



Hack the Web3.0 : SDK3 for Web3

ZKP Tools in the Nano

Renaud Dubois

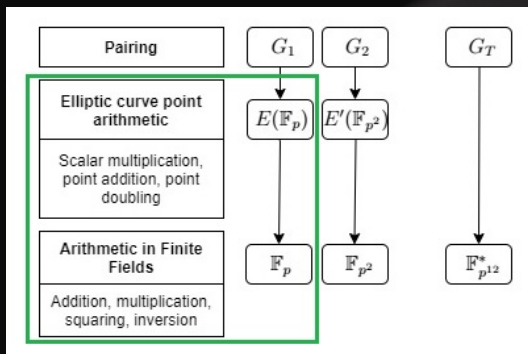
Ledger
Innovation Team

June 29, 2022



Zero Knowledge Proofs

- Zero-knowledge proof is a method by which a prover can prove to a verifier that a given statement is true while the prover.
- ZKP enable transaction hiding (Monero, ZCash) range proof, proof of membership, ZK-Rollups (Layer 2).
- Many building blocks for ZKP rely on the use of **Pairings over Elliptic curves**.



The hack

- Strip modular arithmetic from Open Source (blst library)
- Accelerate using bolos calls (available in green on figure)
- Push the result as a “Package” that external developers can use for ZKP integration on Nano.



Questions ?

