ABSTRACT

Development of permissioned distributed ledger technology has introduced blockchains as a viable solution for decentralizing business-to-business interactions in closed consortium networks. Consequently, in recent years, apart from the usual applications around cryptocurrencies, blockchain has seen application in enterprise scenarios such as supply chain, trade finance, logistics, energy trading, etc. However, such rapid adoption and deployment of permissioned networks have introduced technical fragmentation in terms of protocols, algorithms, formats, architecture, and policies (e.g. governance models). This heterogeneity stands as a barrier between different permissioned consortium blockchain networks that wish to interoperate and communicate for broader business goals. Moreover, permissioned distributed ledgers by design were made private so that entities that are not consortium members and, thus outside the network boundary, have no visibility over the network's data, assets, or functions. As a result, there are no means for the consortium to communicate with external entities such as end-users or consumers to which the businesses that form the consortium might need to dispense services. This thesis studies the challenges, existing works, and gaps in both permissionless-permissioned and permissioned-permissioned blockchain interoperability and introduces methods and apparatus for enabling interoperability.

Towards enabling permissioned consortium blockchains to communicate with their end-consumers in the open network, this thesis proposes the first framework and set of protocols for permissionless-permissioned blockchain interoperability. This includes a mechanism allowing the transfer of data such as end-consumer requests, from the open network to the consortium, while ensuring consensus of the consortium participants on the data and the order in which the data arrive. Another protocol facilitates verifiable transfer of data from the consortium to the public blockchain. A proof-of-concept implementation for the use case of cloud federations and scalability evaluations demonstrates the system's viability.

Existing protocols for inter-consortium verifiable transfer of data require the pre-configuration of identities such as public keys / certificates of the blockchain participants. For robust permissioned-permissioned interoperability while eliminating manual identity configuration, in this thesis, we propose an architecture and protocols for exchanging identities across permissioned blockchain networks. We introduce a decentralized identity infrastructure for trust basis that utilizes the decentralized identifier and verifiable credential concepts. Our solution requires minimal changes to the existing deployed networks, and we demonstrate its usability by applying it in a trade-finance and trade-logistics interoperability scenario.

Determining a common trust basis is an essential requirement for cross-blockchain identity exchange. However, revealing all trust anchors results in loss of privacy since the trust anchors are often well-known organizations such as governments, NGOs, large companies, political organizations, etc. Revealing a trust anchor reveals the entity's association with the same. We develop protocols for privacy preserving negotiation of common trust anchors across blockchain networks to facilitate cross-chain identity exchange. We propose two variants of solutions, one with the active participation of the trust anchors themselves and the other without involving the trust anchors using secure multiparty computation. Through experiments, we evaluate the efficiency of our protocol, and we also prove its security against malicious adversaries.

Finally, we extend the privacy-preserving trust anchor negotiation for blockchains to a more general use case of any verifiable credential presentation flow that requires a common credential certifier. We formally define this problem as 'private certifier intersection' (PCI). Through a novel extension of secret sharing based secure multiparty computation protocols for elliptic curve pairings, we introduce efficient solutions for two different variants of PCI. We perform a detailed evaluation of the protocols on consumer hardware in a real-world setting by placing parties at two different continents.

To summarize, we introduce methods and apparatus for blockchain interoperability and identity management for facilitating cross-chain interactions between permissioned networks and permissionless networks, as well as between different permissioned networks. Bridging the gaps between different decentralized systems, our conrtibutions pave the way for end-to-end connected decentralized networks starting from closed groups of entities such as businesses, and ending at the open network of end-users.

Keywords: blockchain; identity; distributed ledger technology; interoperability