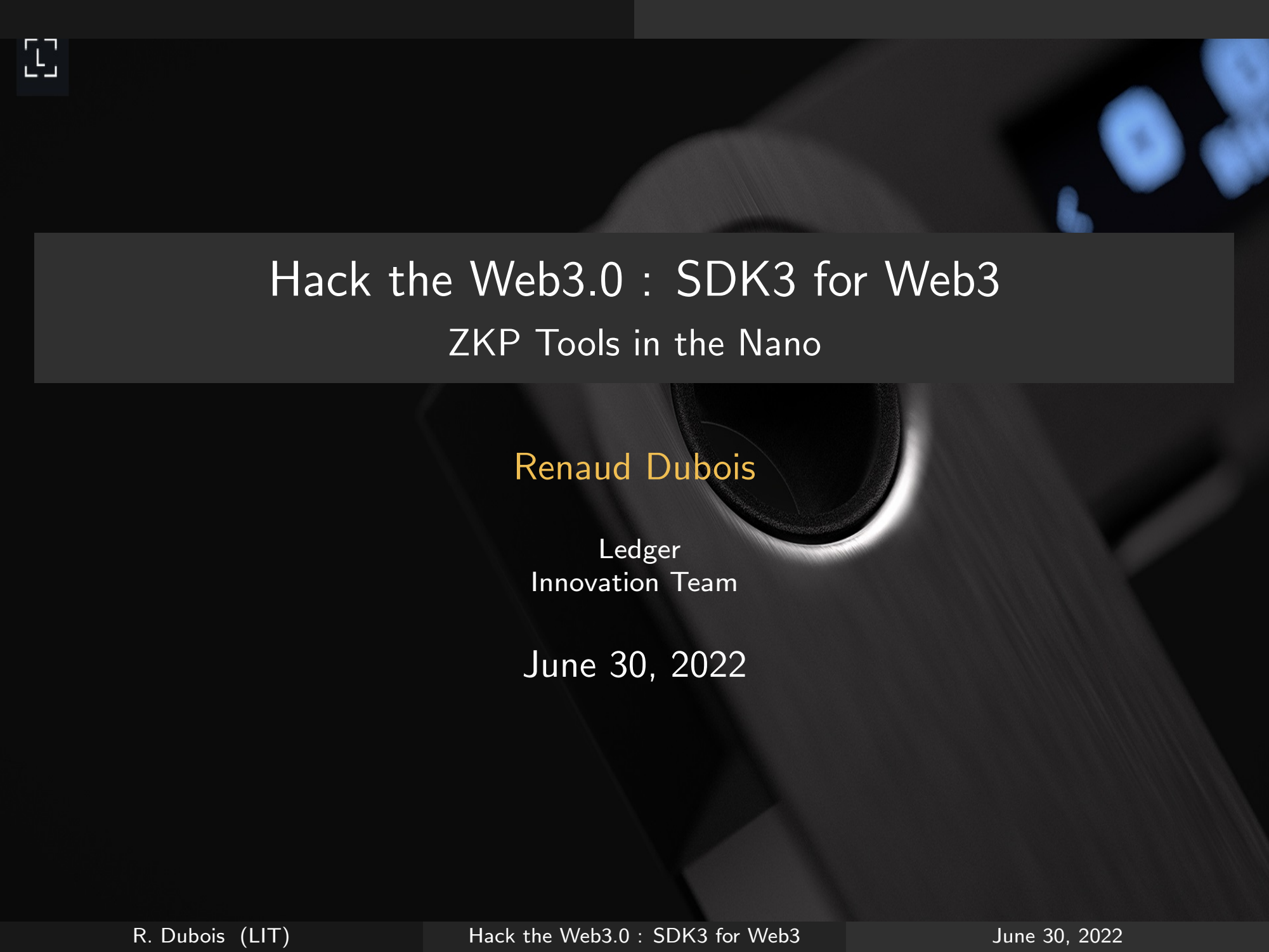


Hack the Web3.0 : SDK3 for Web3

ZKP Tools in the Nano

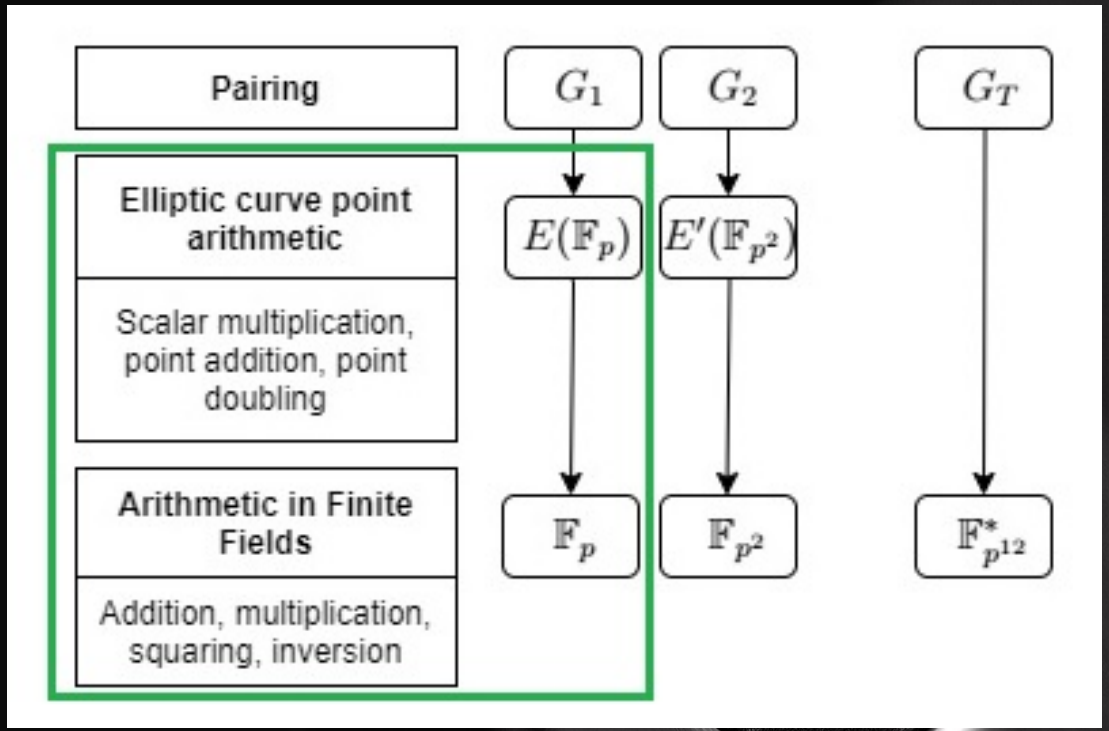
Renaud Dubois

Ledger
Innovation Team

June 30, 2022

Zero Kowledge Proofs

- Zero-knowledge proof is a method by which a prover can prove to a verifier that a given statement is true while the verifier doesn't learn information except the statement result.
- ZKP enable transaction hiding (Monero, ZCash), range proof, proof of membership, ZK-Rollups (Layer 2).
- Most of building blocks for Privacy-Preserving and ZKP rely on the use of **Pairings over Elliptic curves** (Zk-snarks, Commitments, Efficient signatures)
- Ledger direct examples : Linkable Signatures for Anonymous airdrop (**device ID**), Ring signature (**endorsement**), Strongly Verifiable SS (**Protect**), **Decentralized Identifiers**.



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 developpers can use for ZKP integration on Nano.
- Join slack #zero-knowledge

Questions ?