Zk-Rollups: paving the way for new blockchain applications

**Blockchain Background**
- A blockchain is a decentralized, distributed database responsible for executing, securing, and making data available.
- Execution is limited by node computing power and secured by a consensus algorithm.
- To verify execution, nodes independently re-execute instructions and compare results to those provided in the block.

**ZKP Background**
- Zero-Knowledge Proofs succinctly prove computations, reducing the cost of verification in a decentralized system.
- Centralizing the computation and providing the proof can significantly reduce verification costs in a decentralized system without lost of security.

**Verifiable Computation: How it works**

1. Transform a program into a polynomial equation satisfiability.
2. The Schwartz-Zippel lemma succinctly verifies the equation with high probability.
3. A polynomial commitment scheme provides blind verification of the polynomial equation.
4. The Fiat-Shamir transform makes the proof non-interactive.

**Arithmetization**
- Code or Program to verify
- Transformation into one univariate polynomial
- Reduce to random check

\[ L(X) = \text{representation of left gates values} \]
\[ R(X) = \text{representation of right gates values} \]
\[ O(X) = \text{representation of output gates values} \]

\[ T(X) = \prod (X - \text{gate}) \]
\[ P(X) = L(X) \cdot R(X) - O(X) \]

- \[ P(X) = 0 \text{ when X is the gate number} \]
- \[ P(X) \] must be divisible by \( T(X) \)

**Polynomial Commitment**
- A private polynomial
- \( P(Z) = Y \)
- Public zero-knowledge proof

**Zk-Rollup: A High Security Layer**

- A smart contract stores the funds and state of the zk-rollup accounts.
- Transaction execution is centralised around a validator.
- Data is stored on the blockchain.
- Execution is verified by the smart contract.
- Funds cannot be stolen.
- The validator cannot perform cryptographic attacks but can censor a transaction (only) on the zk-rollup.

**Thesis**
- Develop applications beyond the financial scope.
- Connect the IoT with blockchain technology using zk-rollups.

**Perspectives**
- Reinforce the security of embedded systems.
- Enable blockchain technology inside any device.
- Explore new arithmetization designs for specific applications.

---