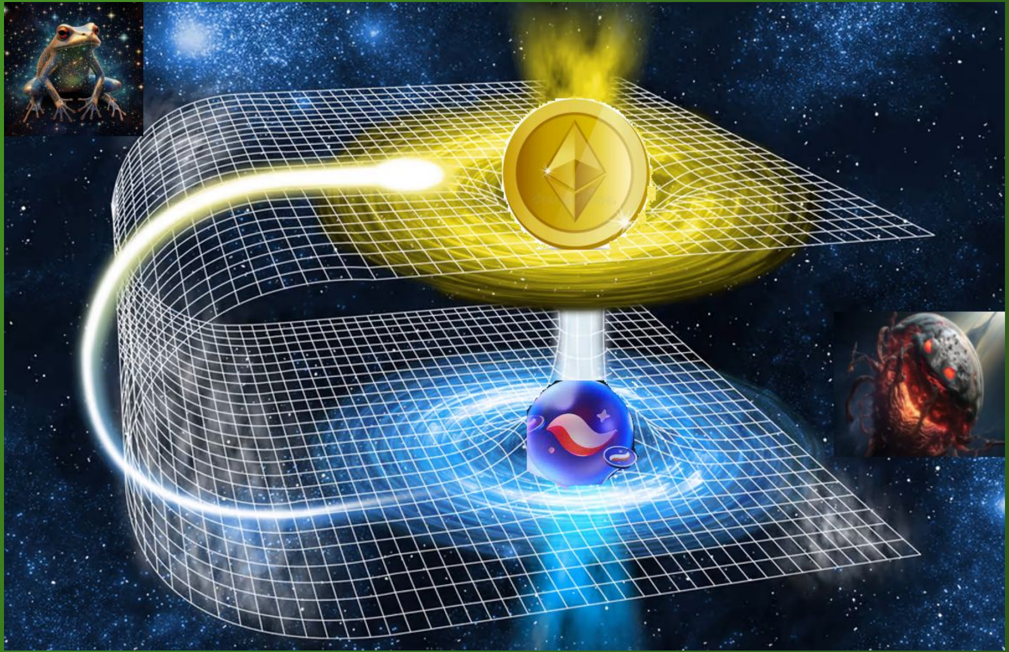
Stark, Bridge n Frogs



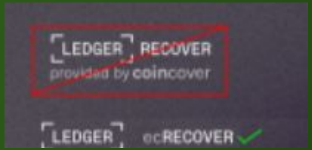
Renaud Dubois 19.10.23
(rdubois-crypto)

Froggyculum Vitae

- 15+ years as Cryptographer for Defense Industry (HSM, Radio Systems)
- 1.5 years as Cryptographer at Ledger Innovation Lab

Specialization in ECC optimizations

- FCL lib (fastest EIP7212/secp256r1 in pure solidity for 4337 UserOp)
- Self custody engaged



By the way I'm French, so according to UK slang, i'm a FROG !!

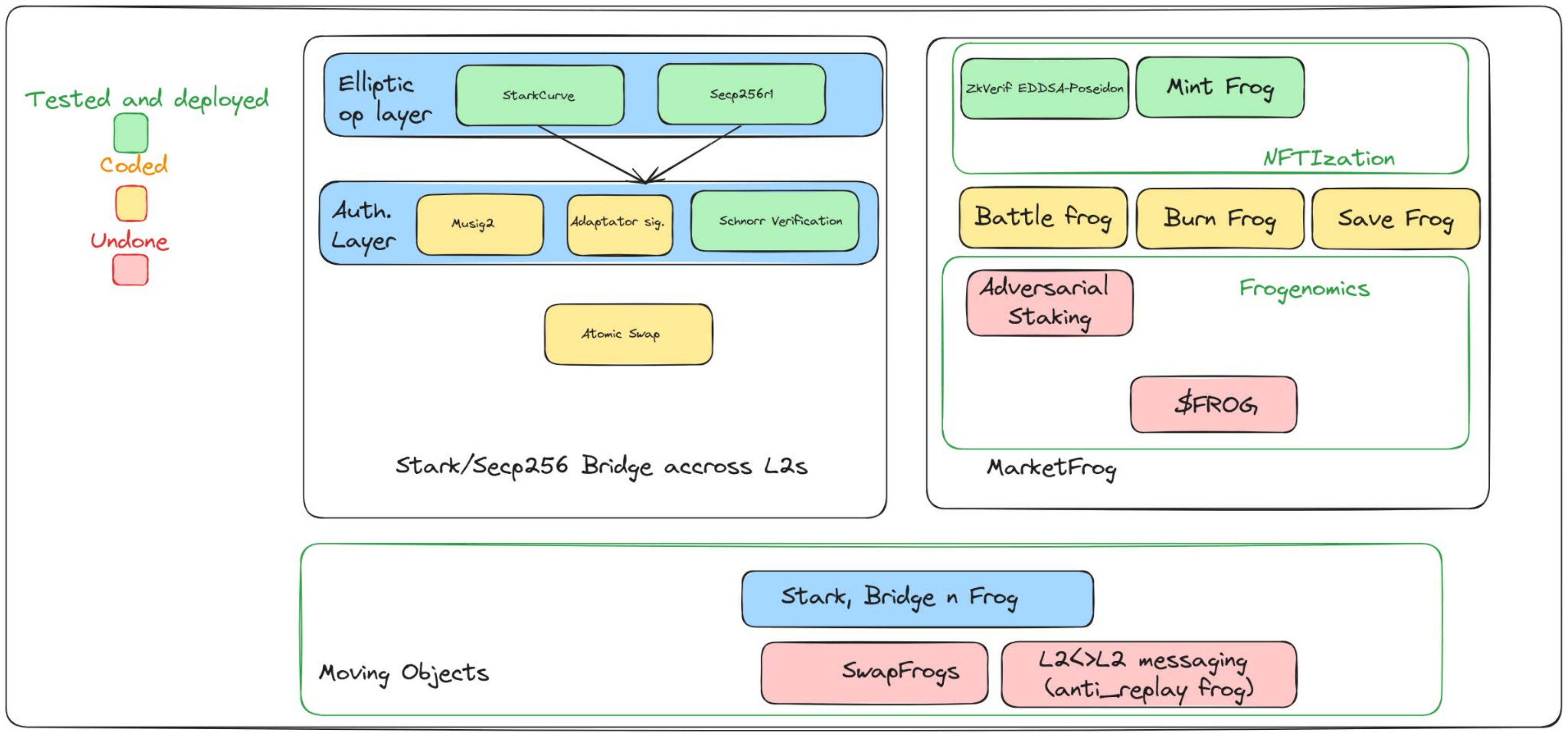
FrogMary

You have Frogs, now you want to trade their value.

We wanna burn, trade and send them across existing universes (Layer 2s)

- Permissionless Bridging : use ECC Schonrr based atomic Swaps to exchange $(CROACROA)
- Including the strange Starknet universe

FrogChitecture of the solution



4-4337

FrogTribution

StarkCurve

- Native curve of starknet + Schnorr signature deployed in many L2s
- We modified our FCL secp256r1 to implement Starkcurve in solidity
- Now we can verify ECDSA and Schnorr (Taproot/Lightning) using Starkcurve

Bridging

- Atomic Swap is a Schnorr-based mechanism to implement interchain Swapping
- StarkCurve +Schnorr + Atomic Swap = StarkBridge
- StarkBridge + MarketFrog + L2 messaging = Send Frogs across Etherverse !

MarketFrog :

How to chase 2 rabbits

FrogeNomics (1/3)

Frogs ($CROACROA) tokens are obtained by Sacrificing frogs on the Altar of Writhing Void, draining their soul to Apocalypse Frog.

We wanna trade them across existing universes (Layer 2s)

Permissionless Bridging

Including Specific Verification Function (Starknet)

FrogeNomics (2/3)

Frogs can be saved from the Void by giving offering (ETH) to GenesisFrog at the Light Altar of Celestial Pond.

Frogs saved by the Light Altar will be randomly selected.

HalleluCroa !

FrogeNomics (3/3)

$(CROACROA) and Frogs can travel through the Etherverse using the StarkBridge, paying their fee to DimensionHopper.

Battlefrogs : Adversarial Staking

There is only 80 staking ponds (one by frog) by Universe. One Frog can fight to claim the staking spot.

Travel across the universe to conquest maximum spots !

Be ranked from your number of claimed spots.

Remaining Issues

For now we don’t have L2<>L2 mechanism to avoid double mint over different chains, solution:

- Fraugd Proof mechanism: add a public signal chainID to append to semaphoreID to prevent multichain Claiming
- With L2<>L2, just check and slash

Eddsa + Poseidon solidity Verification is expensive (around 2M):

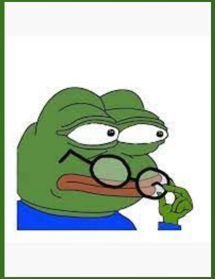
  - Would be worthy to have a dedicated optimized Babyjujub implementation (wink wink Grants)

- There is an MEV issue with the Light Altar saving mechanisms

FrogTure and Ideas

Integrate with 4337

- Stark Schnorr Signature as UserOp
- Paymaster the swaps



Add more features to the game using ZKproofs (currently only anti double spend)

Remarks

- L2<>L2 and L2<>L1 should be standardized as a RIP
- To implement Schnorr Verif with EIP7212, we need ecrecover() APIs (Vitalik’s trick, as used by Ambire and others)

Questions

*No frog were hurt during this frogckaton

Alice : $s_A' = t + r_A + H(R|P|m)p_A$

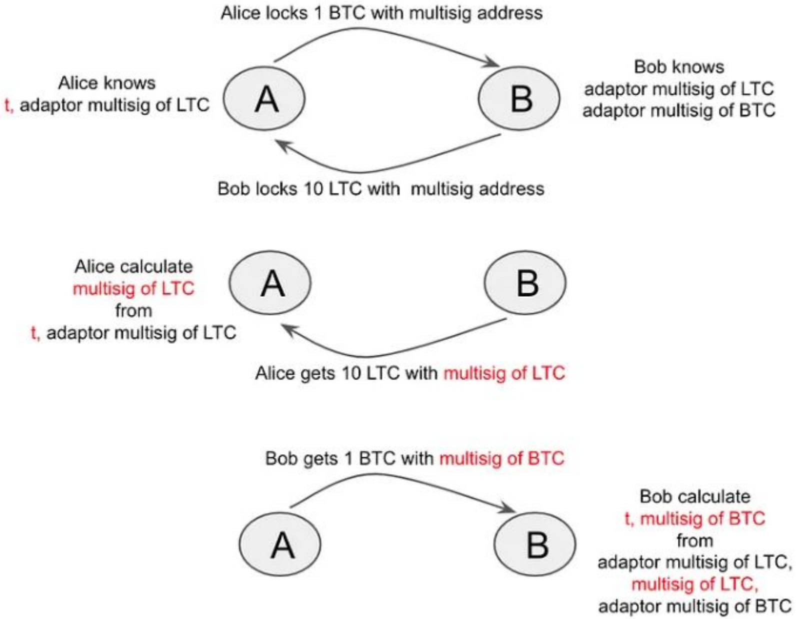
Bob : $s_B = r_B + H(R|P|m)p_B$

Alice, Bob: $s_{AB}' = s_A' + s_B = t + r_A + r_B + H(R|P|m)(p_A + p_B)$

Alice : $s_{AB} = s_{AB}' - t = r_A + r_B + H(R|P|m)(p_A + p_B)$ →Get 10LTC

Bob : $s_{AB}' - s_{AB} = t$

Subtract t from BTC Adaptor signature→ Get 1BTC



Alice locks 1 BTC with multisig address

Alice knows t, adaptor multisig of LTC

Bob knows adaptor multisig of LTC adaptor multisig of BTC

Bob locks 10 LTC with multisig address

Alice calculate multisig of LTC from t, adaptor multisig of LTC

Alice gets 10 LTC with multisig of LTC

Bob gets 1 BTC with multisig of BTC

Bob calculate t, multisig of BTC from adaptor multisig of LTC, multisig of LTC, adaptor multisig of BTC