ABSTRACT

The increasing emphasis on autonomous decentralized systems has accelerated interest in distributed ledger technologies (DLT). Blockchain, as one of the prominent DLTs, has established its role in enterprise environments. Along with the advent and expansion of blockchain adoption, various interoperability approaches have been developed in recent years, reflecting a broader shift towards inter-blockchain communication. Despite this progress, interoperability in blockchain networks continues to pose certain unique challenges, such as maintaining accountability, inter-blockchain access control, and cross-consortium redactability in permissioned blockchain networks. These are explored in this thesis. Existing solutions are thoroughly reviewed, and open research scopes and gaps are highlighted. Subsequently, novel mechanisms and architectural frameworks are proposed that enable secure, auditable, access-governed interoperability and redactability among distinct blockchain systems.

In interactions between permissioned blockchains, cross-chain transactions cannot be verified outside the chain, because the private ledgers of either chain are not observable externally. This gap creates the possibility of forged claims or non-repudiation issues, as faults or system-wide failures in one blockchain can be utilized by the other to defraud. To address this challenge, we introduce cross-chain transaction receipts. The receipts record the acknowledgment of cross-chain transactions necessary for non-repudiation and are encapsulated in snapshots. These snapshots can ensure auditable proof of bilateral agreements between distinct blockchain networks.

On the other hand, in the context of enterprise blockchain systems, robust access control is crucial for enabling the secure and governed exchange of data and assets across networks. While most existing studies focus on access control mechanisms within individual blockchains, cross-chain data and asset transfers introduce additional complexities. Such transfers often span multiple blockchain networks, each governed by distinct internal stakeholders and access control policies. Also the source of an inter-consortium request can vary widely, ranging from individual members within an organization, to entire organizations, or even joint requests from multiple organizations acting

together. To address these, we introduce an end-to-end access control framework discussed in this thesis to address the complexities for cross-chain interactions between permissioned networks. Through experiments, we demonstrate that our solution can handle cross-chain access control for access request-responses with minimal overhead.

Additionally, blockchain networks often require erasure or modification of data for reasons such as eliminating redundant records, correcting erroneous information, or removing illegitimate content. To handle such cases effectively, appropriate redaction governance mechanisms must be in place. These are essential when modifications or deletions need to be managed inside and across multiple autonomous systems. A few existing approaches enable redaction, but they lack focus on governance mechanisms for enterprise cross-consortium redactions. A comprehensive redaction control framework is introduced and detailed in this thesis. The said approach regulates and validates redaction requests across blockchains. Our evaluation indicates that the solution can effectively enforce redaction policies across interoperable blockchains, maintaining low performance overhead and demonstrating scalability under increasing workload.

Keywords: blockchain, cross-chain, interoperability, snapshot, inter-blockchain disputes, access control, decentralized systems, RTBF, privacy, security, redactable Blockchain, GDPR