Post-quantum resistant bitcoin transactions

Supervisor Joaquin Garcia-Alfaro[1]
Lab/Team TSP/SAMOVAR

Over 60% of today's bitcoin transactions are quantum-vulnerable, meaning that an adversary with quantum resources can potentially steal unspent transaction outputs. A new bitcoin improvement proposal (BIP-360, `https://bip360.org`) suggests to move all those vulnerable outputs with a new transaction type, Pay to Quantum Resistant Hash (P2QRH). This would require from an additional upgrade, facing some potential challenges (e.g., key size increase, untested trapdoors, etc.).

Expected deliverables/milestones

- 1. Simple description of the problem and its rationale;
- 2. Analysis of BIP-360 limitations, both theoretical and practical;
- 3. State-of-the-art on alternatives to the topic (cf. `https://pq-bitcoin.org/`);
- 4. Implementation of a PoC to validate uncovered findings;
- 5. Paper-like manuscript reporting all the work.

[1] garcia_a@telecom-sudparis.eu