SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

A Privacy-Preserving Data Sharing Framework for Public Blockchains

Yepeng Ding * Hiroyuki Sato *

Keywords: data sharing, privacy preservation, access control, blockchain, decentralized storage

Abstract

Blockchain technology has been adopted in a wide range of fields [3, 4, 2]. Particularly, worldwide decentralization of data persistence and sharing is advancing with the evolution of public blockchain technologies, as can be seen by the boom of decentralized applications (DApp). These DApps have presented a set of attractive properties including accessibility, automation, transparency, interoperability, finality, borderlessness, and innovativeness. These properties are generally achieved through on-chain data persistence and sharing supported by transparent public blockchains such as Ethereum [5] that are permissionless and fully disclose all types of data.

However, full transparency may lead to privacy issues. Besides, the on-chain persistence of large data is significantly expensive technically and economically. These issues lead to the difficulty of sharing fairly large private data while preserving attractive properties of public blockchains. Although direct encryption for on-chain data persistence can introduce confidentiality, new challenges such as key sharing, access control, and legal rights proving are still open. Meanwhile, cross-chain collaboration still requires secure and effective protocols, though decentralized storage systems such as IPFS [1] bring the possibility for fairly large data persistence.

In this paper, we propose Sunspot, a decentralized framework for privacy-preserving data sharing with access control on transparent public blockchains, to solve these issues. Sunspot protocols are generalized to be independent of blockchain platforms and support multiple access control mechanisms to enable flexible data sharing in various scenarios. Particularly, we show an identity management model and a management-free model for identification based on two different access control mechanisms. Besides, we present MyPub, a decentralized privacy-preserving publishing platform based on Sunspot to demonstrate the practicality and applicability of Sunspot in practice. Furthermore, we evaluate the security and privacy of Sunspot through theoretical analysis and experiments.

* The University of Tokyo, 7 Chome-3-1 Hongo, Bunkyo City, Tokyo 113-8654, Japan
{youhoutei,schuko}@satolab.itc.u-tokyo.ac.jp

References

[1] Juan Benet. Ipfs-content addressed, versioned, p2p file system. *arXiv preprint arXiv:1407.3561*, 2014.

[2] Yepeng Ding and Hiroyuki Sato. Bloccess: towards fine-grained access control using blockchain in a distributed untrustworthy environment. In *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, pages 17–22. IEEE, 2020.

[3] Yepeng Ding and Hiroyuki Sato. Dagbase: a decentralized database platform Using DAG-based consensus. In *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, pages 798–807. IEEE, 2020.

[4] Yepeng Ding and Hiroyuki Sato. Derepo: a distributed privacy-preserving data repository with decentralized access control for smart health. In *2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, pages 29–35. IEEE, 2020.

[5] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014.