

Integration of privacy preserving primitives in hardware wallets

Simon Masson, Renaud Dubois
ZKNox



Privacy and Compliance Summit

November 19th, 2025 – Buenos Aires, DevConnect

ZKNOX team



Nicolas Bacca

20+ years experience (10+y web3)

Security and hardware specialist

Prev. Ledger cofounder/CTO



Renaud Dubois

20+ years experience (3+y web3)

Cryptographer

Prev. Ledger, Thales



Simon Masson

8+ years experience (4+y web3)

Cryptographer

Prev. Heliax, Thales

ZKNOX team



Nicolas Bacca

20+ years experience (10+y web3)
Security and hardware specialist
Prev. Ledger cofounder/CTO



Renaud Dubois

20+ years experience (3+y web3)
Cryptographer
Prev. Ledger, Thales



Simon Masson

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 team



Nicolas Bacca

20+ years experience (10+y web3)
Security and hardware specialist
Prev. Ledger cofounder/CTO



Renaud Dubois

20+ years experience (3+y web3)
Cryptographer
Prev. Ledger, Thales



Simon Masson

8+ years experience (4+y web3)
Cryptographer
Prev. Heliax, Thales

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

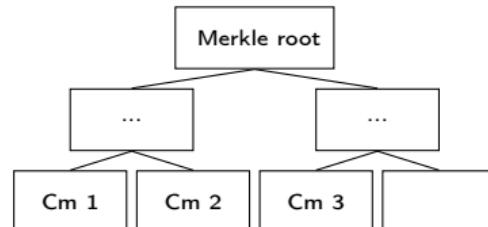
- ▶ user end
(secure enclaves,
hardware wallets),
- ▶ back end
(TEE, HSMs),
- ▶ on-chain
(smart contracts).

<https://zknox.eth.limo/>

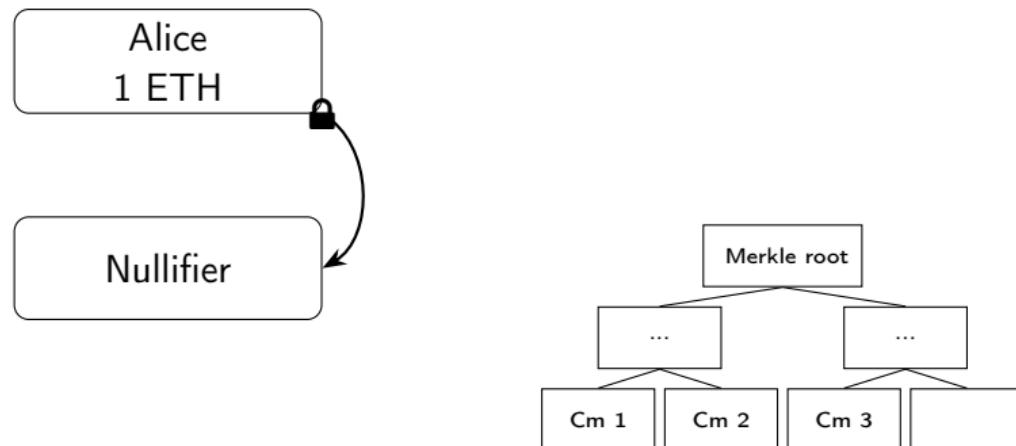
<https://github.com/zknoxhq/>

Introduction: privacy in Ethereum (Railgun)

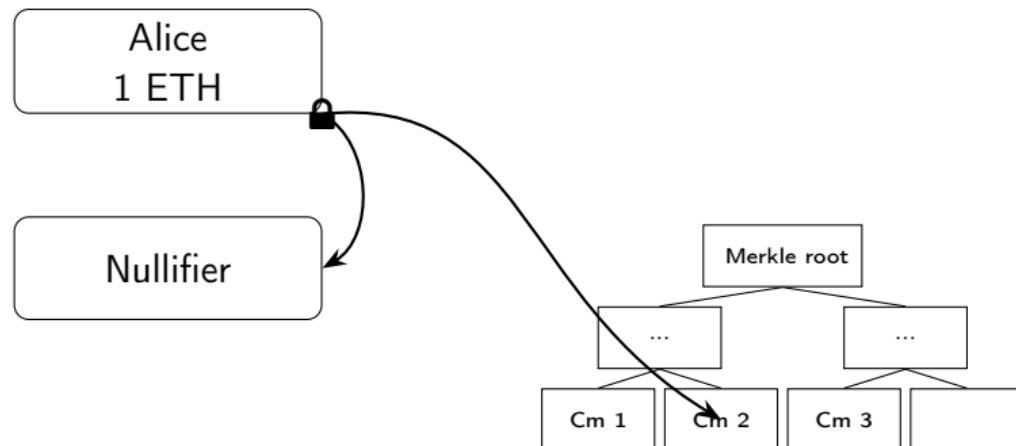
Alice
1 ETH



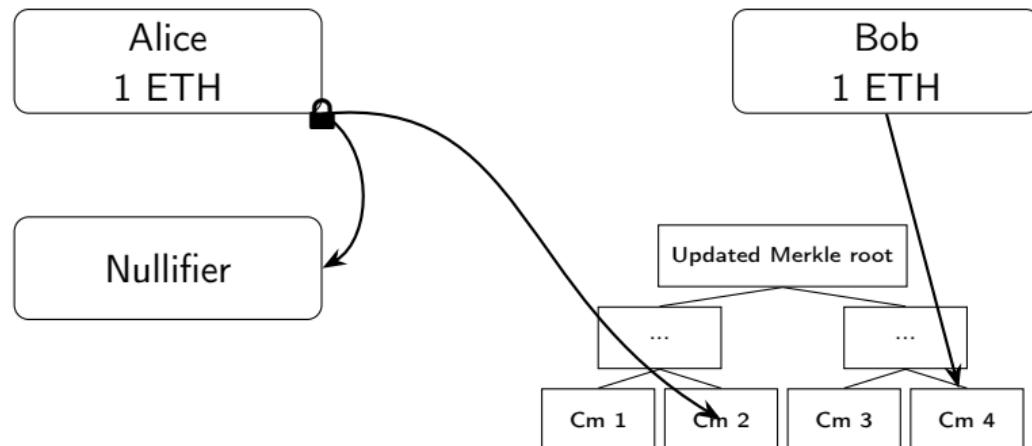
Introduction: privacy in Ethereum (Railgun)



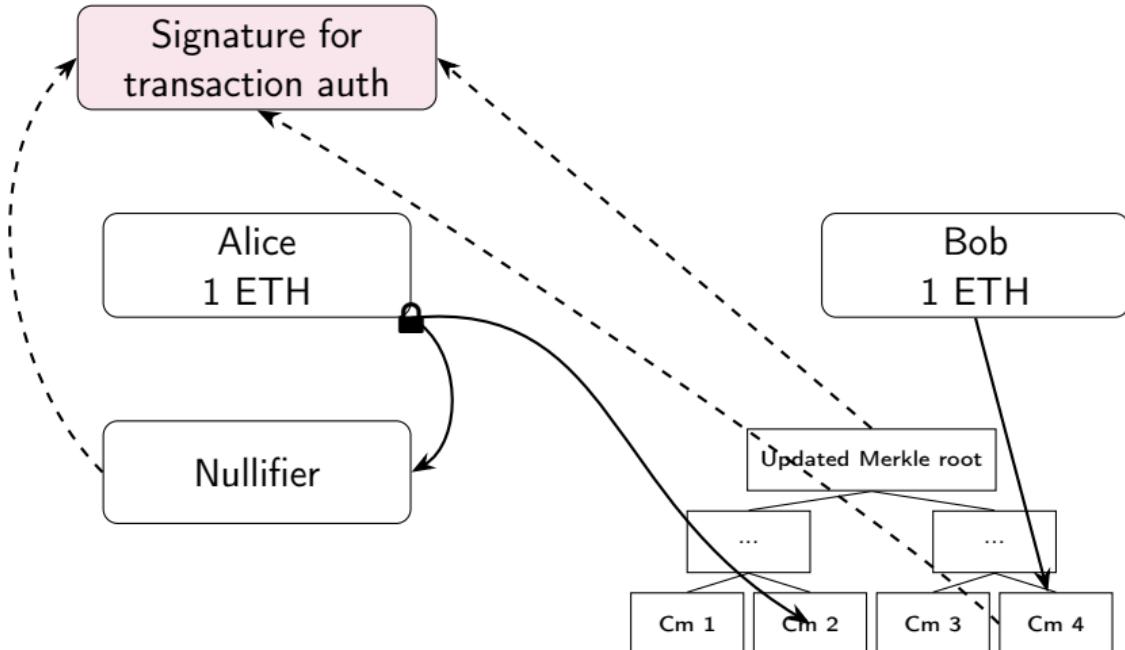
Introduction: privacy in Ethereum (Railgun)



Introduction: privacy in Ethereum (Railgun)



Introduction: privacy in Ethereum (Railgun)



Signature and hardware wallet

Computing a signature requires the *secret key*.

Signature and hardware wallet

Computing a signature requires the *secret key*.

It can be split into different signers using threshold signatures (FROST: ia.cr/2020/852)

We rather want to sign with a hardware wallet for a better security:

Signature and hardware wallet

Computing a signature requires the *secret key*.

It can be split into different signers using threshold signatures (FROST: ia.cr/2020/852)

We rather want to sign with a hardware wallet for a better security:



Signature and hardware wallet

Computing a signature requires the *secret key*.

It can be split into different signers using threshold signatures (FROST: ia.cr/2020/852)

We rather want to sign with a hardware wallet for a better security:



Signature and hardware wallet

Computing a signature requires the *secret key*.

It can be split into different signers using threshold signatures (FROST: ia.cr/2020/852)

We rather want to sign with a hardware wallet for a better security:



Signature and hardware wallet

Computing a signature requires the *secret key*.

It can be split into different signers using threshold signatures (FROST: ia.cr/2020/852)

We rather want to sign with a hardware wallet for a better security:



Issue: custom signature (BabyJubjub elliptic curve, Poseidon hash).

Signature and hardware wallet

Computing a signature requires the *secret key*.

It can be split into different signers using threshold signatures (FROST: ia.cr/2020/852)

We rather want to sign with a hardware wallet for a better security:



Issue: custom signature (BabyJubjub elliptic curve, Poseidon hash).

We implement Railgun EdDSA signer in a Ledger application.

Demonstration

Let's see how it works in practice

Integrated in Railgun



soon in



Kohaku

Conclusion and perspectives

- ✓ Hardware implementation of Poseidon hash in Ledger,

Conclusion and perspectives

- ✓ Hardware implementation of Poseidon hash in Ledger,
- ✓ Hardware implementation of EdDSA signature for BabyJubjub elliptic curve,

Conclusion and perspectives

- ✓ Hardware implementation of Poseidon hash in Ledger,
- ✓ Hardware implementation of EdDSA signature for BabyJubjub elliptic curve,
- ✓ Modular implementation for enabling Jubjub and Bandersnatch elliptic curves,

Conclusion and perspectives

- ✓ Hardware implementation of Poseidon hash in Ledger,
- ✓ Hardware implementation of EdDSA signature for BabyJubjub elliptic curve,
- ✓ Modular implementation for enabling Jubjub and Bandersnatch elliptic curves,
- ✓ FROST integration with Railgun developers (see later this week),

Conclusion and perspectives

- ✓ Hardware implementation of Poseidon hash in Ledger,
- ✓ Hardware implementation of EdDSA signature for BabyJubjub elliptic curve,
- ✓ Modular implementation for enabling Jubjub and Bandersnatch elliptic curves,
- ✓ FROST integration with Railgun developers (see later this week),
- Optimized scalar multiplication for specific curves,

Conclusion and perspectives

- ✓ Hardware implementation of Poseidon hash in Ledger,
- ✓ Hardware implementation of EdDSA signature for BabyJubjub elliptic curve,
- ✓ Modular implementation for enabling Jubjub and Bandersnatch elliptic curves,
- ✓ FROST integration with Railgun developers (see later this week),
- Optimized scalar multiplication for specific curves,
- BIP32 compliant secret derivation,

Conclusion and perspectives

- ✓ Hardware implementation of Poseidon hash in Ledger,
- ✓ Hardware implementation of EdDSA signature for BabyJubjub elliptic curve,
- ✓ Modular implementation for enabling Jubjub and Bandersnatch elliptic curves,
- ✓ FROST integration with Railgun developers (see later this week),
- Optimized scalar multiplication for specific curves,
- BIP32 compliant secret derivation,
- Integration into Kohaku wallet.

Conclusion and perspectives

- ✓ Hardware implementation of Poseidon hash in Ledger,
- ✓ Hardware implementation of EdDSA signature for BabyJubjub elliptic curve,
- ✓ Modular implementation for enabling Jubjub and Bandersnatch elliptic curves,
- ✓ FROST integration with Railgun developers (see later this week),
- Optimized scalar multiplication for specific curves,
- BIP32 compliant secret derivation,
- Integration into Kohaku wallet.

Thank you for your attention.