Kohaku Wallet: Post-Quantum Smart Accounts on Ethereum Today

Simon Masson, Renaud Dubois
ZKNox

Privacy and Compliance Summit

November 18th, 2025 – Buenos Aires, DevConnect

ZKNOX Casting

Nicolas Bacca, "Chief"
20^+ years experience (10^+y web3)
Security and hardware specialist
Prev. Ledger cofounder/CTO

Renaud Dubois, "Agent Smith"
20^+ years experience (3^+y web3)
Cryptographer
Prev. Ledger, Thales

Simon Masson, "Bizut"
8^+ years experience (4^+y web3)
Cryptographer
Prev. Heliax, Thales

ZKNOX Casting

Nicolas Bacca, "Chief"
20^+ years experience (10^+y web3)
Security and hardware specialist
Prev. Ledger cofounder/CTO

Renaud Dubois, "Agent Smith"
20^+ years experience (3^+y web3)
Cryptographer
Prev. Ledger, Thales

Simon Masson, "Bizut"
8^+ years experience (4^+y web3)
Cryptographer
Prev. Heliax, Thales

Expertise and innovation to every challenge on the whole security chain:

- user end
  (secure enclaves,
  hardware wallets),
- back end
  (TEE, HSMs),
- on-chain
  (smart contracts).

ZKNOX Casting

Nicolas Bacca, "Chief"
20^+ years experience (10^+y web3)
Security and hardware specialist
Prev. Ledger cofounder/CTO

Renaud Dubois, "Agent Smith"
20^+ years experience (3^+y web3)
Cryptographer
Prev. Ledger, Thales

Simon Masson, "Bizut"
8^+ years experience (4^+y web3)
Cryptographer
Prev. Heliax, Thales

Expertise and innovation to every challenge on the whole security chain:

- user end
  (secure enclaves,
  hardware wallets),
- back end
  (TEE, HSMs),
- on-chain
  (smart contracts).

`https://zknox.eth.limo/`

`https://github.com/zknoxhq/`

Summary

Quantum Apocalypse

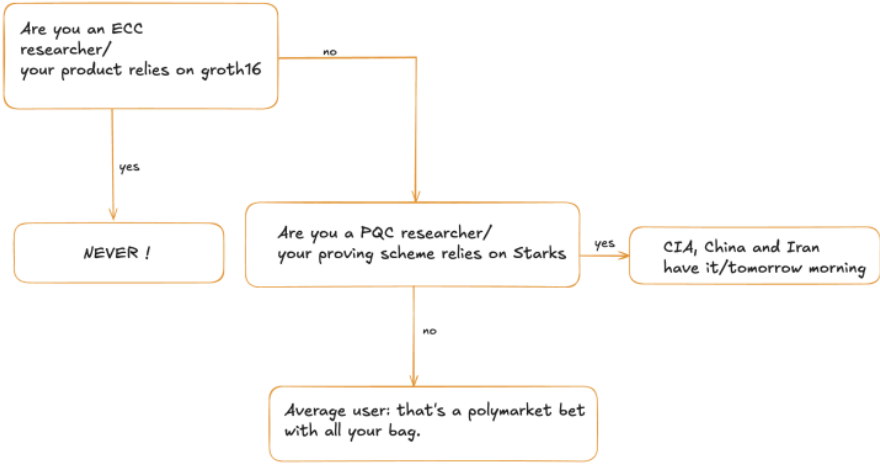
Verifiers

Quantum Apocalypse

Shor algorithm solves factorization and discrete logarithm problems. All current authentication systems are cooked as soon as Quantum computer rises.

When ?

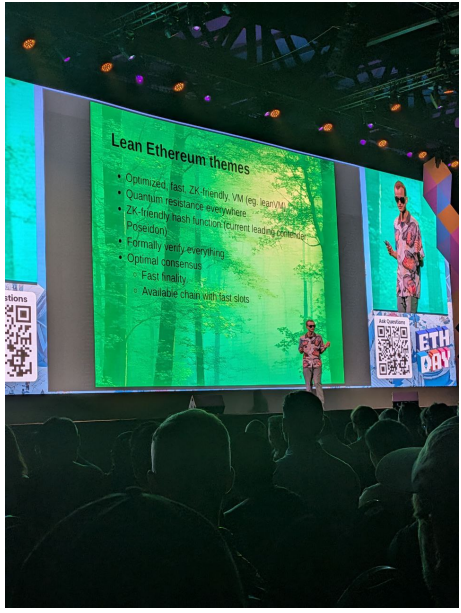
When ?


Are you an ECC researcher/ your product relies on groth16
no
yes
NEVER !
Are you a PQC researcher/ your proving scheme relies on Starks
yes
CIA, China and Iran have it/tomorrow morning
no
Average user: that's a polymarket bet with all your bag.

When ?

Federal agencies:
NIST: 2035 ANSSI/BSI: 2030
Blockchains might not care about feds, but for stablecoins regulation, those might be hard deadlines.

EF got your back



Candidates

Complexity metric	FALCON512	DILITHIUM2	SPHINCS+	GemSS
Public Key size	897	1312	32	33
Private Key size	7553	2528	32	64
Signature size	666	2420	17088	21952

Current proposals:

- FALCON: EIP8052/EIP7619
- Dilithium: EIP8051

Difference for 8052/7619: zk friendly hash (separate core from hashing to domain), 7932 specification

8051 and 8052 comes with contracts, signers, and hardware signer (8051 only). (Wait for next talk for the onchain demonstration).

Advertisement

All is delivered as public good, experiment, integrate, give feedback, hack this week end (ETHGLOBAL).

A PQ-vault, staking ETH (gas cost is high, better suited for high amount with few movements)

Remarks

- Authentication must be solved later, (but we shall on the shelf solution).
- Confidentiality shall be solved NOW.

Ethereum components at risk:

- EoA private keys (notably using ECDSA)
- Private Payments (Private Pool, RAILGUN)
- BLS signatures in consensus
- Data Availability Sampling (leveraging KZG commitments)

ZKNOX current roadmap is to solve all but last point. (Design and integrate signature schemes, not proving scheme).

Progressive Roadmap

Verifiers:

- Step1: use Account Abstraction (EIP-7702+7579/4337) with full solidity to experiment
- Step2: benchmark in nodes (validate gas hypothesis)
- Step3: EIP accepted
- remove eoA (EIP-7701/EIP-7560)

Signers:

- Step1: Software signers
- Step2: hardware signers
- remove eoA (EIP-7701/EIP-7560)