Blockchain Security: Primitives and Protocols

Yannan Li[0000−0002−4407−9027]*

Institute of Cybersecurity and Cryptology, School of Computing and
Information Technology, University of Wollongong, Wollongong, NSW 2522,
Australia. yannan@uow.edu.au

Abstract. It is widely accepted that blockchain is a disruptive technology that reshapes the way of doing business in finance due to its decentralization, transparency and immutability. Blockchain can serve as the backbone technique in various applications with its salient features. However, these blockchain-based systems may still suffer from security concerns. In this talk, we will discuss blockchain security, in terms of its underlying primitives and built-on protocols. To be more specific, we will talk about the privacy and regulation in blockchain-based cryptocurrencies, the security concerns in blockchain-based e-voting and the non-equivocation in blockchain systems. In each scenario, we will discuss the remaining problems of the existing works and present possible solutions.

1 Introduction

Blockchain is a distributed database that records all the transactions in the system. Blockchain can be used to achieve fully decentralized systems with its consensus, incentive, transparency and immutability. Gartner, a leading research and advisory company, forecasts that the business value generated by blockchain will reach $176 billion by 2025 and $3.1 trillion by 2030, respectively [2]. Blockchain has a spectrum of applications ranging from healthcare, manufacture, transportation to IoT. However, there are still many things to do to improve blockchain security. In this talk, we will introduce several cryptographic primitives and protocols to enhance blockchain security and achieve blockchain-based secure protocols. protocols. This talk is structured into three important scenarios in blockchain and the corresponding security issues and potential solutions.

Cryptocurrencies are among the successful applications of blockchain, with growing attention and significant influence. The global crypto market capitalization is $2.05 trillion US dollars (Sep 2022). Compared to the traditional trading model in real life, which leak personal information, Bitcoin uses pseudonyms, which is a random account rather than real-world identities, to conduct transactions in the system so as to protect users' privacy. However, it is proved that the security level provided only by pseudonyms is far from satisfactory. These

* This work is also supported by the Australian Research Council Discovery Early Career Researcher (ARC DECRA DE230100001).

pseudonyms can be linked to real-world identities if enough transactions are collected and analyzed [3]. Therefore, anonymous cryptocurrencies were proposed to intensively protect transaction privacy and user anonymity based on various of cryptographic tools, such as Zerocoin [4], Zerocash [5] and Monero [6]. Anonymous cryptocurrencies gain attention due to enhanced privacy guarantee, however, this makes blockchain susceptible to abuse, security concerns, and even cybercrimes. Besides, the governments are politically conservative about blockchain. For example, the decentralized payment company Ripple (https://ripple.com/) was sustained a $700,000 fine by the U.S. Financial Crimes Enforcement Network (FINCEN) because of inadequate regulation on their transactions networks [7]. In Feb 2020, the Australian government released National Blockchain Roadmap, with a special emphasis on blockchain security and regualtion [8]. How to deal with the conflict user privacy and proper regulation on malicious users is a tricky problem. In the first part of this talk, we introduce a protocol to balance the anonymity and regulation in privacy-preserving cryptocurrencies Monero [9,10]. Specifically, we provide two mechanisms to trace the one-time key and long-term key of a malicious user, while still maintaining the privacy of honest users.

Election is one of the most important measures to achieve democracy. However, traditional voting with a central election authority suffers from privacy issues when ballots are tallied. With the salient nature of blockchain, it can effectively remove the central party who controls the system with privacy concerns. Thus we proposed a blockchain-based self-tallying e-voting system [11, 12] with no central authority to tally the votes. The voting results can be calculated and released publicly after all the legitimate votes cast their ballots on blockchain. However, the involvement of blockchain will bring new drawbacks in these self-tallying voting systems, that are the fairness issues - the abortive issues and adaptive issues [13, 14]. In the second part of the talk, we will demonstrate the possible solutions to address the security and privacy concerns in blockchain-based e-voting systems, and achieve a secure self-tallying e-voting system with various implementation results [15].

Equivocation is to convey conflicting statements in a protocol, which is a quite common problem and happens often in distributed systems, such as double-spending in cryptocurrencies and issuing two certificates for one identity [16]. Therefore, non-equivocation is one of the fundamental requirements in distributed systems. Existing literature to solve the equivocation problems is based on trusted hardware or strong assumptions, which is not satisfactory in real life. The public logs provide a breakthrough in addressing the equivocation issues in distributed systems. However, all the existing solutions are to deal with double-spending or double authentication [17, 18]. The solutions to tackle more general type of equivocation are still missing in the literature. The third part of this talk is to provide a contractual solution to handle generalized equivocation, which also supports user-defined policies [19]. We will introduce a new cryptographic primitive, the policy-authentication-preventing signatures, to support our design and then introduce the integration with blockchain systems.

References

1. S. Nakamoto and A. Bitcoin. A peer-to-peer electronic cash system. Bitcoin.?URL: https://bitcoin. org/bitcoin. pdf, 4, p.2, 2008.
2. https://www.gartner.com/en/doc/3855708-digital-disruption-profile-blockchains-radical-promise-spans-business-and-society.
3. F. Reid and M. Harrigan. An analysis of anonymity in the bitcoin system. In Security and privacy in social networks, pages 197-223. Springer, 2013.
4. I. Miers, C. Garman, M. Green, and A. D. Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In 2013 IEEE Symposium on Security and Privacy, pages 397-411. IEEE, 2013.
5. E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. Zerocash: Decentralized anonymous payments from bitcoin. In 2014 IEEE Symposium on Security and Privacy, pages 459-474. IEEE, 2014.
6. S. Noether. Ring signature con
dential transactions for monero. IACR Cryptol. ePrint Arch., 2015:1098, 2015.
7. https://www.financemagnates.com/cryptocurrency/news/ripple-fined-700k-by-ncen-for-msb-aml-violations/.
8. https://www.industry.gov.au/data-and-publications/national-blockchain-roadmap.
9. Y. Li, G. Yang, W. Susilo, Y. Yu, M. H. Au, and D. Liu. Traceable monero: Anonymous cryptocurrency with enhanced accountability. IEEE Transactions on Dependable and Secure Computing, 18(2): 679-691, 2021.
10. Y. Li, W. Susilo, G. Yang, Y. Yu, X. Du, D. Liu, and N. Guizani. Toward privacy and regulation in blockchain-based cryptocurrencies. IEEE Network, 33(5):111-117, 2019.
11. F. Hao, P. Zielinski: A two-Round Anonymous Veto Protocol. Security Protocols Workshop, pages: 202-211, 2006.
12. A. Kiayias and M. Yung. ?Self-tallying elections and perfect ballot secrecy?. In International Workshop on Public Key Cryptography, Springer, Berlin, Heidelberg, pages 141-158, 2002.
13. J. Liu, T. Jager, Saqib A. Kakvi, Bogdan Warinschi: How to build time-lock encryption. Des. Codes Cryptography 86(11): 2549-2586, 2018.
14. T. Jager: How to build time-lock encryption. Cryptology ePrint Archive, Report 2015/478. http://eprint. iacr.org/, 2015.
15. Y. Li, W. Susilo, G. Yang, Y. Yu, D. Liu, X. Du, and N. Guizani. A blockchain-based self-tallying voting protocol in decentralized iot. IEEE Transactions on Dependable and Secure Computing, 19(1), 119-130, 2022.
16. T. Ruffing, A. Kate, and D. Schröder, Liar, liar, coins on fire! Penalizing equivocation by loss of bitcoins. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pages 219-230, 2015.
17. B. Poettering, and D. Stebila. Double-authentication-preventing signatures. International Journal of Information Security, 16(1), 1-22, 2017.
18. D. Derler, S. Ramacher, and D. Slamanig, Short double-and n-times-authentication-preventing signatures from ECDSA and more. IEEE European Symposium on Security and Privacy, pages 273-287, 2018.
19. Y. Li, W. Susilo, G. Yang, Y. Yu, T. V. X. Phuong, and D. Liu. Non-equivocation in blockchain: Double-authentication-preventing signatures gone contractual. In Proceedings of the 2021 ACM ASIACCS, pages 859-871, 2021.