SCIENCE CHINA
Information Sciences

• EDITORIAL •

March 2020, Vol. 63 130100:1–130100:2
https://doi.org/10.1007/s11432-020-2781-0

Special focus on security and privacy in blockchain-based applications*

The concept of blockchain was introduced by Satoshi Nakamoto in 2008. Blockchain is the core technique to support and achieve Bitcoin. Roughly speaking, a blockchain is a chained data structure that combines data blocks in a sequential manner in terms of time. It also can be viewed as a tamper-proof and unforgeable distributed ledger guaranteed by cryptography. Blockchain technology is a new application mode of distributed data storage, point-to-point transmission, consensus mechanism and encryption. It features decentralization, openness, tamper-proofing, anonymity and traceability. Blockchain has become a popular research topic in many fields due to its advantages, such as finance, e-government, Internet of things, public services, the regulatory traceability of food and drug, and supply chain. It has been regarded as a new trend of technological changes and industrial revolutions in the future, and promoted around the world.

With the rapid development and wide utilization of blockchain technology, the security and privacy issues have arisen, which must be taken into consideration. Compared to the traditional centralized structures, a blockchain does not depend on the centralized nodes. Every blockchain node in the system stores data and processes data independently. It can effectively address the problem of single point of failure. However, to achieve public verification, all transaction records in a blockchain must be made public. It will result in privacy leakage. It is a serious threat of personal security and national security, when the transaction records are sensitive, such as personal health records, bank account numbers and military data. Therefore, before transforming block chain technology to real-world application from theory, the data security and privacy problem must be addressed. The cryptography provides the core technical support for solving these problems. Targeting the above goals, this special focus about the security and privacy in blockchain-based applications of *SCIENCE CHINA Information Sciences* attempts to present recent advances related to blockchain, covering a wide array of topics.

Group data sharing enables information sharing between multiple parties for cooperative purposes. However, the existing schemes only consider scenarios in which all parties in the same organization want to share data. Achieving secure data sharing between users of different groups is also a relevant research issue. Based on this observation, Huang et al. proposed a blockchain-based data sharing scheme for multiple groups with anonymity and traceability. Owing to the consortium blockchain technique, any user in the system can easily verify the validity of the shared data without interacting with a third-party auditor. Additionally, the proposed scheme can not only enable data sharing between different groups with enhanced security anonymously but also achieve traceability and non-frameability.

A robust and scalable crowd management infrastructure is crucial in addressing operational challenges when deploying high-density sensors and actuators in a smart city. While crowdsourcing is widely used in crowd management, conventional solutions. Lin et al. pointed out that there exist several potential security concerns (e.g., sensitive leakage, single point of failure and unfair judgment) in such a centralized paradigm. Hence, a recent trend in crowdsourcing is to leverage blockchain (a decentralized ledger technology) to address some of the existing limitations. A small number of blockchain-based crowdsourcing

*Citation Zhong S, Huang X Y. Special focus on security and privacy in blockchain-based applications. Sci China Inf Sci, 2020, 63(3): 130100, https://doi.org/10.1007/s11432-020-2781-0

systems (BCSs) with incentive mechanisms have been proposed in literature, but they are generally not designed with security in mind. Thus, Lin et al. studied the security and privacy requirements of a secure BCS and proposed a concrete solution (i.e., SecBCS) with a prototype implementation based on JUICE.

In the Bitcoin network, the simplified payment verification protocol (SPV) enables a lightweight device such as a mobile phone to participate in the Bitcoin network without need to download and store the whole Bitcoin blocks. A Bitcoin SPV node initiates and verifies transactions of the Bitcoin network through the Bitcoin wallet software. Thus, the security of the wallet is critical for the SPV nodes as it may affect the security of user's cryptocurrencies. Recently, Park et al. proposed a two-party authenticated key exchange protocol for the mobile environment. They claimed that their protocol is not only secure against various attacks but also can be deployed efficiently. However, after a thorough security analysis, Zhou et al. found that Park et al.'s protocol is vulnerable to user forgery attack, smart card stolen attack and unable to provide user anonymity. To enhance security, Zhou et al. proposed an efficient and secure user authentication protocol for the SPV nodes in the mobile environment which can fulfill all the security requirements and has provable security. Additionally, the performance analysis shows the proposed protocol is efficient for the SPV nodes in the Bitcoin network.

The core Bitcoin technology is the so-called blockchain protocol. In recent years, several studies have focused on rigorous analyses of the security of Bitcoin's blockchain protocol in an asynchronous network where network delay must be considered. Wei, Yuan, and Zheng investigated the effect of a long delay attack against Nakamoto's blockchain protocol. However, their proof only holds in the honest miner setting. Yuan et al. improved Wei, Yuan and Zheng's result using a stronger model where the adversary can perform long delay attacks and corrupt a certain fraction of the miners. Yuan et al. proposed a method to analyze the converge event and demonstrated that the properties of chain growth, common prefix, and chain quality still hold with reasonable parameters in their stronger model.

Ni et al. provided the formal analysis of Bitcoin backbone protocol in the non-flat model. Precisely, they rethought and redefined the model of computing puzzles to capture the real-world protocol execution, where each party owns different amount of computational power and does sequential computations towards a puzzle independently. Their work obtains the better results in analyzing the security of Bitcoin backbone protocol, which can reflect the real-world protocol execution better, without any additional assumptions but the honest majority assumption. Finally, they showed that a robust public transaction ledger can be built on top of Bitcoin backbone protocol in their model securely.

Guest Editors:
Sheng ZHONG
Nanjing University, China
Xinyi HUANG
Fujian Normal University, China