Mercury wallet

From blind coin swaps to blinded statechains

Tom Trevethan

Why statechains

Scaling trade-offs

- On-chain bitcoin does not scale
- Lightning - fully trustless - but substantial limitations
- Custodial solutions:
    - Proof of reserves/solvency
    - Federations
    - Privacy

Why statechains

Scaling trade-offs

- Statechains - hybrid solution - *proactively* non-custodial
- *Proactively* censorship resistant
- Not private by default

Mercury statechains

Implementation

- Decrementing timelocks (nLocktime) for backup txs
- Single shared pubkey (via 2P-ECDSA)
- Multiparty key share update scheme
- Full verifiability and proof-of-publication
- Proof of theft
- Batch (atomic) transfer proofs

Mercury statechains

Coin swaps

- UTXO statechains are public
- Fixed amount UTXOs
- Coins can be swapped using a Chaumian token scheme
- Rapid off-chain transfers potentially access much larger anonymity sets
- Different on-chain and statechain anonymity sets

Blinded statechains

Challenges:

- Statecoin UTXOs not identifiable on-chain
- Statechain entity incapable of identifying UTXOs
- Fees must be collected out-of-band (i.e. not from statecoins).
- Cannot enforce proportional fees
- All verification performed client-side
- Server guarantee of key uniqueness
- Proof-of-publication?

Blinded state chains

Solutions:

- Fee payment in advance (via Lightning)
- Blind 2P-ECDSA
- Statechain entity signature count
- Receiving wallet must check all previous signed txs
- Wallets fully responsible for expired tx broadcast
- Fee amounts enable swap pool registration
- Pruning via coin expiry