ICT22-045 - SCALE2: SeCure, privAte, and interoperabLe layEr 2

Abstract

Blockchains are revolutionizing the digital economy, but scaling them to meet the demands of DeFi and Web 3.0 has proven difficult, even after a decade of research. Multiple solutions have been proposed to address this issue, the most prominent of which are the so-called Layer 2 (L2) solutions. In L2, the main transaction load is moved off-chain, thereby dramatically reducing the storage and computation overhead of blockchain validators, while maintaining the on-chain security guarantees. The two leading L2 paradigms are payment channel networks (PCNs) and rollups: these expose a trade-off between capital requirements and on-chain footprint that hinders their practicality. Besides the previous trade-off, several system assumptions, such as synchrony and online participation, prohibit the widespread adoption of these protocols. To add insult to injury, both solutions suffer from significant privacy and interoperability limitations and operate in isolation, which obstructs the design of scalable DeFi and Web 3.0 applications. SCALE2 will deliver the first L2 framework that reconciles practicality, privacy, interoperability, and bridging of various L2 solutions. This vision will be realized through a series of game-changing advances, including a formal analysis of the minimal system assumptions and privacy leakage, as well as novel constructions for efficient, privacy-preserving, and interoperable PCNs and rollups.

Scientific disciplines:
Theoretical computer science (60%) | Practical computer science (40%)

Keywords:
Layer 2, payment channels, rollups, security, efficiency, interoperability

---

Principal Investigator:	Georgia Avarikioti
Institution:	TU Wien
Co-Principal Investigator(s):	Krzysztof Pietrzak (Institute of Science and Technology Austria) Matteo Maffei (TU Wien)

v.l.n.r. Georgia Avarikioti; Eleftherios Kokoris-Kogias; Matteo Maffei

---

Status: Ongoing (01.06.2023 - 31.05.2027)

Further links to the persons involved and to the project can be found under
https://www.gmbh.wwtf.at/funding/programmes/ict/ICT22-045/