the future of hardware wallets

D419 C410 1E24 5B09 0D2C 46BF 8C3D 2C48 560E 81AC

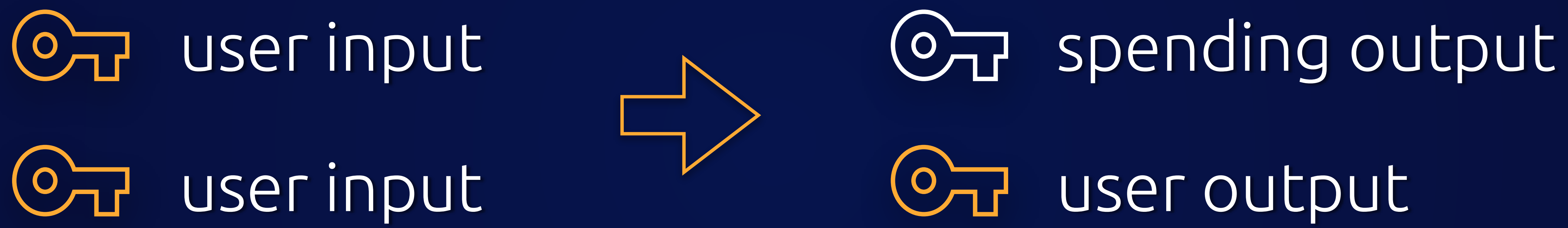
crypto
advance.

@StepanSnigirev

✉ stepan@cryptoadvance.io

hardware wallets can :

■ spend funds



user input

user input

spending output

user output

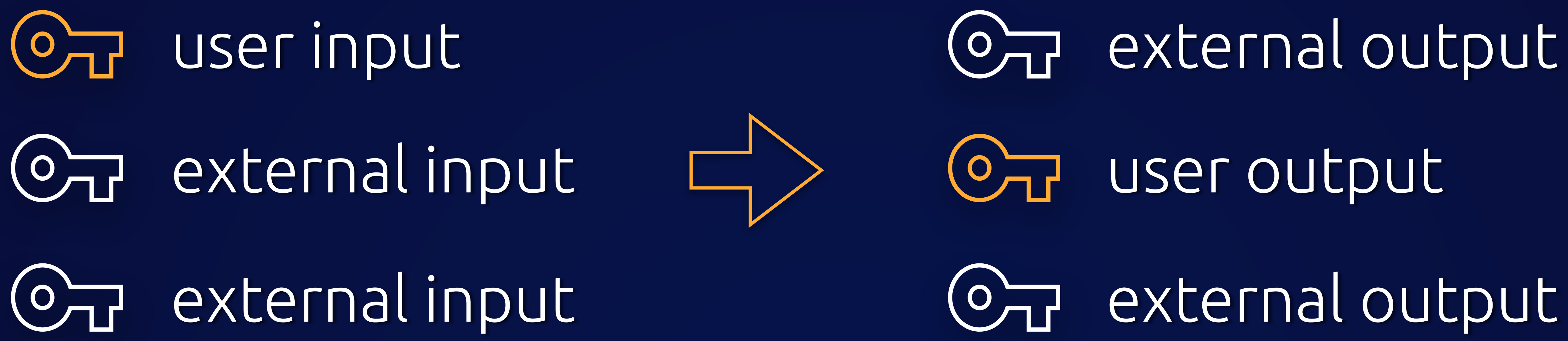
■ receive funds

□ multisig

💩 do shitcoins

hardware wallets could do :

■ CoinJoin



user input

external input

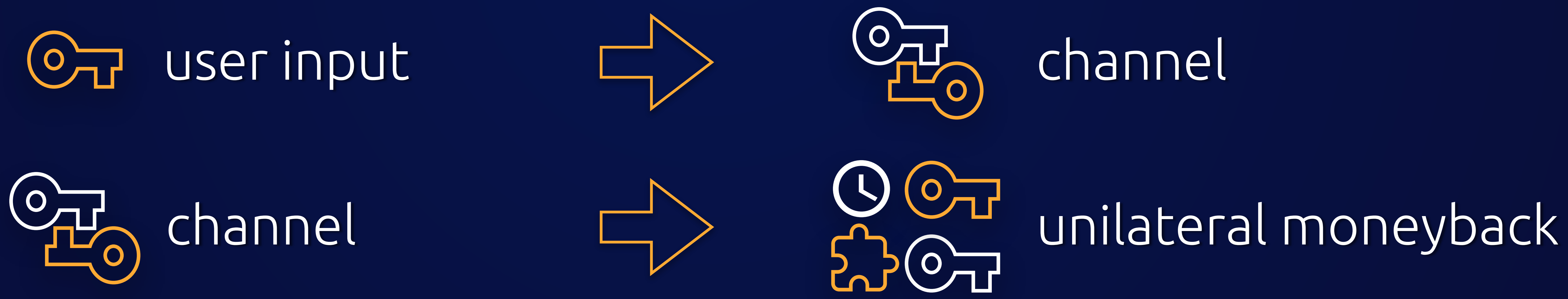
external input

external output

user output

external output

■ Lightning



user input

channel

channel

unilateral moneyback

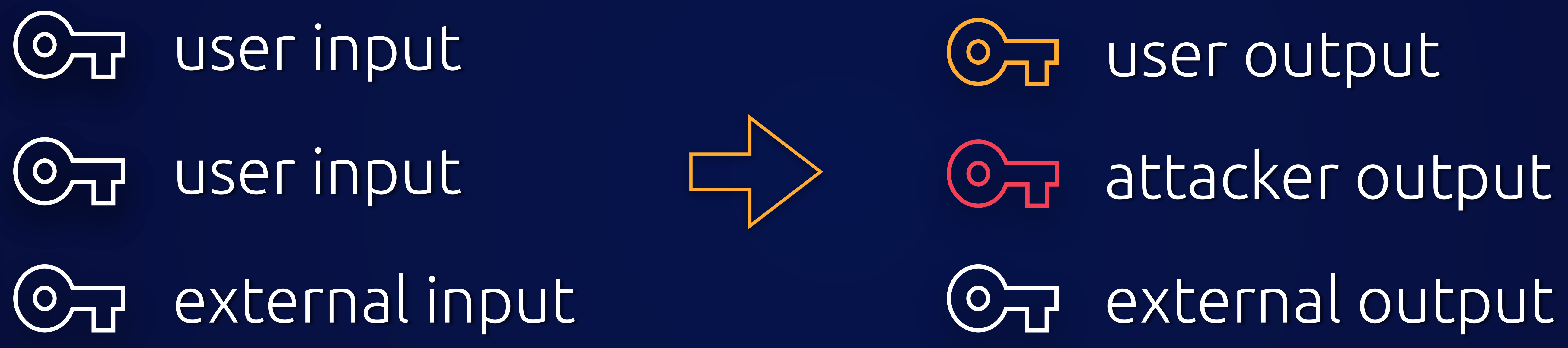
□ custom scripts

□ sidechains

Coin Join

- register inputs with CoinJoin server
- sign CoinJoin transaction
- retry if someone fails

attack with Coin Join



user input

user input

external input

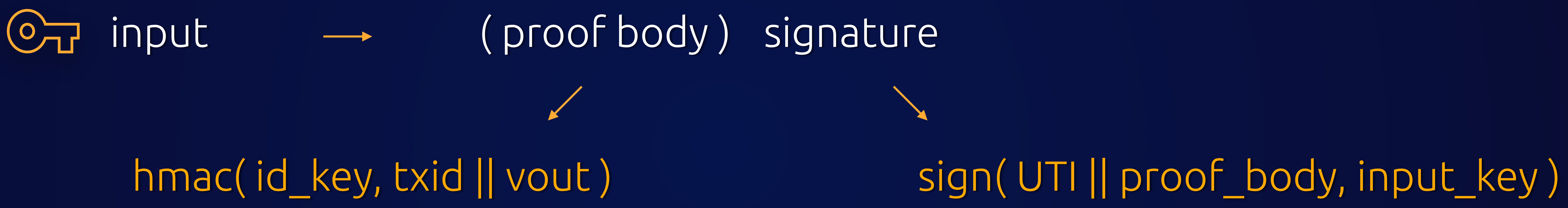
user output

attacker output

external output

proof of (not) ownership

TREZOR



input → (proof body) signature

hmac(id_key, txid || vout)

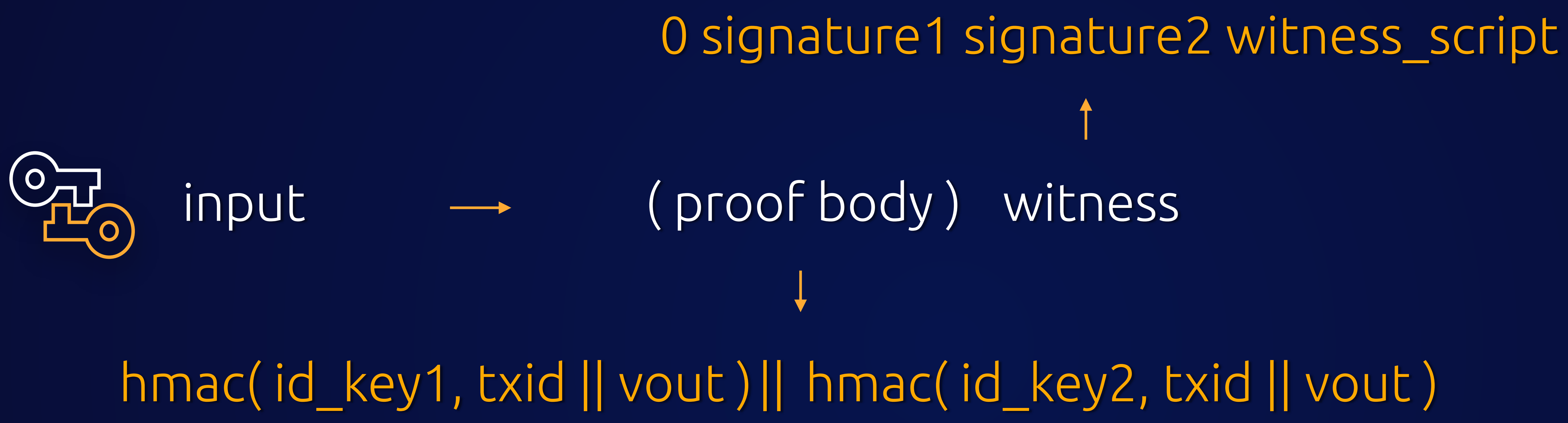
sign(UTI || proof_body, input_key)

- □ can be wallet-specific
- □ host may collect them for utxos

- □ prevents DoS on CoinJoin server
- □ only wallet can sign
- □ not replayable

https://github.com/satoshilabs/slips/blob/slips-19-20-coinjoin-proofs/slip-0019.md

beyond P2WPKH



0 signature1 signature2 witness_script

input → (proof body) witness

hmac(id_key1, txid || vout) || hmac(id_key2, txid || vout)

https://github.com/satoshilabs/slips/blob/slips-19-20-coinjoin-proofs/slip-0019.md

challenges

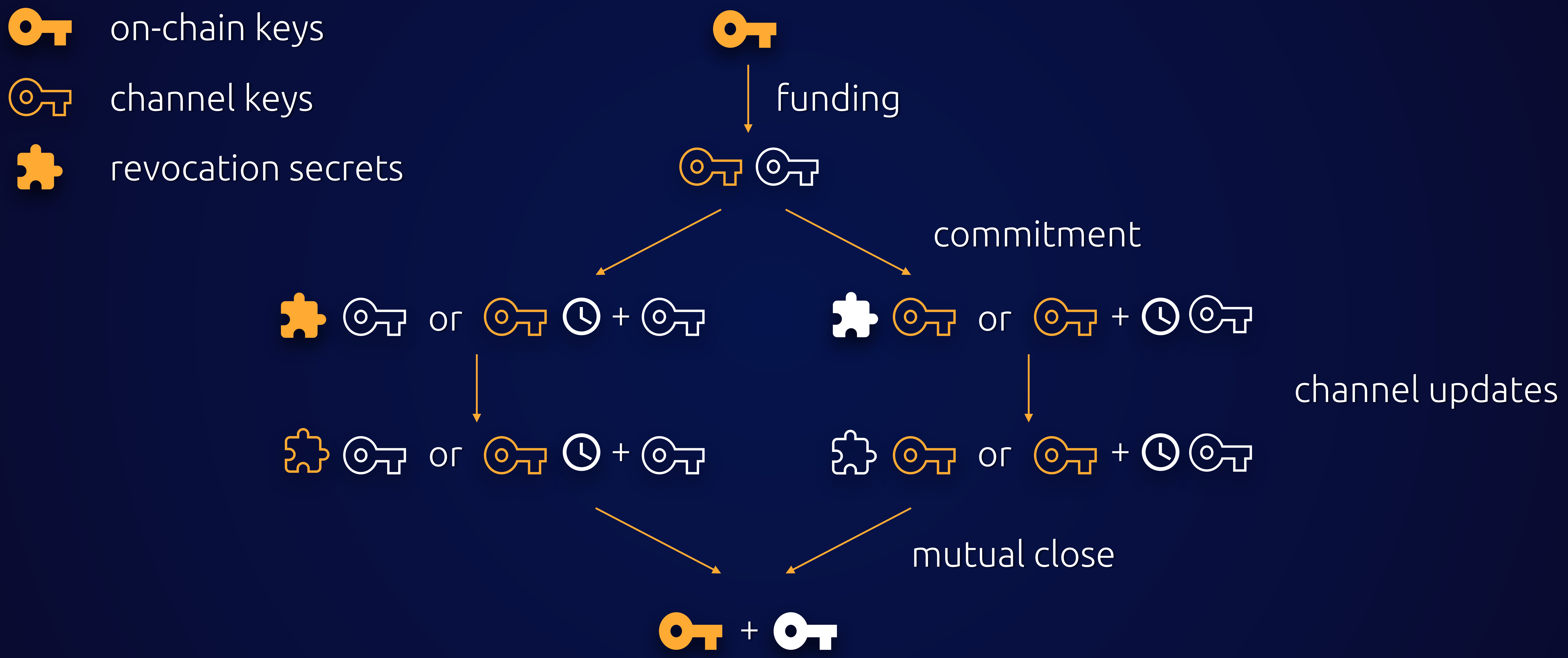
- requires script verification on HW
- needs full previous transactions for signature verification
- Schnorr and Taproot — fix-size proofs?

https://github.com/satoshilabs/slips/blob/slips-19-20-coinjoin-proofs/slip-0019.md

Lightning

- some keys need to be online
- timelocks everywhere
- monitor blockchain

secrets in Lightning



on-chain keys

channel keys

revocation secrets

funding

commitment

or

+

channel updates

mutual close

just storing secrets is not enough

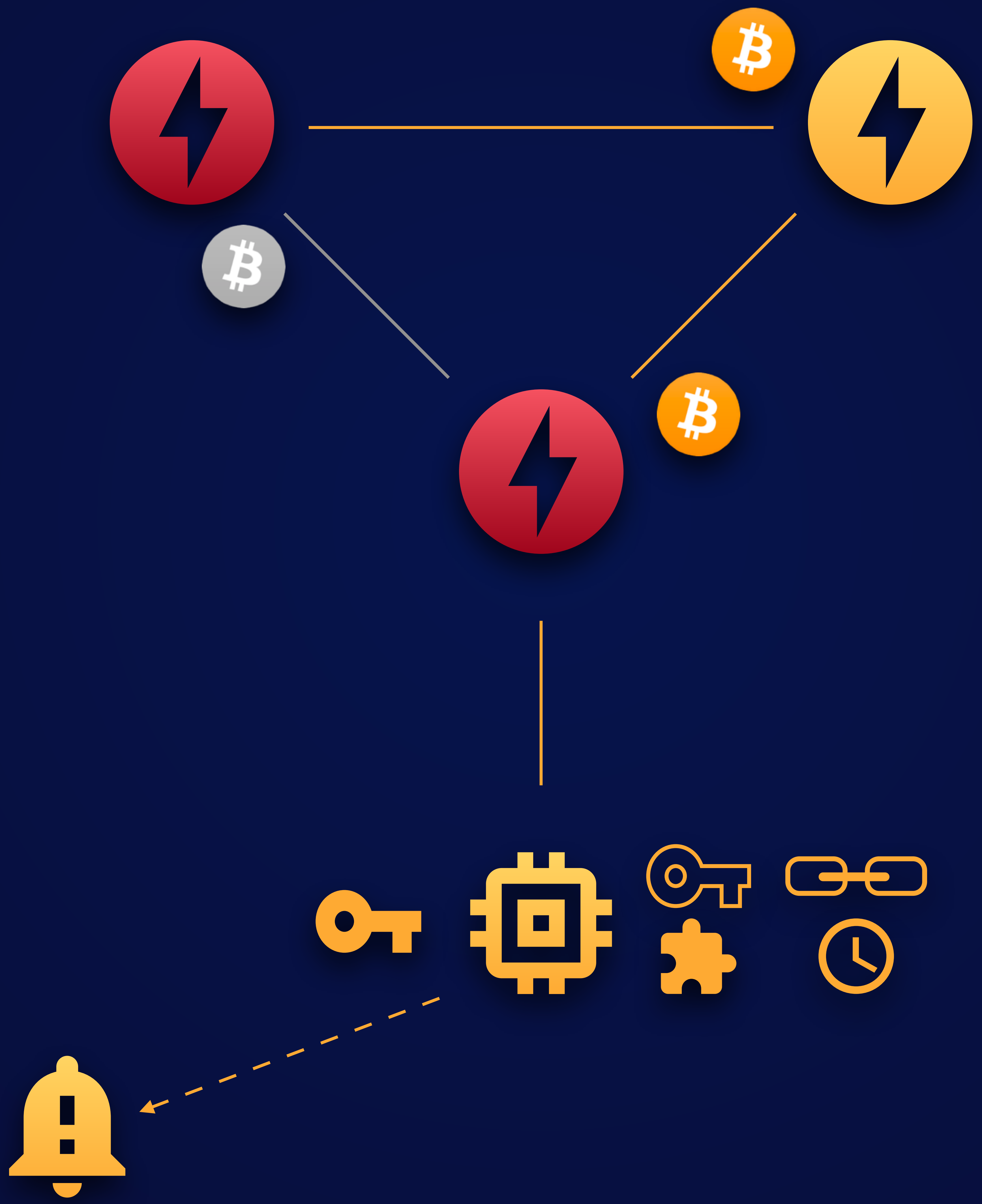
Operations:

Manual:

- Open channel
- Pay invoice

Automatic:

- Remote open
- Route payments
- Close channel



Extra functionality:

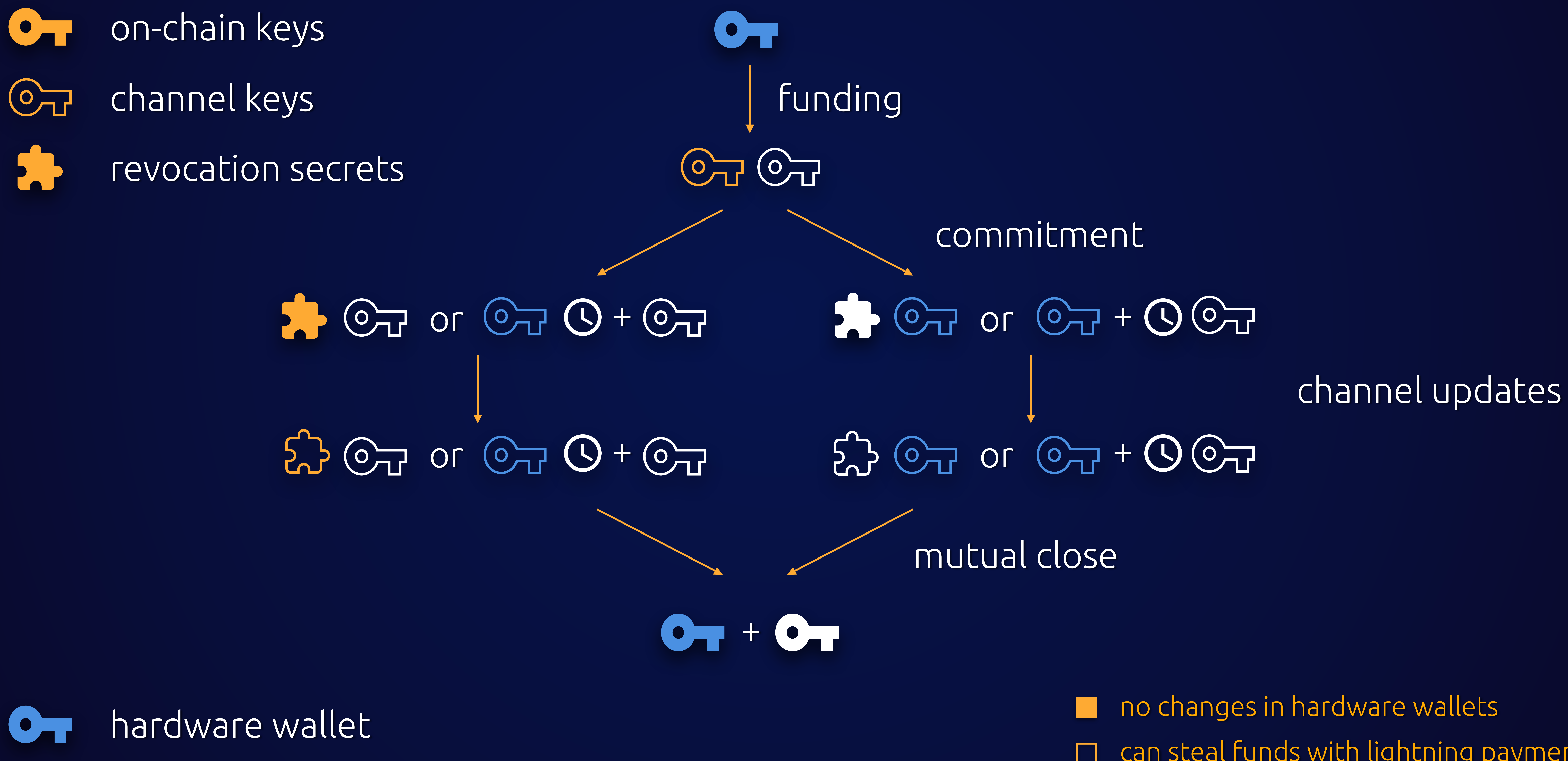
Checks:

- First commitment tx
- HTLC propagation
- Channel lock

Extensions:

- Custom derivation path
- Revocation calculation
- Storage / encrypted DB
- Blocks parsing
- Real time clock
- Backup channel

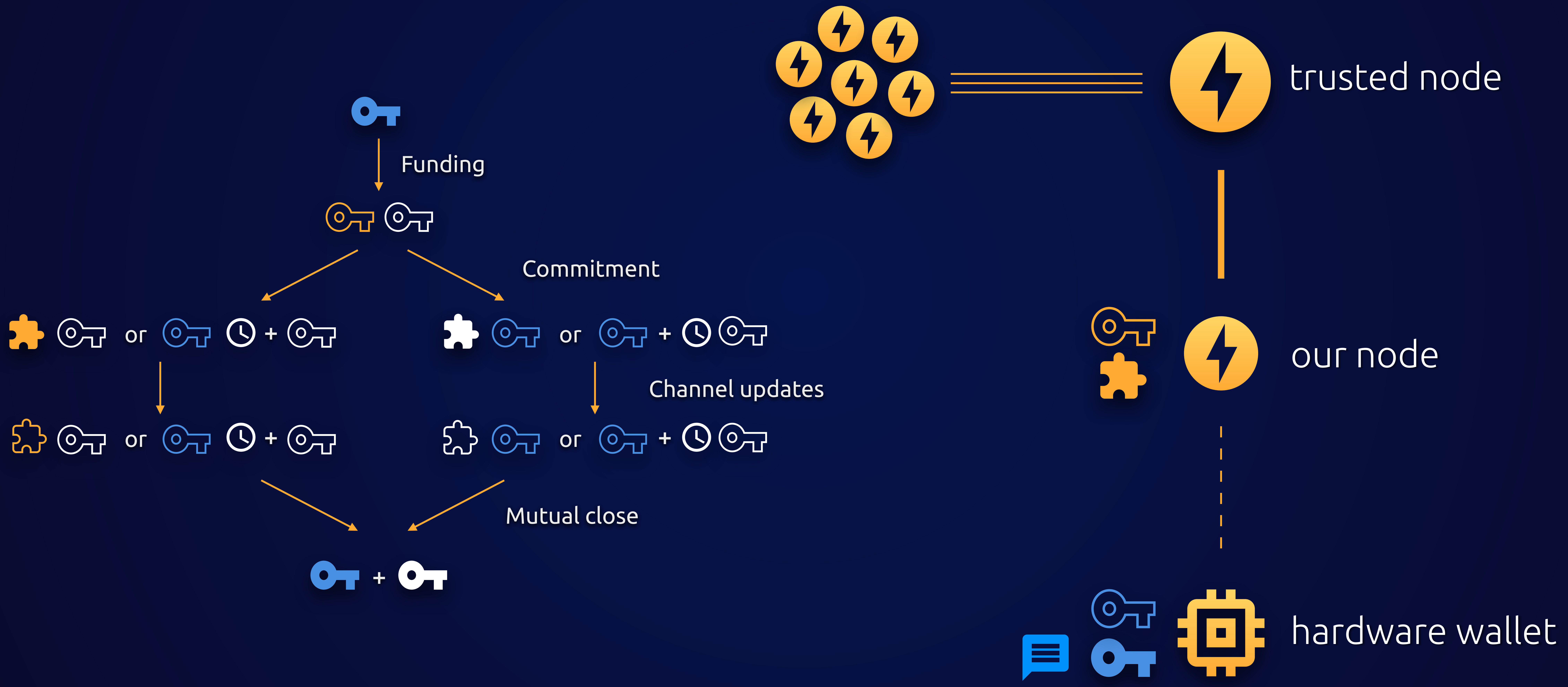
initial hardware wallet support



■ no changes in hardware wallets

□ can steal funds with lightning payments

initial hardware wallet support



thanks ,,,^_^,,,

D419 C410 1E24 5B09 0D2C 46BF 8C3D 2C48 560E 81AC

crypto
advance.

@StepanSnigirev

stepan@cryptoadvance.io

Additional attack surface

Operations:

Manual:

- Open channel
- Pay invoice

Automatic:

- Remote open
- Route payments
- Close channel

Increased attack surface:

MCU-based:

- Side channels with automatic signing

SE-based:

- Parsing transactions on the secure element

Extra functionality:

Checks:

- First commitment tx
- HTLC propagation
- Channel lock

Extensions:

- Custom derivation path
- Revocation calculation
- Storage / encrypted DB
- Blocks parsing
- Real time clock
- Backup channel