Abstract

The increasing adoption of blockchain systems and Self-Sovereign Identity frameworks is reshaping the way digital assets and personal data are managed, enabling new forms of decentralization and user control. However, these systems also introduce important challenges, particularly in enabling interoperability across heterogeneous blockchains and in designing secure privacy-preserving identity protocols. In this context, this thesis develops cryptographic protocols that address these challenges: a new protocol for atomic swaps is introduced, a post-quantum implementation of an anonymous credential scheme is presented, and a scheme for delegatable presentations of verifiable and anonymous credentials is proposed.

The thesis is organized into two main parts. The first part provides the theoretical background required to understand the contributions developed in the second part. In particular, Chapter 1 introduces the main cryptographic preliminaries, Chapter 2 describes the core principles of blockchain technology, and Chapter 3 focuses on verifiable and anonymous credential schemes. The second part of the thesis presents the original contributions. In Chapter 4, a new two-phase protocol (BTLE) for the decentralized exchange of digital assets between heterogeneous blockchains is presented. BTLE replaces the hash-time-locked contract (HTLC) mechanism commonly used in atomic swaps with a construction based on time-lock puzzles, thereby enabling exchanges even between blockchains that lack a compatible scripting language or shared hash functions. A second contribution of this work is the introduction of a new time-lock puzzle construction based on Pell conics, offering better performance compared to the classical approach of Rivest, Shamir, and Wagner. Chapter 5 focuses on the design and implementation of a post-quantum anonymous credential framework for Self-Sovereign Identity systems, and presents an initial performance evaluation at the 128-bit security level. Finally, Chapter 6 introduces the formal notion of a verifiable presentation delegation scheme. The work defines the core syntax and security requirements of delegation schemes, including correctness, unforgeability, and unlinkability, and presents two concrete instantiations: one compatible with verifiable credentials as deployed in the EUDI Architecture Reference Framework, and one supporting BBS anonymous credentials. Both schemes are formally proven secure, and their integration into real-world infrastructures, such as the European Blockchain Services Infrastructure (EBSI) and the EUDI framework, is discussed.