From Bitcoin to Cybersecurity: a Comparative Study of Blockchain Application and Security Issues

Fangfang Dai, Yue Shi, Nan Meng, Liang Wei, Zhiguo Ye
Security Research Department
China Academy of Information and Communications Technology
Beijing, China

Abstract—**With the accelerated iteration of technological innovation, blockchain has rapidly become one of the hottest Internet technologies in recent years. As a decentralized and distributed data management solution, blockchain has restored the definition of trust by the embedded cryptography and consensus mechanism, thus providing security, anonymity and data integrity without the need of any third party. But there still exists some technical challenges and limitations in blockchain. This paper has conducted a systematic research on current blockchain application in cybersecurity. In order to solve the security issues, the paper analyzes the advantages that blockchain has brought to cybersecurity and summarizes current research and application of blockchain in cybersecurity related areas. Through in-depth analysis and summary of the existing work, the paper summarizes four major security issues of blockchain and performs a more granular analysis of each problem.**

Adopting an attribute-based encryption method, the paper also puts forward an enhanced access control strategy

Keywords-blockchain; cybersecurity; privacy-protection; tamper-proofing

I. Introduction

Blockchain was initially put forward as an underlying technical framework of Bitcoin [1]. Although due to the excessive value fluctuation and supervisory management reasons, Bitcoin was once forbidden or restricted to a variable extent in China, Russia, Europe and some other countries [2-4]. The confidentiality, security and reliability of blockchain technology are realized by the public. Blockchain is considered a bran-new data storage, transmission and management mechanism because it realizes reliable transfer of data and value in a decentralized way, without the need of any trusted third-party organization. As a technical solution which enables the users to participate jointly in data computing, storage, authenticity verification and the maintenance of reliable database, blockchain started from cryptocurrency, grew in assets and credit field, and gradually found its application in information and communication area. With the rapid development of blockchain technology, various industries gradually realize the technological superiority and application value of blockchain. In the meantime, problems and security risks in the application of blockchain are becoming more and more prominent, such as the 51% attack [5], the limited size of block [6-7], and the latency of transaction [8].

In order to identify the primary security challenges of blockchain, this paper performs a comprehensively study on its technical principle, security mechanism, typical applications, security risks, etc. The rest of this paper is organized as follows. Section II introduces the security advantages of blockchain technology. Section III elaborates current research and application of blockchain in cybersecurity related fields. Section IV analyzes major security issues and challenges of blockchain. And Section 5 concludes the paper.

II. Overview of Blockchain Security Advantages

Essentially, blockchain is an underlying technical framework which enables the users to collectively maintain a reliable database in a decentralized manner. As depicted in Figure 1 [1], in a typical blockchain system, data is generated and stored in units of blocks. Consecutive blocks are connected in chronological order to form a chained data structure. All user nodes participate in the validation, storage and maintenance of data. Usually the creation of a new block should be approved by more than half of the users, and broadcasted to all user nodes to perform a network-wide synchronization. Once synchronized, the modify or delete operation is not allowed optionally.

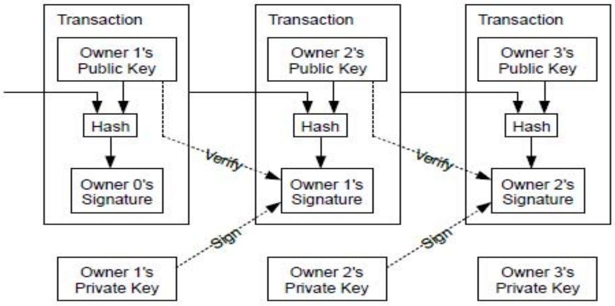

Figure 1. Blockchain technical framework.

This paper is sponsored by National Science Foundation of China No.61471129.

978-1-5386-1107-4/17/$31.00 ©2017 IEEE

Owing to its integration of technological superiorities of distributed data storage, P2P network, cryptography and consensus mechanism [9], blockchain sacrifices proper computing capacity, bandwidth and storage resource for the improvement of security. The major advantages that blockchain has brought to security is described as below.

A. Tamper-proofing

The advantage of tamper-proofing is achieved by the unique date structure and data writing mechanism of blockchain. Once a record, which is known as a transaction [10], is being created in the chained data structure of blockchain, a new timestamp [11] will be recorded at the same time, as depicted in Figure 2. And any modification of data created before that timestamp will not be allowed any more. In addition, whether a new transaction can be recorded should be decided by a consensus mechanism. In other words, the approval of a specific percentage of users is needed to write data in blocks, in general, this percentage is set to more than 50%. With the existence of the consensus mechanism, the adversaries have to control over half of the network nodes, or possess a stronger computing power to tamper with data in data recording process.

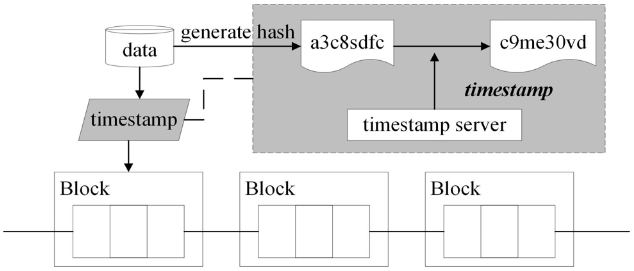

Figure 2. Tamper-proofing mechanism of blockchain.

B. Disaster Recovery

Blockchain performs data recording and storing synchronously at all users' side by constructing open source sharing protocols. Unlike the traditional centralized database which stores data in one or several centers. In an application built on blockchain, every user has the right to generate data and keep a full copy of data. This mechanism may cause redundancy to some extent [12-13], but reliability and fault-tolerance capability of the network is improved. Because arbitrary attack on one or more nodes will not cause destructive damage to the whole network.

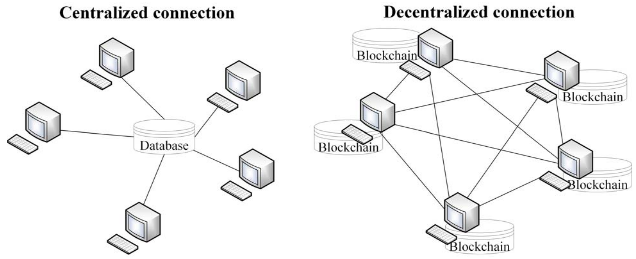

Figure 3. Decentralized and distributed storage of blockchain.

C. Privacy Protection

Blockchain adopts asymmetric encryption mechanism to enable users to encrypt data with their own private key [14-16]. Moreover, the hash value of a user's public key is calculated and perform as the ID indicator of the user. On one hand, the hash value has no relation with the real identity of user, thus keeping user's personal privacy information safe. On the other hand, the process of calculating hash value is invertible, which means an adversary can't figure out a user's public key from the public user address, and calculating the private key from the public key is impossible. Therefore, blockchain achieves the goal of preserving user anonymity and privacy.

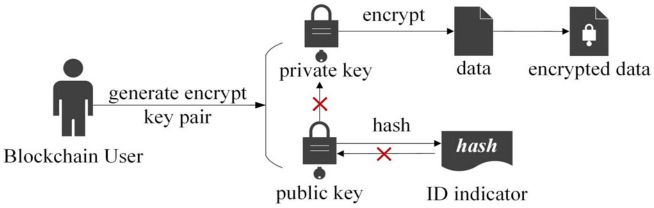

Figure 4. Privacy protection of blockchain.

III. Current Research and Application of Blockchain in Cybersecurity

As mentioned before, blockchain was originally put forward as a foundational technology to construct Bitcoin. The basic principle of blockchain is opening, transparency and sharing. The way that blockchain guarantees trust is by applying cryptographic and mathematical algorithms, instead of using a third-party intermediary. By effectively guarantee the authenticity and uniqueness of transaction, blockchain starts to become the technical core of cryptocurrency, asset management, credit control, etc. And gradually exploring its application in financial, medical, energy and ICT fields. The typical application scenarios are summarized in Figure 5.

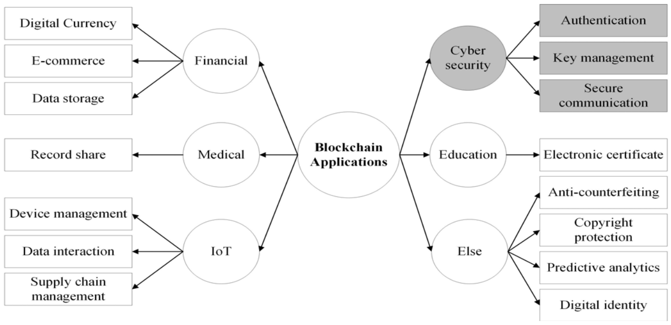

Figure 5. Typical application scenarios of blockchain.

For example, in the field of finance, by introducing blockchain in business operation level, blockchain is able to provide clearing and cross-border payment without changing existing supervision system. Adoption of blockchain also brought in an improvement of business interaction efficiency and an optimization of operational procedures. In medical fields, hospitals and security companies start to cooperate and use blockchain to store medical data, supporting exchange of electronic patient records among different hospitals. And explore a solution to solve the problem of information sharing between different medical mainstays. While in energy fields, blockchain has been applied in smart grid to trade decentralized power resources. In a word, the technical and security advantages provided lots of innovation space for the development of blockchain. Moreover, the innovative privacy and trust mechanism of blockchain has brought possibility in making it an effective means to solve some major problems in cybersecurity. The representative blockchain application scenarios in cybersecurity can be described as follows.

A. Decentralized distributed secure domain name service

Traditional domain name services adopt a hierarchical resolution process and the core functions are centralized in the DNS server. Therefore, DNS servers are highly susceptible to attacks such as DDoS attacks, DNS hijacking and cache poisoning. To address the above problems, [17-18] develops comprehensive studies on blockchain based DNS and construct domain name infrastructures on Bitcoin blockchain. By establishing a map between DNS and hash, users can perform the registration, transmission and data revision of domain name in any system node. A node is responsible for storing the public and private key of domain name owner, as well as recording the domain names after resolution. The combination of blockchain and domain name service enables domain owners to encrypt operation process in blockchain. The originally centralized domain name service becomes decentralized and adversaries can't find a central record to attack or manipulate. Since every system node can act as a DNS server in a DNS system constructed on blockchain, attacks aiming at one or more servers such as the DNS hijacking and cache poisoning will do no harm to the whole system.

B. Keyless Signature Infrastructure

With the explosion of data and equipment, authentication and signature schemes that rely on keys face the problems of key publication, update and revocation in big data environment. The emergence of quantum computers increases the chance of cracking the traditional asymmetric encryption algorithms. To address the above security threats, a Keyless Signature Infrastructure (KSI) is put forward by security researchers [19-22]. KSI takes full advantage of the timestamp in blockchain. A block, in KSI scenario, stores the current state of data, system or network as well as the hash value. KSI will then conduct a continuous monitoring on these hash values with timestamp, thus detecting whether a file, operating system or application is suffering from an unauthorized access. By adapting the timestamp mechanism as a monitor object, it's no need for KSI to maintain, distribute or revoke keys. This makes it easy for KSI to extend to protect a data volume of EB. Security protection systems using KSI have been applied in critical information infrastructures such as nuclear power stations and flood-control systems in England.

C. Secure Data Storage

For a long time, large-scale user data leakage incidents caused by the centralized storage of data occur frequently, especially in important fields which is closely related to national economy and people's livelihood, such as financial, medical, etc. In these areas, sensitive data once leaked will cause disastrous consequences. [23-25] explored to use blockchain to manage the hash value of medical data such as patients' identity, disease situation and therapeutic schedule. By developing customized access rules that meet unique security requirements in particular business scenarios using multi-signature technique, users can only create, share and update a clinical case under permission of the blockchain network. In that way, the transparency of healthcare industry is improved and the various privileges such as doctors, nurses and patients can be managed reasonably and effectively.

Apart from the above use cases, the IoT equipment certification [26-27], Cloud data desensitization [28] and secure data transmission [29] areas are also exploring the application mode of blockchain technology.

IV. Security Issues of Blockchain

With the continuous growth of global attention on blockchain, blockchain related research is becoming in full swing. But objectively, seen from the application layer, blockchain is still in its exploratory stage. There is still a long process of integration and development to go till the perfection of technology and the deep-going of application. Despite the innovative changes of blockchain, the technology itself still has some inherent security risks. Moreover, the revolutionary nature of decentralization and self-organization in blockchain has already triggered ignorable security problems.

A. Technical Limitations

- Limitation of block capacity restricts the wide application of blockchain to a great extent. The capacity of a single block was set to 1MB originally to resist possible DDoS attacks. And there has always been a controversy between bigger or smaller block capacity. Because a bigger block can store more records which will meet the requirement of development. But bigger blocks may cause difficulty in running and managing blockchain nodes. On the other hand, although smaller blocks are easy to manage and more reliable to a third-party payment solution, the available space is extremely limited especially in complex big data environments.

- Distributed storage mechanism creates a boarder attack surface in blockchain. A blockchain system chooses to store a complete copy of all data in every user's side. That means an attacker will have more alternatives to get access to those data. Although content in blockchain is not allowed to tamper, attackers can utilize other techniques such as data mining and correlation analysis to retrieve valuable information related to blockchain applications, users, network structure, etc.

- Consensus mechanism may trigger a cooperative attack. The consensus mechanism of blockchain is based on an assumption that the majority of nodes is honest to run and maintain the system. Once one or more nodes control more than 51% computing power of the whole system, they can join together to launch an attack to tamper with the content in blocks and conduct disruptive attacks such as DDoS.

B. Potential Risk of Cryptography Application

- The problem of private key management is not solved in blockchain. Existing blockchain applications usually use private key to confirm a user's identity and complete a payment transaction. So, the precondition that information can't be falsified is the security of private key. Unlike traditional public key cryptography, blockchain users are responsible for their own private keys, which means that a private key is generated and taken care of by user instead of a third-party. If a user loses his private key, it will be impossible to get access to his digital assets on blockchain.
- Wide application of cryptographic algorithm may introduce unknown backdoors or vulnerabilities. There is an extensive adoption of cryptographic algorithms in blockchain, such as ECC and RSA. Backdoors and security vulnerabilities may emerge in the algorithms themselves or the implementation processes. And then do harm to the blockchain applications and the entire system. Moreover, the new computing technologies like quantum computer will also increase the chance of cracking the asymmetric encryption algorithms.

C. Opensource Blockchain Platforms Attract Intensive Attacks

As an underlying technology of upper-layer applications, blockchain platform supports interoperation of different applications and users. For example, industry data of medical, financial and communication field can be produced, stored, updated and transmit via blockchain platform. The huge economic benefit motivates hackers flocking to digging the security vulnerabilities of open source blockchain platform.

D. Security Management of Self-organization and Anonymity

- Distributed data storage may cause autonomous and frequent data cross border in blockchain use cases. Because blockchain adopts a distributed data storage manner and maintain a full copy of data at every user's side. Once a new transaction is being added to a block, all the data copies should update synchronously. When the blockchain users from different countries, initiative and frequent data cross border will improve the difficulty of supervision.
- Anonymity mechanism may trigger attack backtrack problem. Blockchain calculates the hash value of a user's public key to identify a unique user. But this privacy preserving operation make it impossible verify and trace a user's true identity in network attack backtrack and cybersecurity regulation.

V. Conclusion

Blockchain has been given high expectations in recent years. The application of blockchain has already extended to ICT and network security fields from finance. And the issues of blockchain security is being brought to the table. As a revolutionary new technology in the Internet era, blockchain is accelerating its combination with existing technology and constantly generating new business model. Meanwhile, it's also becoming a challenge to network security regulation mode. This paper conducts a comprehensive research on blockchain in cybersecurity, and analyses the security issues we still face. In future works, more efforts will be done to addressing the security problems of blockchain and exploring better solutions, including the standards for blockchain security requirements and technology testing, mechanism for securing the business flow, clarifying security operations in blockchain, etc.

Acknowledgment

The first author would like to thank Dr. Yixun Hu and Dr. Xuan Zha for proofreading and improving this manuscript. The authors are grateful to the reviewers for their detailed reviews and constructive comments.

References

[1] N. Satoshi, "Bitcoin: A peer-to-peer electronic cash system," Consulted, 2008, pp:1-9.

[2] G. Varriale, "Bitcoin: how to regulate a virtual currency," International Financial Law Review, 2013, 32(6), pp: 43-45.

[3] D. Swartz N., "Bursting the Bitcoin bubble: The case to regulate digital currency as a security or commodity," Tul. J. Tech. & Intell. Prop., 2014, 17, pp: 319-335.

[4] N. Wenker, "Online Currencies, Real-World Chaos: The Struggle to Regulate the Rise Bitcoin," Tex. Rev. L. & Pol., 2014, 19, pp: 145-184.

[5] M. Swan, "Blockchain: Blueprint for a New Economy," O'Reilly Media, Inc.; 2015.

[6] Bitcoinwiki; 2015, https://en.bitcoin.it.

[7] AM. Antonopoulos, "Mastering Bitcoin: unlocking digital cryptocurrencies," O'Reilly Media, Inc., 2014.

[8] Double-spending, https://en.bitcoin.it/wiki/Double-spending

[9] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, "Where Is Current Research on Blockchain Technology?- A Systematic Review," PLoS ONE, 2016, 11(10), pp: 1-27.

[10] D. Tapscott, A. Tapscott, "Blockchain Revolution: How the Technology behind Bitcoin is Changing Money, Business, and the World," 2016.

[11] B. Gipp, N. Meuschke, A. Gernandt, "Decentralized Trusted Timestamping using the Crypto Currency Bitcoin," in Proceedings of the iConference 2015, Newport Beach, CA, USA, Mar. 24-27, 2015.

[12] G. Paul, P. Sarkar, S. Mukherjee, "Towards a More Democratic Mining in Bitcoins" In: Prakash A, Shyamasundar R, editors. Information Systems Security. vol. 8880 of Lecture Notes in Computer Science. Springer International Publishing, 2014. pp: 185-203.

[13] L. Wang, Y. Liu, "Exploring Miner Evolution in Bitcoin Network," In: Mirkovic J, Liu Y, editors. Passive and Active Measurement. vol. 8995 of Lecture Notes in Computer Science. Springer International Publishing, 2015, pp: 290-302.

[14] Zyskind, Guy, O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," Security and Privacy Workshops (SPW), IEEE, 2015, pp: 180-184.

[15] Kosba, Ahmed, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," Security and Privacy (SP), 2016 IEEE Symposium on. IEEE, 2016, pp:839-858.

[16] Meiklejohn, Sarah, Claudio Orlandi, “Privacy-enhancing overlays in bitcoin,” International Conference on Financial Cryptography and Data Security, Springer Berlin Heidelberg, 2015, pp:127-141.

[17] H. Weihong, A. Meng, Sh. Lin, X. Jiagui, L. Yang, “Review of blockchain-based DNS alternatives,” Chinese Journal of Network and Information Security, 2017, 3(3), pp: 71-77.

[18] M. Ali, J. Nelson, R. Shea, M. Freedman, “Blockstack: Design and Implementation of a Global Naming System with Blockchains”, Last visited on, 2016, 25(2).

[19] Tosh, K. Deepak, “Security implications of blockchain cloud with analysis of block withholding attack,” Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. IEEE Press, 2017, pp:458-467.

[20] Liang, Xueping, “Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability,” Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. IEEE Press, 2017, pp:468-477.

[21] Jämthagen, Christopher, Martin Hell, “Blockchain-based publishing layer for the Keyless Signing Infrastructure,” Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 2016 Intl IEEE Conferences. IEEE, 2016, pp: 374-381.

[22] Emmadi, Nitesh, Harika Narumanchi, “Reinforcing Immutability of Permissioned Blockchains with Keyless Signatures' Infrastructure,” Proceedings of the 18th International Conference on Distributed Computing and Networking. ACM, 2017 (46).

[23] Azaria, Asaph, “Medrec: Using blockchain for medical data access and permission management,” Open and Big Data (OBD), International Conference on. IEEE, 2016, pp: 25-30.

[24] Yue, Xiao, “Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control,” Journal of medical systems, 2016 (218).

[25] Ekblaw, Ariel, “A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data,” Proceedings of IEEE Open & Big Data Conference. 2016, pp: 1-13.

[26] Christidis, Konstantinos, Michael Devetsikiotis, “Blockchains and smart contracts for the internet of things,” IEEE Access, 2016, pp: 2292-2303.

[27] Zhang, Yu, Jiangtao Wen, “The IoT electric business model: Using blockchain technology for the internet of things,” Peer-to-Peer Networking and Applications, 2017, pp: 983-994.

[28] Wilkinson, Shawn, J. Lowry,T. Boshevski, “Metadisk a blockchain-based decentralized file storage application,” Technical Report, Available: http://metadisk. org/metadisk. pdf, 2014.

[29] Rowan, Sean, “Securing Vehicle to Vehicle Communications using Blockchain through Visible Light and Acoustic Side-Channels.” arXiv preprint arXiv:1704.02553 (2017).