Bandwidth-Efficient and Storage-Efficient Blockchain on Hyperledger Fabric

Abstract—Bitcoin network this is the abstract for the storage

Index Terms—Bitcoin Network, Mining Pools, Malthusian Trap, Incentive Mechanism

1 Introduction

BITCOIN [1] is a decentralized peer to peer (P2P) cryptocurrency that was first proposed by Satoshi Nakamoto in 2008. Without resorting to any trusted third party, Bitcoin adapts a cryptographic proof mechanism that enables anonymous peers to complete transactions through the P2P network. Blockchain is the core mechanism of the Bitcoin system. It not only records historical transactions from Bitcoin clients, but also prevents the Bitcoin network from double spending attacks [2]. The Bitcoin network participants, who maintain and update the ongoing chain of blocks, are called miners. These miners compete in a mining race driven by an incentive mechanism [3], [4], where the one who first solves the Bitcoin cryptographic puzzle [5] has the right to collect unconfirmed transactions into a new block, append the new block to the main chain, i.e., the longest chain of blocks, and gain some BTCs [6] as a mining reward.

2 Related Work

¡The Privacy Protection Mechanism of Hyperledger Fabric and its Application in Supply Chain Finance¿–"Multi-channel": Blockchain technology ensures that data is tamper-proof, traceable, and trustworthy. This article introduces a well-known blockchain technology implementation-Hyperledger Fabric. The basic framework and privacy protection mechanisms of Hyperledger Fabric such as certificate authority, channel, private data collection, etc, are described. As an example, a specific business scenario of supply chain finance is figured out. And accordingly, some design details about how to apply these privacy protection mechanisms are described.

¡Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation¿–"Private Data": in this work we explored adding private-data support to Hyperledger Fabric using secure multiparty computation (MPC). Specifically, in our solution the peers store on the chain encryption of their private data, and use secure MPC whenever such private data is needed in a transaction. This solution is very general, allowing in principle to base transactions on any combination of public and private data.

¡Private Data Objects: An Overview¿–"Private Data": We present private data objects (PAOs), a technology that enables mutally untrusted parties to run smart contracts over private data.

¡The Approach to Managing Provenance Metadata and Data Access Rights in Distributed Storage Using the Hyperledger Blockchain Platform¿–"Fault-tolerant, safe and secure": The paper suggests a new approach based on blockchain technologies and smart contracts to creation of a distributed system for managing procenance metadata, as well as access rights to data in distributed storages, which is fault-tolerant, safe and secure from the point of view of preservation of metadata records from accidental or intentional distortions. The implementation of the proposed approach is based on the permissioned blockchains and on the Hyperledger Fabric blockchain platform in conjuction with Hyperledger Composer.

¡ForkBase: An Efficient Storage Engine for Blockchain and Forkable Applications¿–"Performance": In this paper, we present ForkBase, a storage engine specifically designed to provide efficient support for blockchain and forkable applications. By integrating the core application properties into the storage, ForkBase not only delivers high performance but also reduces development effort.

¡A Blockchain-Based Decentralized Data Storage and Access Framework for PingER¿–"Efficient Lookup": We use the permissioned blockchain Hash Tables (DHT) for this purpose. In the proposed framework, metadata of the files are stored on the blockchain whereas the actual files are stored off-chain through DHT at multiple locations using a peer-to-peer network of PingER Monitoring Agents.

¡A Public Blockchain Solution Permitting Secure Storage and Deletion of Private Data - Draft¿–"Security and Privacy": We present the design for a blockchain network and minimum requirements for governing aggrement among a privileged subsets of the nodes' operators to ensure that sensitive and private data can be handled and securely deleted on demand. The guiding design criteria are based on an operational blockchain application and include data minimization under the constraint of providing fault tolerance, postquantum security, privacy of sensitive data, and the freedom to join as a (non-privileged) node without any special provisions or legal obligations.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] G. O. Karame, E. Androulaki, M. Roeschlin, A. Gervais, and S. Čapkun, "Misbehavior in bitcoin: A study of double-spending and accountability," *ACM Transactions on Information and System Security (TISSEC)*, vol. 18, no. 1, p. 2, 2015.

[3] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein, "Bitcoin mining pools: A cooperative game theoretic analysis," in *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*. International Foundation for Autonomous Agents and Multiagent Systems, 2015, pp. 919–927.

[4] O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden, "Incentive compatibility of bitcoin mining pool reward functions," in *International Conference on Financial Cryptography and Data Security*. Springer, 2016, pp. 477–498.

[5] I. Giechaskiel, C. Cremers, and K. B. Rasmussen, "On bitcoin security in the presence of broken cryptographic primitives," in *European Symposium on Research in Computer Security*. Springer, 2016, pp. 201–222.

[6] BTC. [Online]. Available: https://en.bitcoin.it/wiki/Bitcoin, Accessed on 31 January 2019.