Zk-Rollups: paving the way for new blockchain applications

Thomas Lavaur

Directeurs :
Jérôme Lacan
Caroline P.C. Chanel

ISAE-SUPAERO
UT3 - Paul Sabatier

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.

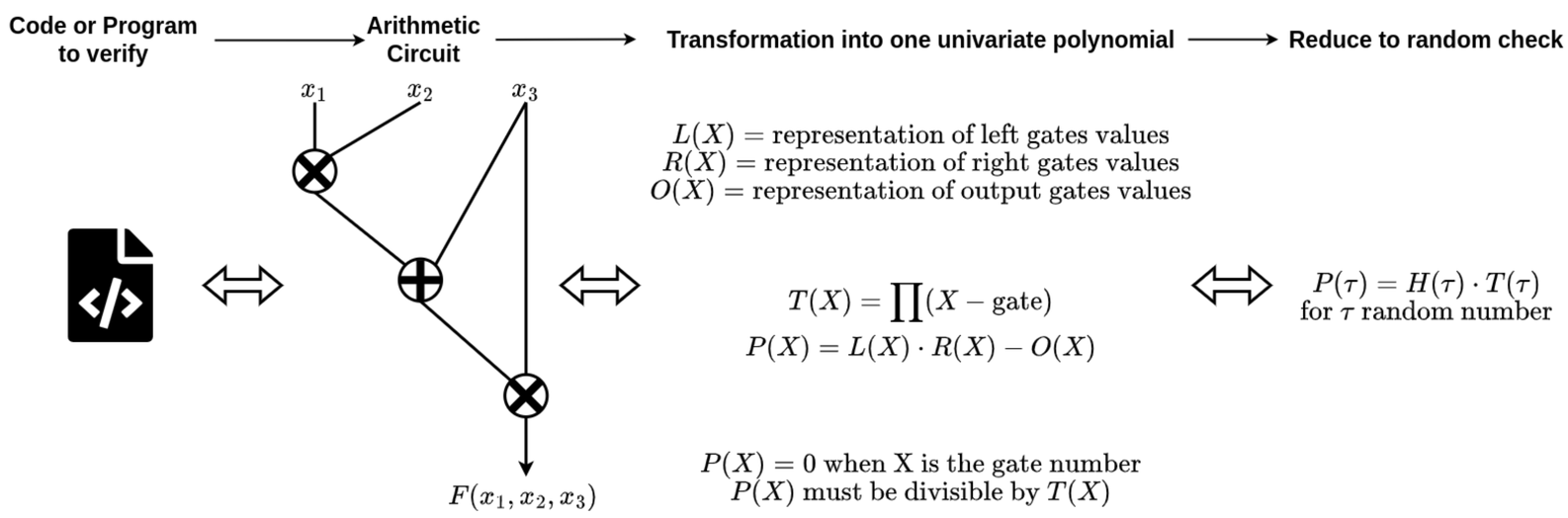
ZKP Background

- **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**.

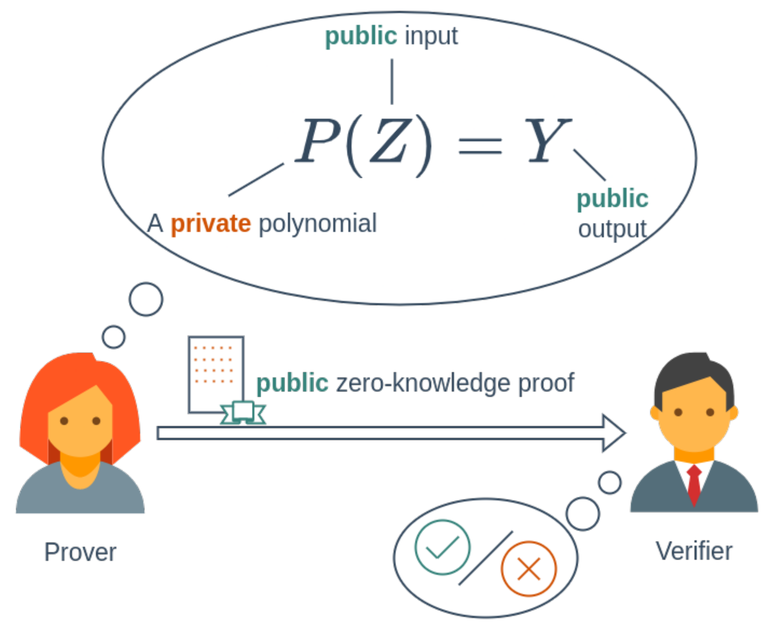
Verifiable Computation: How it works

1. Transform a program into a polynomial equation satisfiability.
2. The Schwartz-Zippel lemma succintly 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.

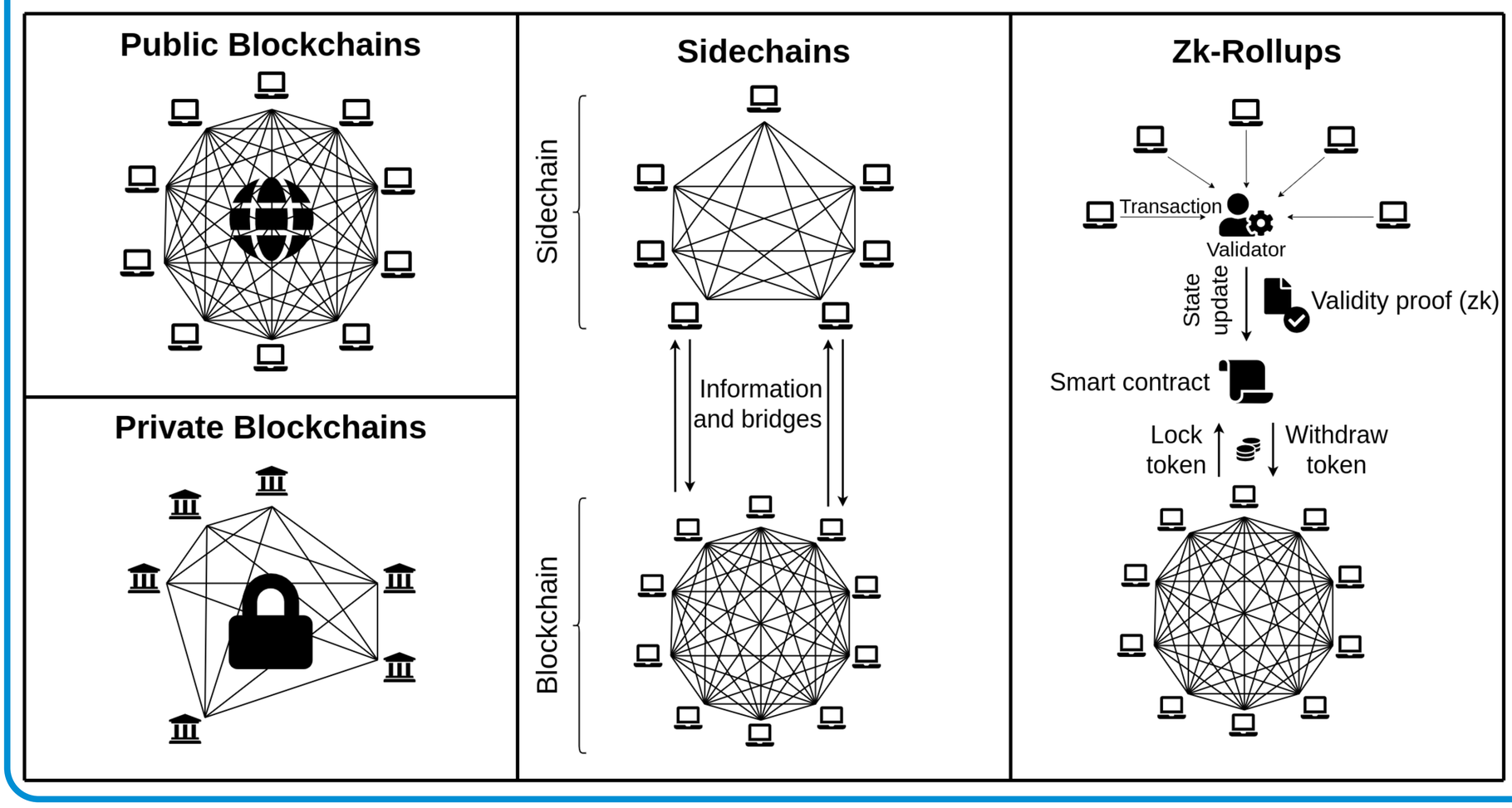
Arithmetization



Polynomial Commitment



Zk-Rollup: a high security layer 2



- A smart contract stores the funds and state of the zk-rollup accounts.
- Transaction execution is centralized 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[1].
- Connect the IoT with blockchain technology using zk-rollups[2].

Perspectives

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

[1] Lavaur, T., Lacan, J. (2022). zkBeacon: Proven Randomness Beacon based on Zero-knowledge Verifiable Computation. Proceedings of the 19th International Conference on Security and Cryptography.
[2] Lavaur, T.; Lacan, J.; Chanel, C.P.C. Enabling Blockchain Services for IoE with Zk-Rollups. Sensors 2022, 22, 6493.

Université Toulouse III Paul Sabatier — Université Fédérale Toulouse Midi-Pyrénées
Université de Toulouse
ISAE Institut Supérieur de l'Aéronautique et de l'Espace SUPAERO