Secure Logging with Blockchains and its Utilization for Central Bank Digital Currency

Ivan Homoliak
Brno University of Technololgy,
Faculty of Information Technology

In this talk, we summarize our contributions in the area of secure logging with blockchains and trusted computing (TEE). The talk is based two papers of us that are under submission to core A* conferences:

1. Homoliak, Ivan, and Pawel Szalachowski. "Aquareum: A centralized ledger enhanced with blockchain and trusted computing." arXiv preprint arXiv:2005.13339 (2020). https://arxiv.org/abs/2005.13339
2. Homoliak, Ivan, et al. "CBDC-AquaSphere: Interoperable Central Bank Digital Currency Built on Trusted Computing and Blockchain." arXiv preprint arXiv:2305.16893 (2023). https://arxiv.org/abs/2305.16893

Moreover, the talk tangentially mentions the data provenance related security issues and countermeasures from another paper of us:

1. Homoliak, Ivan, et al. "The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses." IEEE Communications Surveys & Tutorials 23.1 (2020): 341-390. https://ieeexplore.ieee.org/abstract/document/9239372

The default length of the presentation is 90 mins and the slides can be viewed at https://drive.google.com/file/d/1AypTylUSH99LUZ3Rm6RkgCBQqjy0tgUh/view?usp=sharing . The presentation can be shortened to arbitrary time according to the requirements but ideally it would need at least 40 mins.

Abstract:
We start by briefly introducing the security architecture for blockchains and the application layer categories. We will look in detail at the sub-category of data provenance (and secure logging), where we discuss relevant properties in terms of security and privacy. Next, we will focus on centralized ledger systems that are designed for secure logging as append-only databases providing immutability (i.e., tamper resistance) as a core property. In the next part of the talk, we present Aquareum, a framework for centralized ledgers mitigating their main limitations. Aquareum employs a trusted execution environment (TEE) and a public smart contract platform to provide verifiability, non-equivocation, and mitigation of censorship. In Aquareum, a ledger operator deploys a pre-defined TEE enclave code, which verifies the consistency and correctness of the ledger for every ledger update. Then, proof produced by the enclave is published at an existing public smart contract platform, guaranteeing that the given snapshot of the ledger is verified and no alternative snapshot of this ledger exists. Furthermore, whenever a client suspects that her query (or transaction) is censored, she can

(confidentially) request a resolution of the query via the smart contract platform. The ledger operator noticing the query is obligated to handle it by passing the query to the enclave that creates a public proof of query resolution and publishes it using the smart contract platform. With such a censorship-evident design, an operator is publicly visible when misbehaving, thus the clients can take appropriate actions (e.g., sue the operator) or encode some automated service-level agreements into their smart contracts. Since Aquareum is integrated with a Turing-complete virtual machine, it allows arbitrary transaction processing logic, including tokens or client-specified smart contracts. In the last part of the talk, we present CBDC-AquaSphere, a protocol that uses a combination of a trusted execution environment (TEE) and a public blockchain to enable interoperability over independent centralized CBDC ledgers (based on Aquareum). Our interoperability protocol uses a custom adaptation of atomic swap protocol and is executed by any pair of CBDC instances to realize a one-way transfer. It ensures features such as atomicity, verifiability, correctness, censorship resistance, and privacy while offering high scalability in terms of the number of CBDC instances. Our approach enables two possible deployment scenarios that can be combined: (1) CBDC instances represent central banks of multiple countries, and (2) CBDC instances represent the set of retail banks and a paramount central bank of a single country.