ZKP for Blockchains

Anca Nitulescu, Input Output

Abstract:

In this talk, I will present the application of zero-knowledge proofs in decentralized settings such as blockchains. The main two properties that ZK proofs enhance in public ledgers are transaction privacy and scaling of the information that needs to be published on the chain.

Some of the different concrete use cases that I will discuss are 1) anonymous transactions (ZCash, Midnight), 2) Layer 2 or zk-Rollups, and 3) provable decentralized storage (Filecoin). In particular, the talk will focus on presenting three different strategies to improve proving costs on-chain, while maintaining (or not) privacy: proof aggregation, recursive proof composition, and folding schemes. The main ideas behind the schemes representing the state-of-the-art for each category will be presented, with the different goals and properties: SnarkPack aggregation, Halo2 recursion, and Nova folding.

Biography:

Anca Nitulescu is an Applied Cryptography Researcher at Input Output Global (IOG) working on SNARK-focused projects. Prior to joining IOG, Anca was a Cryptography Researcher at Protocol Labs with contributions to the design and analysis of secure decentralized storage protocols. Anca was a postdoc at Aarhus University in 2018. Before that, Anca completed a PhD at ENS Paris under the supervision of David Pointcheval and Dario Fiore and worked on topics such as post-quantum secure SNARKs based on lattices, verifiable computation over encrypted data and authentication primitives, as well as on writing outreach material about Zero-Knowledge SNARKs. Anca's current main areas of interest are zk-SNARK protocols, focusing on scalability improvements through aggregation or folding. Anca also works on protocols for distributed settings, formalizations, and security studies of blockchain protocols.