Hash function for State Commitment

R&D Session at Forschungsingenieurtagung - June 2025.

Duration: 1 hr

Moderator: Dmitry Khovratovich (@khovratovich)
Note taker: TBA

Agenda

- [10 mins] State commitment as a zkEVM bottleneck. The role of hash functions in the state trie. Hash functions Zoo: from Blake to Poseidon. Tradeoffs and diversity. Security. Proofsystem-friendly hashes.
- [15 mins] Discussion: prover complexity of traditional hashes for various proof systems. Hash as a fraction of the total cost.
- [15 mins] Discussion: impact of future proof system improvements on relative and absolute hash function proof costs.
- [15 mins] Discussion: state domain. Binary vs prime. Conversion issues.
- [5 mins] Discuss next steps

Summary

In this session we discuss the cost of proving the state entries inside zkEVM, and the role of hash functions in this cost. We discuss alternatives to the current MPT: classical (“binary”) hashes, prime-field designs (Poseidon and friends), pre-quantum hashes (Verkle), – and the proof systems that suit them.

Goals

1. Identify if proving the classical MPT is expensive enough to mandate its change.
2. Separate annoying issues of the state of the art – from the bottlenecks.
3. Discuss the existing alternatives to the MPT and to the hash function inside from various perspectives: plain performance, proof cost, GPU friendliness, security status, universality.