

ICT25-056 - Optimal Cross-Chain and Cross-Layer Protocols (CROSS)

Abstract

CROSS addresses a fundamental limitation of today's blockchain infrastructure: the lack of secure interoperability at scale. While blockchains like Bitcoin and Ethereum enable decentralized applications and self-custodial assets, they remain siloed systems. Seamless cross-chain communication—essential for unlocking the full potential of decentralized finance (DeFi)—requires one chain to verify and react to events that occurred on another. However, existing solutions either rely on centralized relays, incur high on-chain costs, or are fundamentally limited by the scripting and scalability constraints of the underlying platforms.

CROSS proposes a new foundation for trustless interoperability based on three core pillars. First, we will design optimal off-chain light clients for diverse consensus models—including proof-of-work, proof-of-stake, and DAG-based protocols—that minimize trust, interactivity, and proof size. Second, we will develop on-chain interoperability protocols that translate these light clients into secure bridge constructions, using Layer 2 architectures and permissionless data availability layers to overcome the limitations of constrained blockchains like Bitcoin. Third, we will establish the first compositional security framework for interoperability, combining simulation-based proofs with economic security arguments to reason about correctness under both adversarial and rational behavior.

Together, these contributions will enable the first trust-minimizing, scalable bridge protocols applicable across heterogeneous blockchain ecosystems. CROSS will provide a principled blueprint for secure cross-chain systems, grounded in formal models and deployable through modular, efficient protocols.

Scientific disciplines:

Distributed systems (40%) | IT security (50%) | Theoretical computer science (10%)

Keywords:

blockchains cross-chain communication light clients bridges interoperability scalability Layer 2 protocols data availability game-theoretic security interactive Universal Composability framework

Principal Investigator: Georgia Avarikioti

Institution: TU Wien

Co-Principal Investigator(s): Matteo Maffei (TU Wien)



Status: Ongoing (01.02.2026 – 31.01.2030)

GrantID: 10.47379/ICT25056

Further links to the persons involved and to the project can be found under
<https://www.wwtf.at.jpeto2.brunner.at/funding/programmes/ict/ICT25-056/>