google Cloud IoT.

In 2017, Gartner forecasted that connected things in use worldwide will reach 20.4 billion by 2020 (https://www.gartner.com/newsroom/id/3598917).

According to a survey conducted by the International Data Corporation (IDC), $674 billion was spent on IoT worldwide in 2017 and this number will reach $772.5 billion in 2018, with an increase of 14.6 percent (https://www.idc.com/getdoc.jsp?containerId=prUS43295217).

IoT has been already employed in our daily lives. Take two scenarios as examples.

IoT in Smart Homes: Suppose your home is equipped with some IoT devices such as smart cameras, smart thermostat, and some sensors. In the morning, the sensors will test the weather and temperature outside to calculate the time it takes you to drive to work and communicate the result with your alarm clock through the Internet to automatically set the right time to wake you up. Moreover, the wake-up time can be synchronized to your smart coffee maker and bread cooker to serve you a fresh breakfast. You will have an easy morning to start a beautiful day. Also, for elderly or disabled individuals in a smart home, it is easy to monitor their demands through cameras and help them by remotely controlling the devices at home.

IoT in Smart Cities: A smart city (https://en.wikipedia.org/wiki/Smart_city) is an urban area that uses data collection sensors to transmit information, and manage assets and resources efficiently. Smart cities always get the support of the government and policies, and it includes many aspects of urban life that can change people's lifestyles [3]. For example, smart traffic management can monitor traffic streams to control traffic lights and avoid congestion on the roadway in rush hours. Smart streetlights with embedded sensors can test the hours of the day to find a proper time to turn themselves on and to become dim when there are no cars or pedestrians on the streets to save energy. Smart cities can provide people the best city services and make city life easier.

IoT brings great convenience to individuals and governments; however, IoT systems with a large number of devices, tens of millions of data, and sophisticated connections may also be a security nightmare. Hackers can penetrate through the wide range of IoT devices. As a result, not only can devices with low security levels in IoT systems be targets by malicious adversaries, but also the connections between smart devices incur many

Digital Object Identifier:
10.1109/MWC.2017.1800116

Yong Yu is with Shaanxi Normal University and the State Key Laboratory of Cryptology; Yannan Li is with the University of Wollongong; Junfeng Tian is with Hebei University; Jianwei Liu is with Beihang University.

security risks. Moreover, the produced data in these systems, if not preserved properly, might expose much privacy and bring concerns to users. The security threats in IoT occur now and then. In 2016, the company Dyn suffered a distributed denial of service (DDoS) attack that was supposed to rely on a great many infected Internet-connected devices like cameras, monitors, and home routers (https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=0). Security is a priority in an IoT system and should be taken into careful consideration. The emerging blockchain can trigger new opportunities in IoT security. Companies and researchers are exploring potential blockchain-based IoT security (https://www.ciodive.com/news/companies-forge-co-operative-to-explore-blockchain-based-iot-security/435007/). However, to the best of our knowledge, there is no publicly accepted framework to embrace blockchain by IoT.

In this article, we bridge the gap with the following three contributions:

- We investigate the traditional architecture of IoT and analyze the security and privacy issues in IoT systems.
- We demonstrate how blockchain can integrate with IoT and describe a framework in which blockchain and IoT work together. We also point out how blockchain can benefit from IoT systems.
- We show a few possible solutions to address the security and privacy issues in IoT systems based on blockchain and Ethereum. More blockchain-based potential solutions beyond security and privacy issues are considered as well to show the powerful functionalities of blockchain in IoT.

Organization: The rest of the article is organized as follows. Some preliminaries are given in the following section. The security and privacy issues in IoT are then analyzed. Several possible blockchain-based solutions to IoT security and privacy are then presented. Finally, the article is concluded.

Preliminary

In this section, we introduce some basic knowledge of blockchain and give a brief description of smart contract and Ethereum.

Blockchain

Blockchain is an append-only decentralized digital ledger based on cryptography. Blockchain provides a platform to conduct trusted transactions without a third party, in which every fund transfer, every task, and every request has a record on the chain with a digital signature for public verification. The ledger is generated and maintained by all participants in the system. Blockchain is one of the underlying techniques in decentralized networking with many potential merits, for example:

- Blockchain is distributed. It allows a variety of peers to join the network without registration, which makes it easier than traditional centralized systems [4–6, 15].
- Blockchain is decentralized. Instead of relying on a third party to build trust, blockchain transplants trust into the system via a consensus mechanism, such as proof of work(PoW) and proof of stack (PoS).

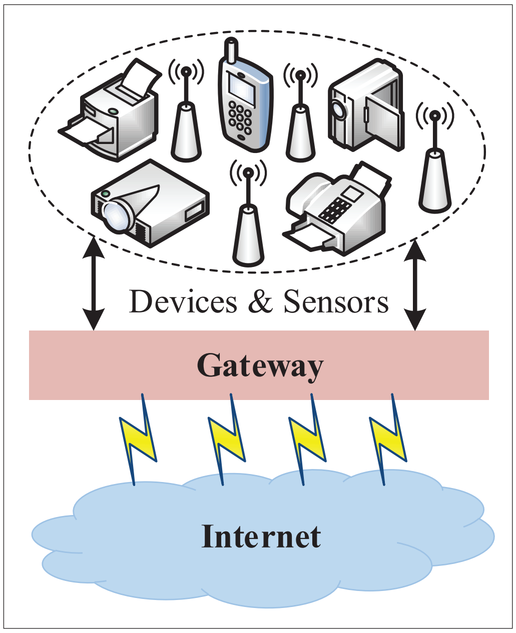

FIGURE 1. IoT architecture.

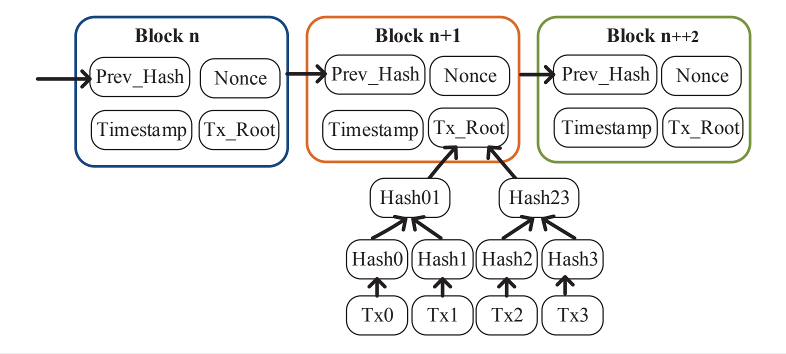

FIGURE 2. Blockchain architectures.

- Blockchain is immutable. Information on blockchain exists as a shared and intact copy. Once it is linked to the chain, it cannot be tampered with. Due to the aforementioned attractive features of blockchain, it serves as the backbone technique in various applications, such as cryptocurrencies, blockchain IoT, blockchain business, and blockchain asset management. Blockchain also has the potential to revolutionize business and redefine economies.

Figure 2 shows a typical structure of blockchain. Peers join the system with unique private-public key pairs. A block contains a block header and a block body, which is composed of some transactions signed by a user with her private key and can be verified with the public key. A block header usually contains some basic information of this block, such as version number, timestamp, block size, and transaction numbers. A Merkle hash tree is usually employed to generate a hash value of all the transactions in this block to reduce the storage overhead of the chain. A block also contains the hash value of the previous block to link the two blocks together. Once a block is generated, it is spread to miners, who need to validate all transactions in the block. Upon the transactions in a block being approved, the consensus protocol, such as PoW, is implemented by finding a *nonce* that makes the

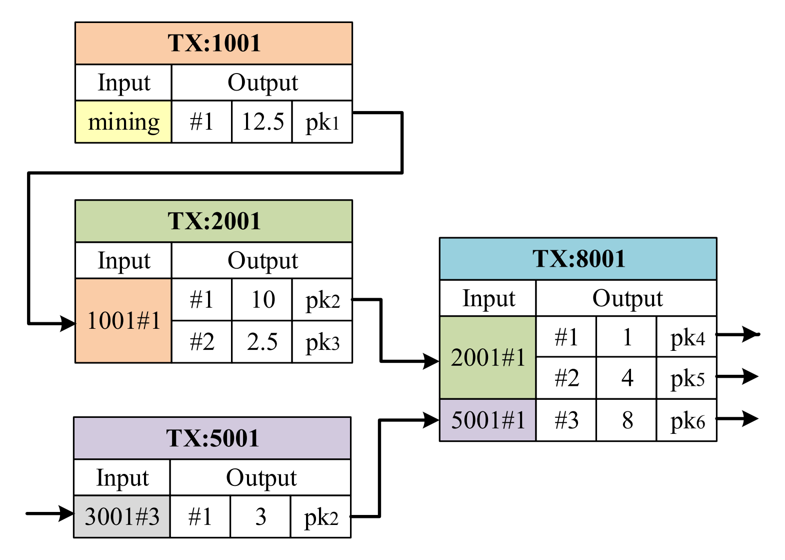

FIGURE 3. Bitcoin transactions.

hash of the block begin with some specific number of zeros. The block is then appended to the chain and broadcast to all the nodes in the system. The other nodes accept this block by using its hash as part of the newly generated block.

Bitcoin Transactions

Bitcoin [7], the first cryptocurrency, is one of the most popular applications of blockchain. Bitcoin was proposed by Nakamoto *et al.* in 2008 and now serves as the underlying platform of a number of other cryptocurrency systems. We take the bitcoin system as an example to show how to trade digital assets via blockchain. The bitcoin system employs the unspent transaction output (UTXO) model to conduct transactions, which were generated by early transactions. The UTXOs spent in a transaction are the inputs and outputs of a transaction, which are the UTXOs that the transaction creates in the system.

As shown in Fig. 3, transaction *TX1001* is the Coinbase transaction, which has no input account, and the output is the rewarded 12.5 bitcoins from mining. The user with pk_1 contains 12.5 bitcoins in her account. In transaction *TX2001*, it takes as input *TX1001* and generates two UTXOs, pk_2 and pk_3, with 10 bitcoins and 2.5 bitcoins, respectively. The miners check whether there is enough bitcoin in the output UTXO in *TX1001* to validate this transaction. Once the transaction is approved, pk_1 is discarded in UTXO lists, and two new records, pk_2 and pk_3, are generated with a specific number of bitcoins, which serves as input accounts in new transactions. Bitcoin supports multiple UTXOs as inputs, as shown in transaction *TX8001*. Transaction *TX5001* has a UTXO 3001#3 with 3 bitcoins in the account generated by previous transactions and now is part of the inputs of transaction *TX3001*. Digital assets are transferred via transactions, and each transaction in the system leads to the generation of new UTXOs and revocation of used UTXOs.

Smart Contract

The *smart contract* concept [8] was proposed by Nick Szabo in 1994 when he realized that the decentralized ledger could achieve a smart contract. Compared to a traditional trusted lawyer or notary, a smart contract can act as a trusted third party without any assumption to help two parties exchange assets, property, shares, and so on. In this framework, contracts can be stored as programming codes and run automatically on the blockchain once the conditions are satisfied. Each party can eventually get the results as defined in the rules as well as the penalties in the agreement. Smart contracts have the following properties:

1. Autonomy. Smart contracts can be executed independently and automatically in a prescribed manner. Even the parties involved in the transaction are the ones who make the agreement rather than execute it. There is no need to worry about manipulation and corruption by a middle party.
2. Trust. The documents on the ledger are encrypted using symmetric encryption algorithms. It is hard for a hacker to crack the codes and infiltrate the smart contract.
3. Accuracy. Smart contracts are faster, cheaper, and more accurate than traditional contracts. They can avoid the human errors caused by filling in forms.

Ethereum

Ethereum (https://github.com/ethereum/wiki/wiki/White-Paper), proposed by Vitalik Buterin in 2013, is an open source public blockchain platform that is built for creating smart contracts. It provides decentralized virtual machines, *Ethereum Virtual Machines* (EVMs), with Ether cryptocurrency to handle point-to-point contracts. The Ethereum platform is commonly regarded as "the next generation of cryptocurrencies and decentralized application platforms," and Ethereum currency is the second largest cryptocurrency with a market capitalization of $82.8 billion in February 2018 (https://coinmarketcap.com/currencies/ethereum/).

Ethereum and Bitcoin are two main applications of blockchain. The main difference is that the Bitcoin blockchain is for tracking the transfer of ownership of cryptocurrencies, while the Ethereum blockchain focuses more on running programming codes on the platform, which achieves more powerful functionality such as voting and ballots. The Ethereum system is under an account-based model with state transitions, which contains two types of accounts, *externally owned accounts* controlled by private keys and *contract accounts* controlled by codes in contracts. Contracts are created by transactions with a special "to" address.

Security Issues in IoT

Several typical security issues in IoT are considered in this section.

Data Integrity

The data generated by IoT systems of a company are critically important, and may involve trade secrets that are closely related to the future development of the company and are often kept confidential from outsiders. Thus, the data should be stored confidentially and intact for future use. Traditional centralized storage, such as cloud storage, can be integrated into IoT architecture; however, it suffers from inherent vulnerabilities. The centralized server is vulnerable and may easily have a single point of failure. Besides, more devices with a central server model may cause many-to-one traffic jams, and incur delayed response and system scalability problems as well. IoT solutions based on blockchain can be built to protect data against pollution or deletion.

Several distributed data storage systems based on blockchain have recently been proposed. Filecoin (https://filecoin.io/) offers a decentralized storage system in which miners earn coins by competitively storing users' files. IPFS provides a peer-to-peer approach to storing and sharing hypermedia in a distributed file system (https://ipfs.io/). However, neither of these systems considers the integrity of outsourced files.

Data Sharing

A primary object of an IoT system is sharing information between objects, which is helpful to manufacturing, transportation, and business to provide better service in people's daily lives [9]. A large quantity of data is produced in IoT systems. As shown in a survey of U.S. manufacturers, 35 percent of manufacturers rely on the data produced by smart sensors to improve their operating processes at present (http://usblogs.pwc.com/industrialinsights/2015/02/24/the-internet-of-things-has-arrived-in-americas-factories/). However, these data are usually not free; thus, a convenient and fair data trading mechanism is needed.

Authentication and Access Control

Another security issue is unauthorized access to the resources and sensitive information in IoT systems. Traditional authentication and access control management to an external entity is based on a centralized party who generates a proper key based on access policies. However, the IoT system makes centralized approaches a bottleneck when the number of devices explosively grows. Moreover, the dynamic nature of IoT deployment leads to complex trust management, which may sacrifice the scalability of the system.

Privacy

An IoT system collects data using a variety of smart devices and sensors to make a comprehensive decision according to customized requirements. However, in the complex IoT system, privacy is easily violated in various ways, such as data acquisition, raw data processing, and data exchange (https://arxiv.org/pdf/1708.05261.pdf). The abuse of data produced by IoT devices may consequently hit user privacy. For example, the hobbies and preferences of an owner in IoT might be leaked to attackers. It is said that smart toys, such as Barbie and CogniToys Dino, collect children's personal information (name, age, etc.) and record children's voices when parents are unaware of it in order to make the toys smarter, which causes privacy concerns (http://www.washington.edu/news/2017/05/10/kids-parents-alike-worried-about-privacy-with-internet-connected-toys/). Thus, privacy preservation in IoT systems, including data privacy and entity privacy, is of great importance and also a challenge.

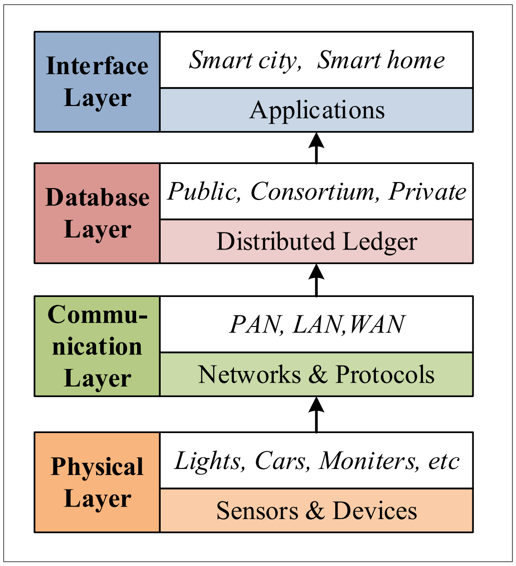

FIGURE 4. Security IoT framework with blockchain.

Blockchain-Based Solutions

To address the aforementioned challenges in IoT environments, exquisite solutions are needed in blockchain-based IoT architecture. Blockchain is supposed to play an important role in IoT systems for management, control and security. In this section, we first describe the framework that collaborates blockchain in IoT. Then we introduce several possible blockchain-based solutions to security and privacy issues in IoT.

IoT Framework with Blockchain

As shown in Fig. 4, the IoT framework [10] with blockchain consists of four layers.

Physical Layer: The physical layer includes all the smart devices, equipped with sensors and actuators, that collect and forward data to upper layers. Usually, there is no single standard for smart devices to share and integrate with each other to provide cross-functionality. Thus, using blockchain to manage devices in IoT system needs to make all the IoT devices from the same manufacturer operate on the same blockchain network [11].

Communication Layer: Smart devices in IoT use different communication mechanisms to get access to the system and exchange information, such as WiFi, 4G, and Ethernet. Security and privacy of the transmitted data within the system are quite important. Blockchain can be integrated with the system and contribute a lot to this circumstance. For example, BitTorrent (www.bittorrent.com/.) can be used for peer-to-peer communication [10]. More solutions to ensure data security need to be explored with the assistance of blockchain.

Database Layer: Blockchain itself is a distributed database that records immutable and continuously growing transactions. Another merit of blockchain, compared to the traditional centralized database, is the public verification and auditing mechanism. There are three main types of blockchain, namely public blockchain, consortium blockchain, and private blockchain. In public blockchain, everyone is able to easily get involved in the system, generate transactions, and achieve consensus. Consortium blockchain is a permissioned one,

Ethereum and Bitcoin are two main applications of blockchain. The main difference is that the Bitcoin blockchain is for tracking the transfer of ownership of cryptocurrencies, while the Ethereum blockchain focuses more on running programming codes on the platform, which achieves more powerful functionality such as voting and ballots.

Zero knowledge proof of knowledge and zero knowledge argument of knowledge are perfect tools to convert any information in a transaction into random ones to restrain any third party to obtain even one bit of the information. When referring to data privacy in IoT systems, for efficiency consideration, symmetric encryption such as AES encryption is used.

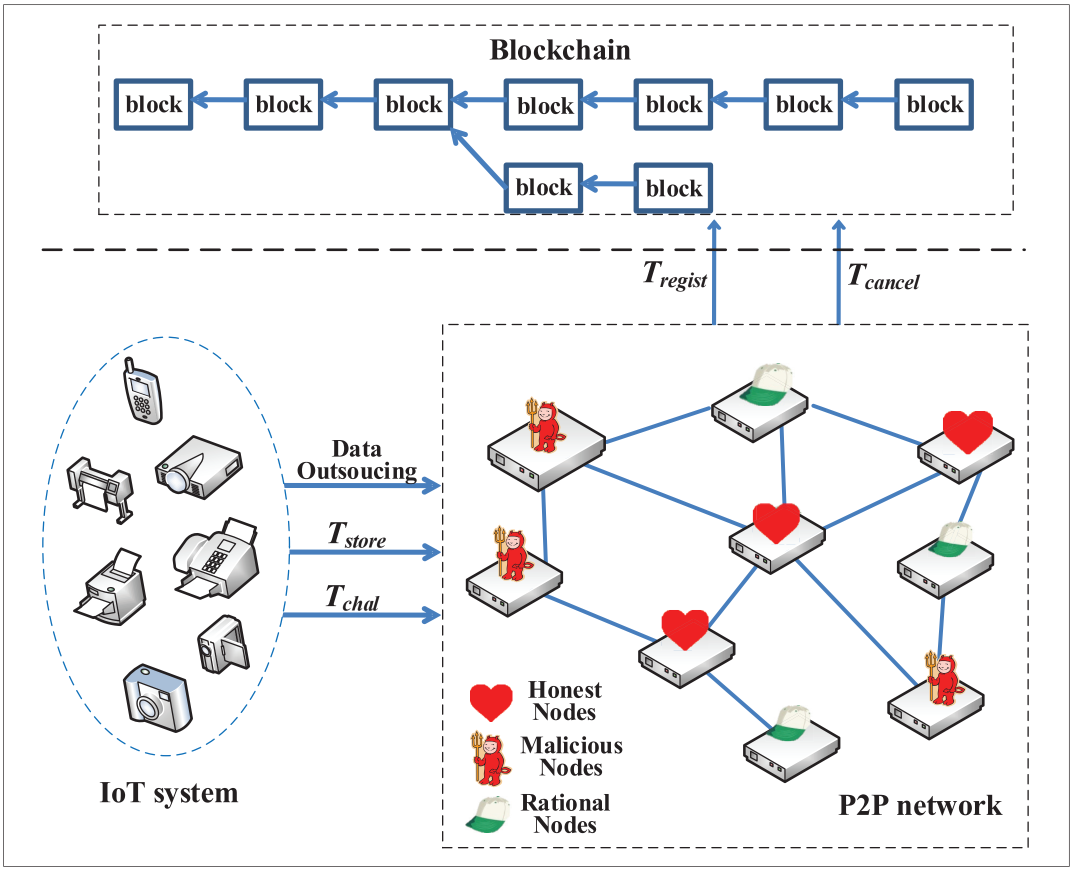

FIGURE 5. Data integrity framework with blockchain in IoT.

where consensus is managed by a pre-selected set of nodes (https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/). In private blockchain, access permission is tightly controlled as well as the authority to read and write. The consensus in permissioned blockchain may not need to solve puzzles or get the incentive. As an alternative, Practical Byzantine Fault Tolerance(PBFT) (https://en.wikipedia.org/wiki/Byzantine_fault_tolerance) saves much time in reaching consensus compared to the public blockchain.

Interface Layer: The interface layer contains applications that communicate with each other to make a beneficial decision collaboratively. Typical IoT applications include smart cities and smart homes, introduced earlier.

Data Integrity

A potential solution to data integrity in a decentralized system is shown in Fig. 5. Specifically, it works as follows, in which Ethereum and smart contract are employed. For data confidentiality, data collected by IoT devices should be encrypted before outsourced. Peers in a peer-to-peer (P2P) system need to commit the space they possess by generating a *proof of space* to prove their claims and make deposits. This is achieved when peers register into the system to generate a transaction T_{regist}. Miners validate the transactions by checking verification equations in proof of space and link valid transactions in blockchain. IoT users announce transactions T_{store} in the P2P network and claim the requirements and involved fees. Miners match the requirements and service in transactions and offer storage to users. When IoT users need to check the integrity of the outsourced data, a new transaction T_{chal} is generated. After that, the miners who store the data compute a proof and put it on blockchain, which will be verified by users. If the proof does not pass the verification, the deposit in transaction T_{regist} will be rewarded to users as a punishment for miners who host the data. If miners want to revoke the storage space, they need to produce a transaction T_{cancel} and withdraw the deposit in a T_{regist} transaction.

Data Sharing

Here, a possible solution is presented by borrowing the idea of fair exchange leveraging Ethereum-based blockchain [12]. Suppose a data owner collects data generated in an IoT system and shares the data at a price of *d* BTC with a receipt. In order to ensure the fairness between a seller and a buyer, the buyer needs to make some deposit in a transaction, as shown in Fig. 6, which should not be less than *d* BTC. In this transaction, a timed commitment [12] is employed with some pre-defined time *t*. The seller can redeem the deposit after she honestly pays the seller within time *t*. Otherwise, the deposit can be forwarded to the seller after time *t* with her signature on transaction *Fuse*. If a seller signs *Fuse* transaction before time *t*, it is invalid because it cannot pass the verification of the miners within time t_{lock} in the transaction. This ensures that a malicious buyer cannot do harm to the seller when she gets the expected data. If the buyer also needs protection from fair exchange, the seller also needs to generate a transaction to make some deposit.

Authentication and Access Control

Ethereum can provide authentication and access control to smart devices, services, and the data in IoT, which removes the dependent central parties and gets better efficiency compared to traditional access control models such as role-based access control, context-based access control, and capability-based access control. Users can pre-define access policies in smart contracts and generate several kinds of transactions, say T_{policy}, T_{access}, and T_{query}. The transaction T_{policy} includes the pre-defined access policies, T_{access} is for access management, and T_{query} is for access query. When a new entity enrolls in an IoT system for the first time, a newly generated public key together with the corresponding access permission is determined and put into a transaction T_{access} on the blockchain. Later, when the entity needs to get access to the IoT system, a query is generated by constructing and signing a transaction T_{query}. The transaction will be verified with her public key, and the authorization will be approved.

Privacy

To protect privacy in an IoT system, consortium and private blockchain are usually involved. For entity privacy in IoT, blockchain uses pseudonyms, say public keys, to achieve anonymity. However, this is not strong enough in some real-world applications. Several cryptographic techniques can be combined to achieve full anonymity. Linkable ring signatures are well suited to sign a transaction that can hide the sender's identity in a spontaneous ring. Homomorphic commitments can hide the amount of currency in billing transactions. Zero knowledge proof of knowledge and zero knowledge argument of knowledge are perfect tools to convert any information in a transaction into random ones to restrain any third party from obtaining even one bit of the information. When referring to data privacy in IoT systems, for efficiency, symmetric encryption such as AES encryption is used.

Other Applications with Blockchain in IoT

Sharing Services and Properties: As a further step on data trading in IoT, blockchain also facilitates sharing services and property with Ethereum. Sharing services is one of the fundamental components in smart cities. It is said that 66 percent of people in the world would like to share their assets for a beneficial gain (https://slock.it/usn.html). The sharing business model can not only improve the utilization of the properties but also save costs and resources. Suppliers can offer idle items, such as spare rooms or vehicles, and customers can rent the stuff at a lower price and transaction fee, which is much cheaper and more convenient than having new ones. The involved blockchain takes care of security issues and helps quickly establish trust between a dynamic group of strangers that can allow counterparties to transact directly. A possible model is shown as follows. Suppliers make a deposit on Ethereum and claim the stuff to be shared with the price p. Until the claim is cancelled, suppliers can redeem the deposit. Customers make the deposit with a timed commitment and value p' when they need a service, in which p' should be larger than p. If the customer honestly pays p to the supplier after enjoying the service within time t, the deposit p' can be placed back in her account. Otherwise, the supplier can obtain the deposit as a punishment for the customer. All the procedures above can be automatically executed without any intermediaries, which is one of the most salient features in property sharing. A German startup offers smart locks *Slock* (www.slock.it) based on Ethereum with a similar framework. *Slock* also claimed that Airbnb may soon become fully automated for sharing accommodations.

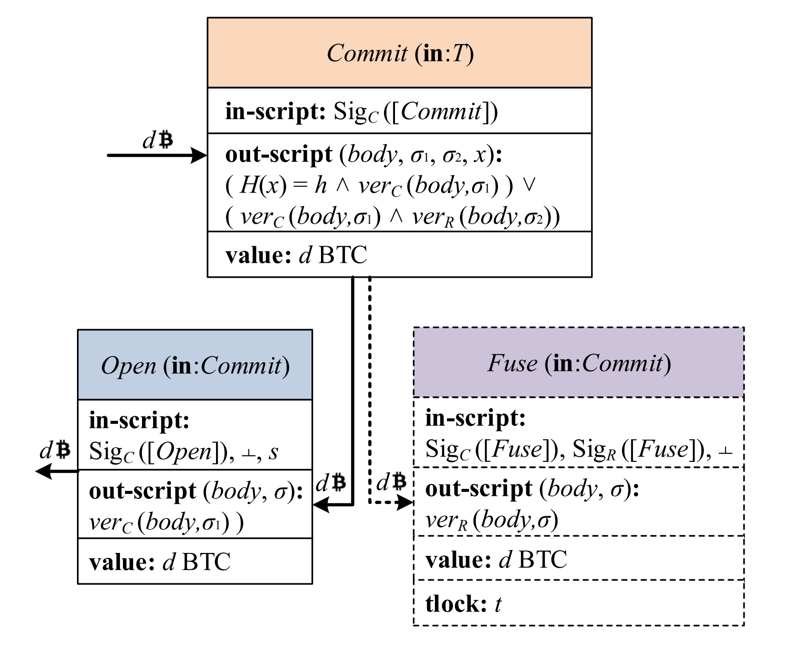
Commit (**in**:T)
in-script: $\mathrm{Sig}_C([Commit])$
out-script $(body, \sigma_1, \sigma_2, x)$**:**
$(H(x) = h \wedge ver_C(body,\sigma_1)) \vee$
$(ver_C(body,\sigma_1) \wedge ver_R(body,\sigma_2))$
value: d BTC
d ฿
Open (**in**:*Commit*)
in-script:
$\mathrm{Sig}_C([Open]), \perp, s$
out-script $(body, \sigma)$**:**
$ver_C(body,\sigma_1)$)
value: d BTC
d ฿
d ฿
d ฿
Fuse (**in**:*Commit*)
in-script:
$\mathrm{Sig}_C([Fuse]), \mathrm{Sig}_R([Fuse]), \perp$
out-script $(body, \sigma)$**:**
$ver_R(body,\sigma)$
value: d BTC
tlock: t

FIGURE 6. Data sharing framework with blockchain in IoT [12].

Device Management: Blockchain can also get involved in governing smart devices in an IoT system. In traditional IoT systems, physical smart devices are identified by IP addresses connected to the network, in which IPv4 and IPv6 have 32-bit and 128-bit address space, respectively. Blockchain, which is based on *elliptic curve cryptography*, has a 160-bit identification address, which can contain a larger number of devices. When the number of devices keeps proliferating, it is hard for the traditional client-server model to handle the issues. In blockchain-based systems, smart devices will be assigned a unique key pair when they enroll in the system for the first time, where the public keys are stored in Ethereum and the corresponding private keys are stored on devices. After that, smart devices in IoT are identified by public keys, which are pseudonyms. Devices communicate with each other by transactions and can be verified by the signatures and public keys. When the devices need to update the embedded firmware, it is easier with a blockchain, because in the traditional server-client model, much more extra information needs to be transferred for checking the validity and reliability of the patch from the manufacturer. In blockchain model, a manufacturer puts the location of the firmware in a transaction on the blockchain. Then the devices can automatically download the update and install as preset.

IoT offers great convenience to people's daily life by exchanging data and making comprehensive decisions. However, it brings security and privacy concerns simultaneously. Blockchain has potential in dealing with these security and privacy issues in IoT.

Supply Chain: Blockchain also provides supply chains for devices to be tracked at every point of the life cycle from manufacturers, shippers, and retailers to owners, and so on. At each point, the entity needs to update the latest position as a transaction and put it on blockchain to let others know about the device. When the owner of the device changes (e.g., the device is resold), the key pairs for the device can be re-issued, which also needs a record on blockchain.

Conclusions and Future Work

IoT offers great convenience to people's daily lives by exchanging data and making comprehensive decisions. However, it brings security and privacy concerns simultaneously. Blockchain has potential in dealing with these security and privacy issues in IoT. In this article, we analyze the typical security and privacy issues in IoT. Then some blockchain-based solutions are proposed to address these issues. Specifically, we propose a framework that can integrate blockchain in an IoT system and discuss a number of potential solutions. A few more solutions beyond security and privacy issues based on blockchain are presented as well.

Future Work: A few alternatives to blockchain to form a distributed ledger were proposed recently. Reference [13] proposed the GHOST protocol, in which they modified blockchain with a tree structure in the main ledger. Lewenberg *et al.* [14] proposed a directed acyclic graph (DAG)-based cryptocurrency model. It is interesting to investigate DAG-based solutions to security and privacy issues in IoT.

Acknowledgment

This work was supported by the National Key R&D Program of China (No. 2017YFB0802000), the National Natural Science Foundation of China (61872229), the National Cryptography Development Fund during the 13th Five-year Plan Period (MMJJ20170216), and the Fundamental Research Funds for the Central Universities(GK201702004).

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, 2010, pp. 2787–2805.

[7] S. Nakamoto, ”Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] A. Dorri, S. S. Kanhere, and J. Raja. "Blockchain in Internet of Things: Challenges and Solutions," arXiv preprint arXiv:1608.05187, 2016.

[4] Y. Li *et al.*, "Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage Systems," *IEEE Trans. Dependable and Secure Computing*, 2016. DOI: 10.1109/TDSC.2017.2662216.

[5] J. Guo, B. Song, and X. Du, "Significance Evaluation of Video Data Over Media Cloud Based On Compressed Sensing," *IEEE Trans. Multimedia*, vol. 18, no. 7, 2016, pp. 1297–1304.

[6] H. Zhang, Q. Zhang, and X. Du. "Toward Vehicle-Assisted Cloud Computing for Smartphones," *IEEE Trans. Vehic. Tech.*, vol. 64, no. 12, 2015, pp. 5610–18.

[3] I. Khajenasiri *et al.*, "A Review on Internet of Things Solutions for Intelligent Energy Control in Buildings for Smart City Applications," *Energy Procedia*, vol. 111, 2017, pp. 770–79.

[8] N. Szabo, "Smart Contracts: Building Blocks for Digital Markets," *EXTROPY: The Journal of Transhumanist Thought*, vol. 16, 1996.

[9] Y. Zhang and J. Wen, "The IoT Electric Business Model: Using Blockchain Technology for the Internet of Things," *Peer-to-Peer Networking and Applications*, vol. 10, no. 4, 2017, pp. 983–94.

[10] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," *Proc. IEEE 14th Int'l. Conf. Smart City*, 2016, pp. 1392–93.

[11] K. Christidis and M. Devetsikiotis. "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol, 4, 2016, pp. 2292–2303.

[12] M. Andrychowicz *et al.*, "Fair Twoparty Computations Via Bitcoin Deposits," *Proc. Int'l. Conf. Financial Cryptography and Data Security*, Springer, 2014, pp. 105–21.

[13] Y. Sompolinsky and A. Zohar, "Accelerating Bitcoins Transaction Processing," *Fast Money Grows on Trees, Not Chains*, 2013.

[14] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive Block Chain Protocols," *Proc. Int'l. Conf. Financial Cryptography and Data Security*, Springer, 2015, pp. 528–47.

[15] Z. Guan *et al.*, "Achieving Efficient and Secure Data Acquisition for Cloud-Supported Internet of Things in Smart Grid," *IEEE Internet of Things J.*, vol. 4, no. 6, Dec. 2017, pp. 1934–44.

Additional Reading

[1] M. A. Khan and K. Salah. "IoT Security: Review, Blockchain Solutions, and Open Challenges," *Future Generation Computer Systems*, 2017.

Biographies

Yong Yu is currently a professor at Shaanxi Normal University, China. His research interest is blockchain. He is an Associate Editor of *Soft Computing*.

Yannan Li is a Ph.D. candidate at the University of Wollongong, Australia. Her research interest is blockchain.

Junfeng Tian is currently a professor and Dean of the School of Cyber Security and Computers, Hebei University. His research interest is network security.

Jianwei Liu is currently a professor and dean of the School of Cyber Science and Technology, Beihang University. His current research interests include cryptographic protocol design and security on wireless network. He has published six books and more than 200 papers in his research fields.