Title:

sigBridge: Cross-chain Bridge for Permissioned Blockchains and its application to access control

Abstract:

With the rise of decentralized systems that span multiple blockchains, there is a growing need for robust cross-chain bridges that ensure the correct working of applications across multiple chains. In this paper, we consider a decentralized user-centric resource-sharing application over a permissioned blockchain that uses a cross-chain bridge to extend the correct working of the application to multiple chains. The application allows a blockchain member to define per-object policy for access to digital objects that they are willing to share with other members of the blockchain ecosystem and be confident that the policy will be enforced. The system uses smart contracts to enforce user-defined policies in the user's home blockchain, and a bridge to extend the guaranteed control to members of other blockchains. To ensure consistent and secure working of the system across multiple chains, we adapt zkBridge, a cross-chain bridge protocol that was proposed for non-permissioned blockchain (CCS'22) to the setting of permissioned blockchain. We show that in this new setting, the computationally expensive zero-knowledge proofs of zkBridge can be avoided, and that this results in the same cross-chain security guarantee as zkBridge in permissioned setting. We use the new bridge protocol, called *sigBridge*, to extend an existing decentralized resource-sharing application with the correctness guarantee, to multiple blockchains and argue the security of the design. We also give a proof-of-concept implementation for an attribute-based resource-sharing application that is implemented using two private Ethereum blockchains, and report the computation costs of the protocol.

Keywords:

Cross-chain Bridge, Permissioned blockchain, User-centric access control, Attribute-based resource sharing