Off-chain

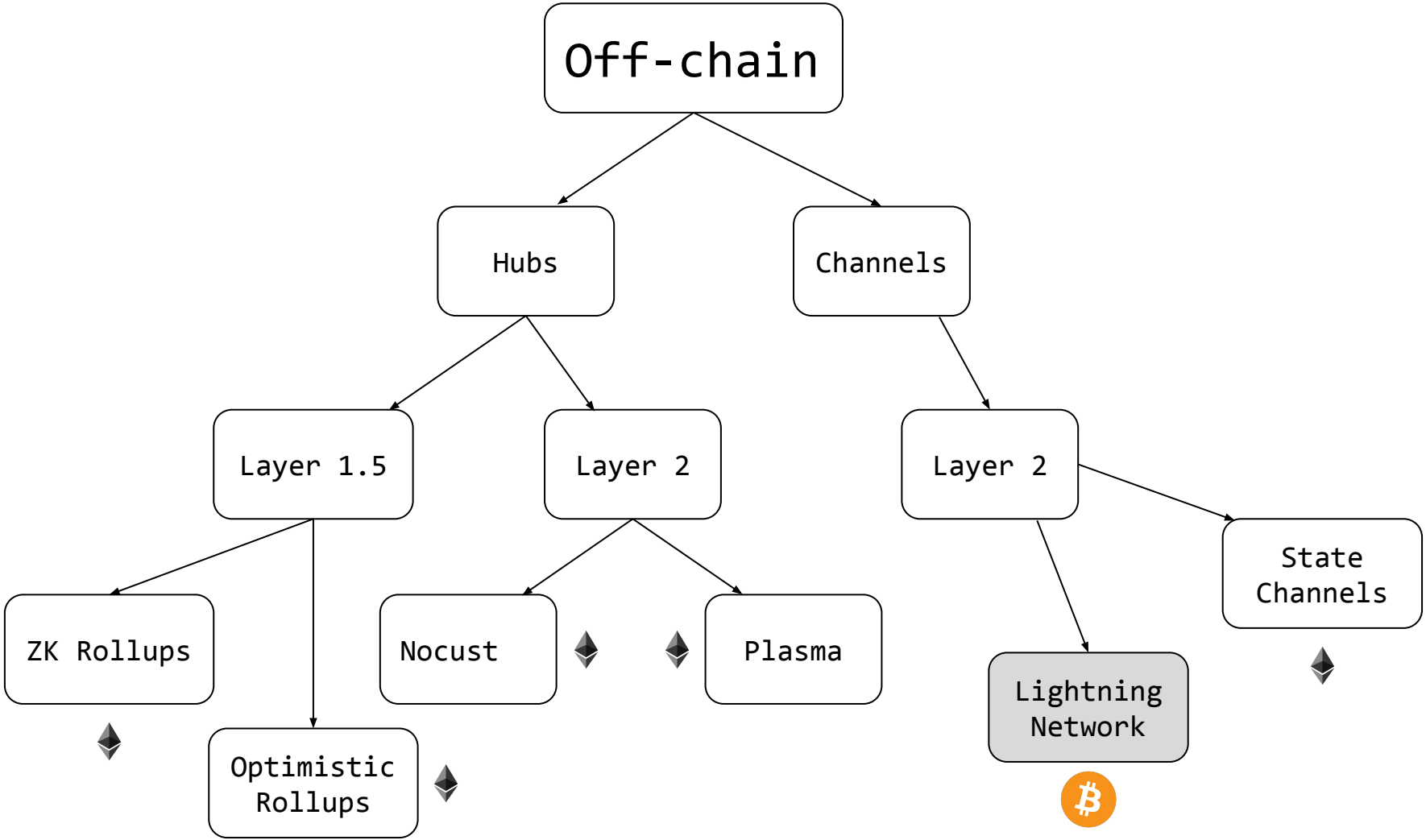
Tejaswi Nadahalli

ETH Zurich – Distributed Computing Group – www.disco.ethz.ch

Layer-1 Blockchains have low throughput

Bitcoin ~ 7 tps

Ethereum ~ 15 tps


Off-chain
Hubs
Channels
Layer 1.5
Layer 2
Layer 2
ZK Rollups
Nocust
Plasma
State Channels
Lightning Network
Optimistic Rollups

Layer-2: Payment channels

- Bitcoin - constrained smart contracts

Payment Channels (and Networks)

- Duplex Micropayment Channels (ETH contribution)
- Lightning Channels
- Eltoo Channels (ETH alumni)

Lighting Network

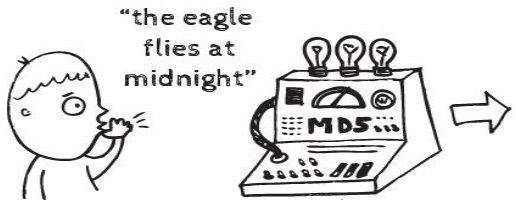
~3000 nodes, ~30000 channels, ~843 BTC

Lighting Network in Production

- BOLT - a specification for the Lightning Network (https://github.com/lightningnetwork/lightning-rfc)
- Implementations
  - LND (golang)
  - C-Lightning (C)
  - Eclair (Scala)

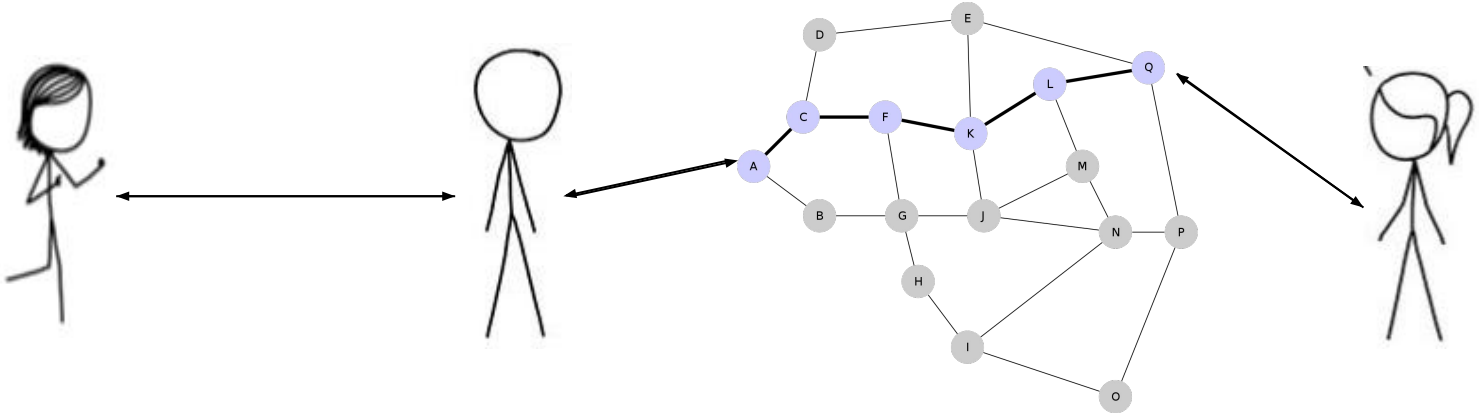
Bitcoin Primitives

- UTXO - Unspent Transaction Output
- Cryptographic Hash Function
- Timelocks



Hashed Timelocked Contracts

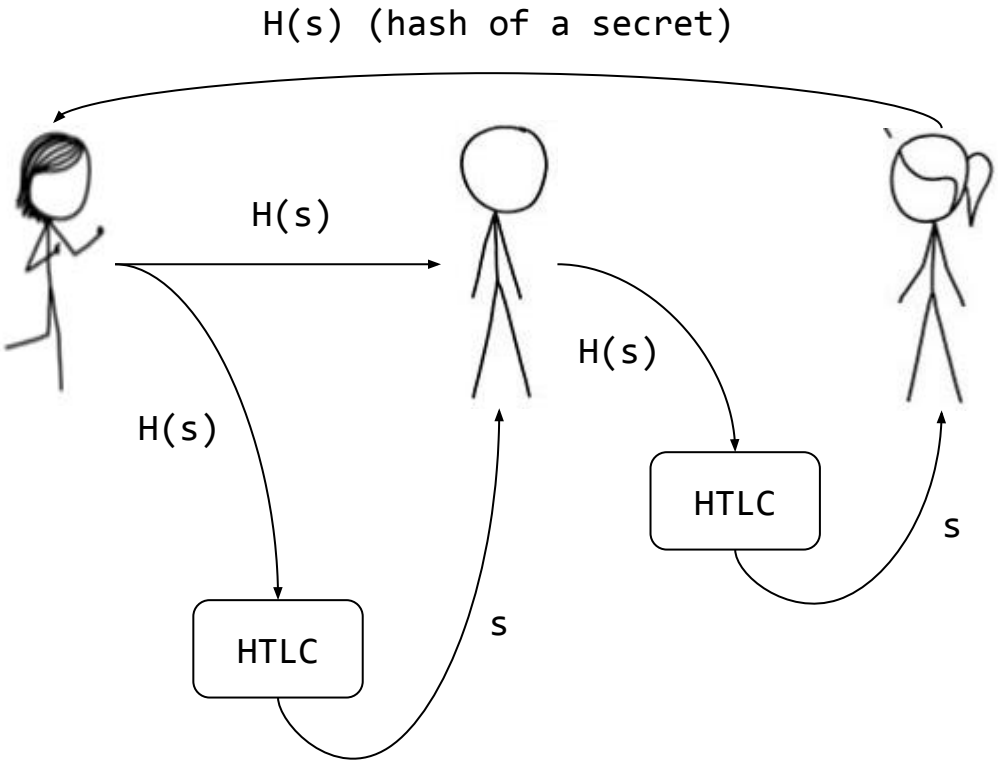
Alice ⇒ Carol



- Alice open a channel to any other node, say Bob.
- Carol gives Alice an invoice
- Alice pays Carol through Bob and the Network

stick figures: XKCD

Chained Payments



stick figures: XKCD

Lightning Channels

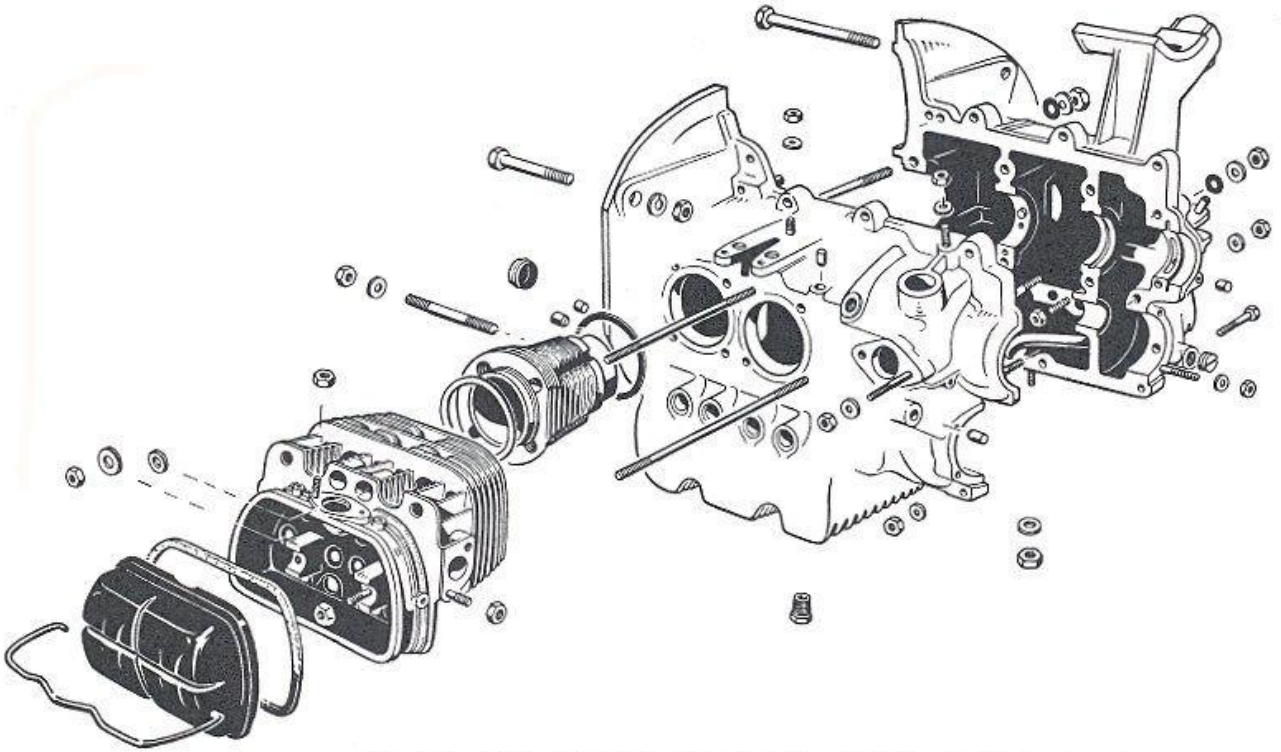


Fig. K-1. Each cylinder head serves two individual cylinder barrels, and crankcase is split in two vertically.

Lightning Channels

Bitcoin Transactions - 0100000000111744.....b0488ac00000000

- Opening/Funding Transaction
- Commitment Transaction(s)
- Bilateral Closure
- Delivery
- Revocable Delivery
- Breach Remedy

Lightning Channels (the good)

- (Once) Opening/Funding Transaction ($$$$)
- (Many) Commitment Transaction(s) ($)
- (Once) Bilateral Closure ($$$$)
- ~~Delivery~~
- ~~Revocable Delivery~~
- ~~Breach Remedy~~

Lightning Channels (the bad)

- (Once) Opening/Funding Transaction ($$$$)
- (Many) Commitment Transaction(s) + Unilateral Closure

($) ($$$$)

- ~~Bilateral Closure~~
- (Once) Delivery ($$$$)
- (Once) Revocable Delivery ($$$$)
- ~~Breach Remedy~~

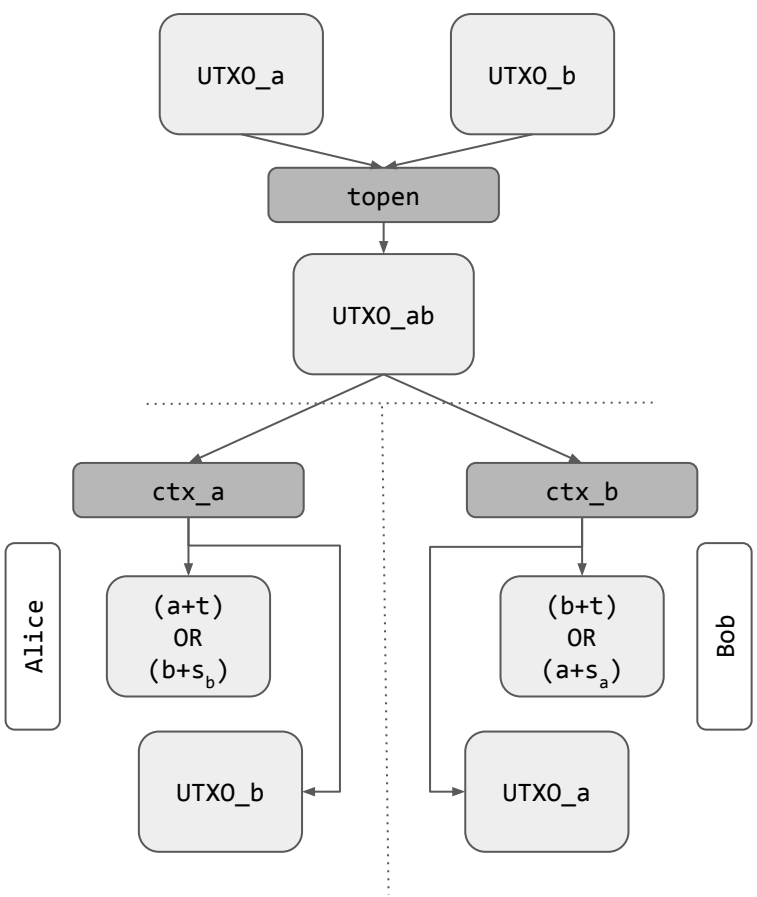
Lightning Channels (the ugly)

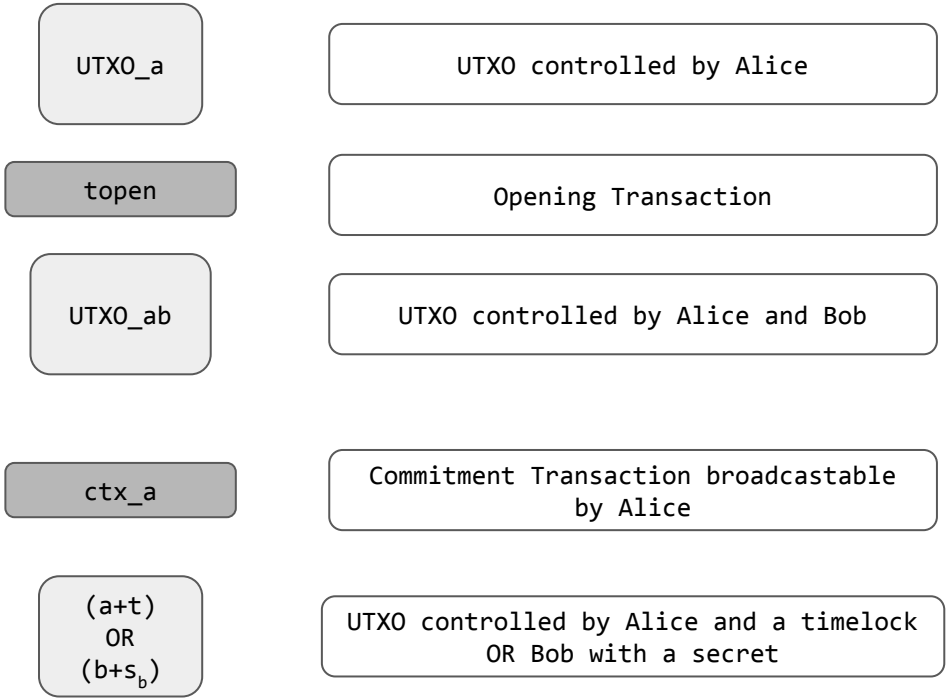
- (Once) Opening/Funding Transaction
- (Many) Commitment Transaction(s) + Cheating transaction

($) ($$$$)

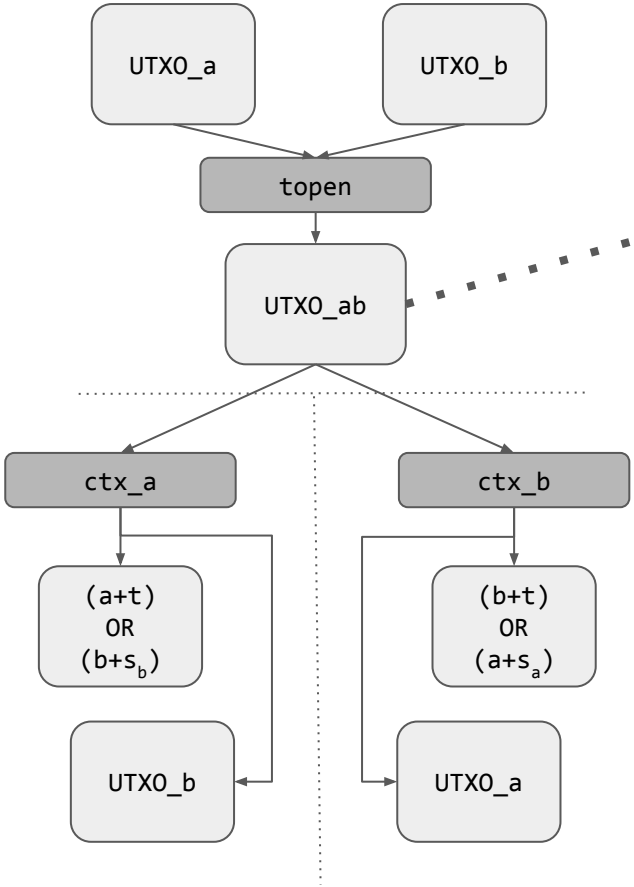
- ~~Bilateral Closure~~
- (Once) Delivery ($$$$)
- ~~Revocable Delivery~~
- (Once) Breach Remedy ($$$$)

Lightning Channel

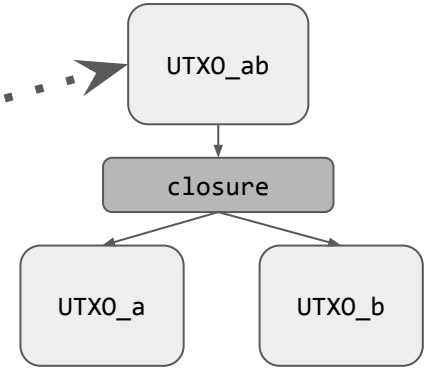




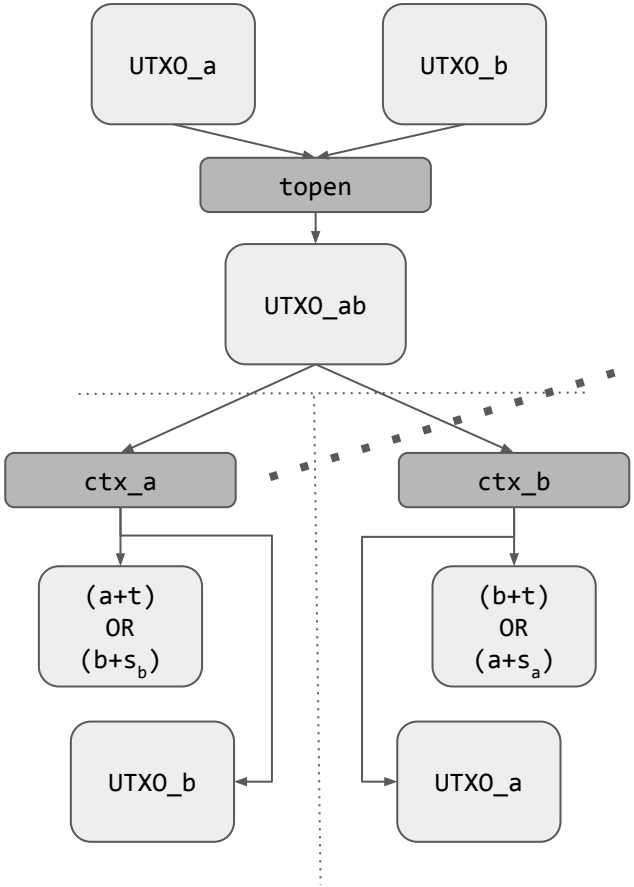
Lightning Channel



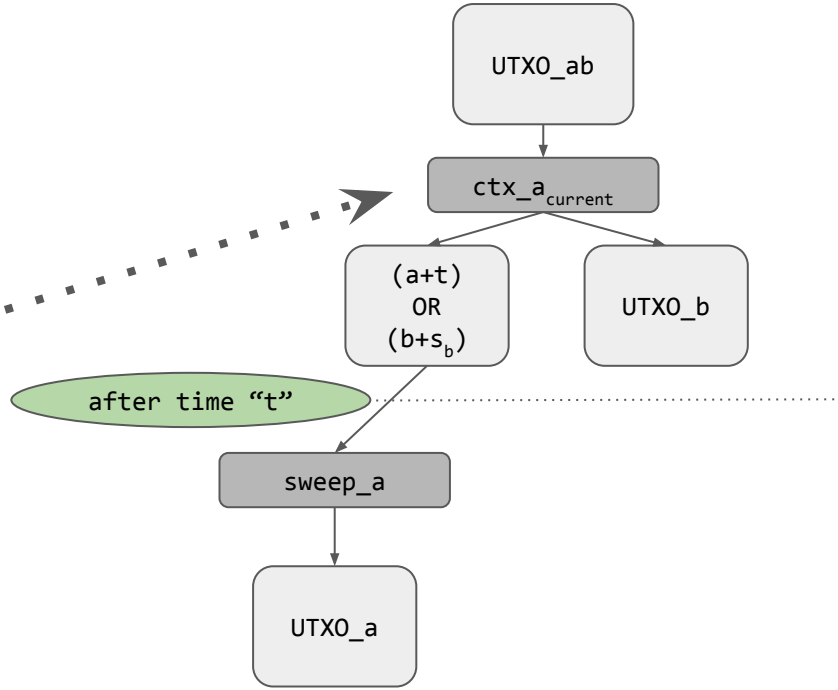
Bilateral Closure



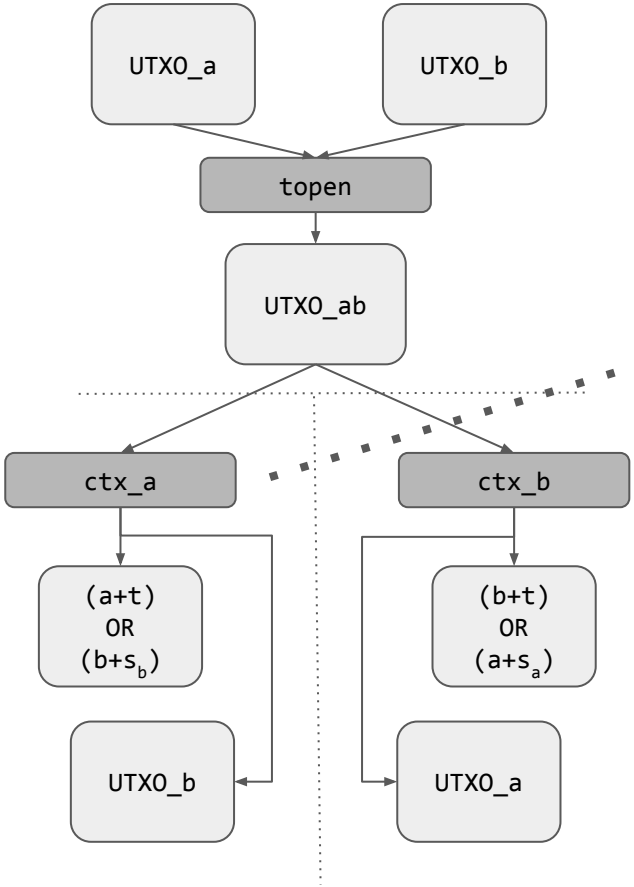
Lightning Channel



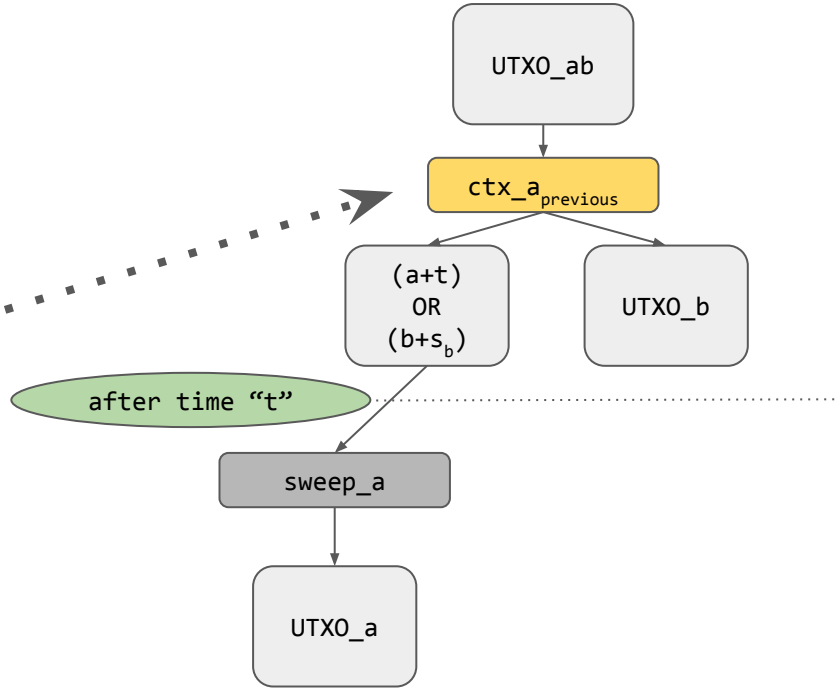
Unilateral Closure



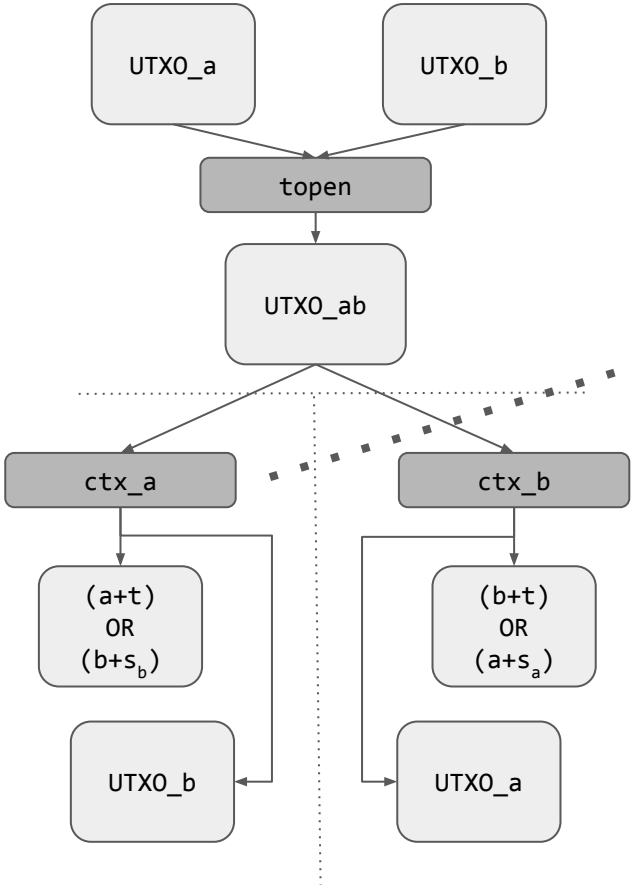
Lightning Channel



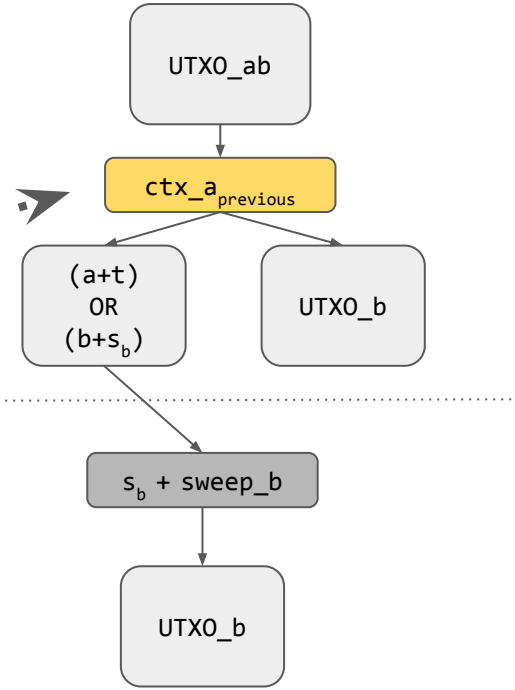
Cheating Closure



Lightning Channel



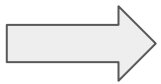
Justice Transaction



Code

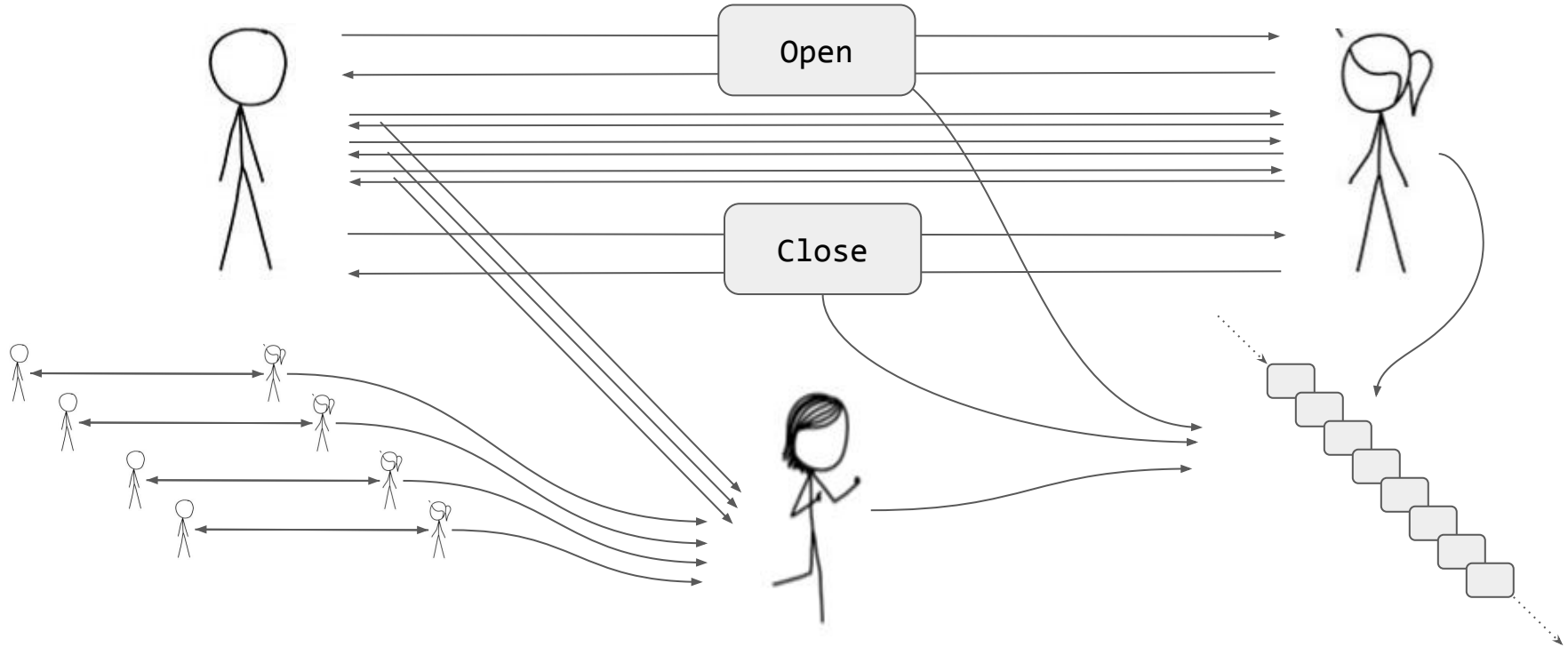
```
# To remote node with revocation key
OP_DUP OP_HASH160 <RIPEMD160(SHA256(revocationpubkey))> OP_EQUAL
OP_IF
    OP_CHECKSIG
OP_ELSE
    <remote_htlcpubkey> OP_SWAP OP_SIZE 32 OP_EQUAL
    OP_NOTIF
        # To local node via HTLC-timeout transaction (timelocked).
        OP_DROP 2 OP_SWAP <local_htlcpubkey> 2 OP_CHECKMULTISIG
    OP_ELSE
        # To remote node with secret.
        OP_HASH160 <RIPEMD160(payment_hash)> OP_EQUALVERIFY
        OP_CHECKSIG
    OP_ENDIF
OP_ENDIF
```

Offline...



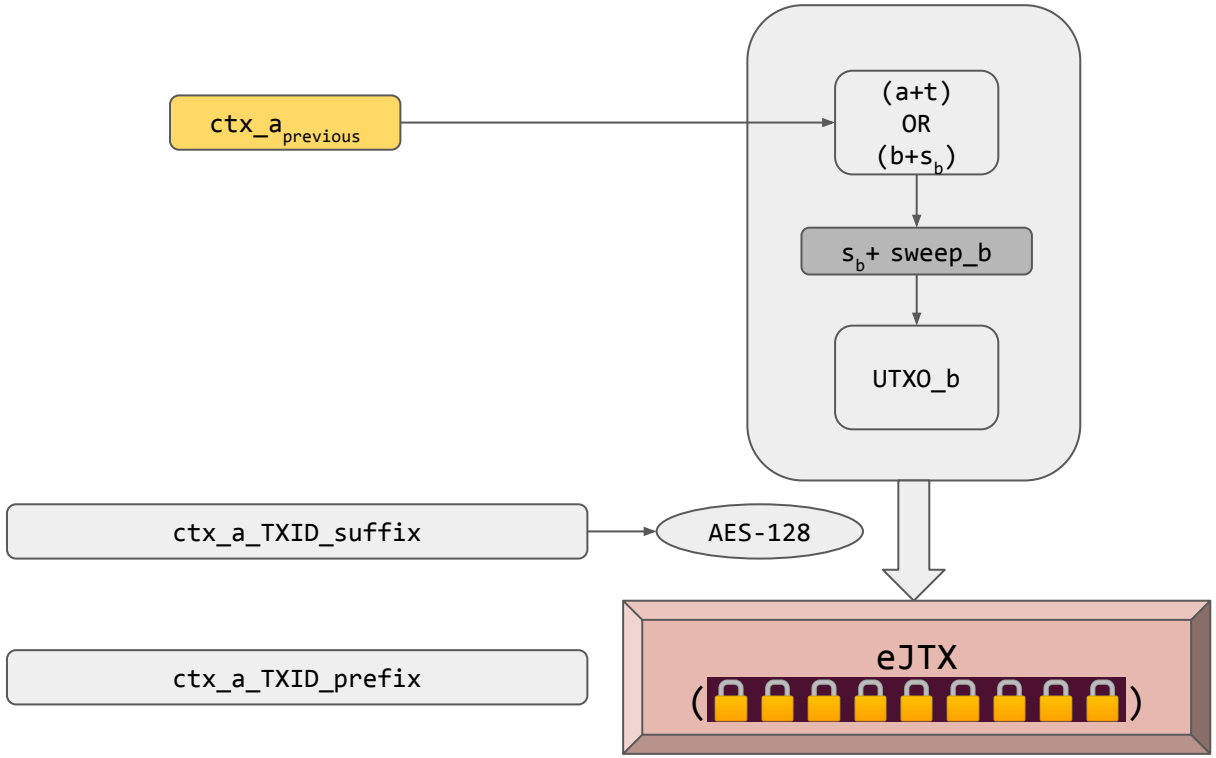
Watchtower

Watchtower



stick figures: XKCD

Justice Kit


ctx_a_previous
(a+t)
OR
(b+s_b)
s_b+ sweep_b
UTXO_b
ctx_a_TXID_suffix
AES-128
ctx_a_TXID_prefix
eJTX
(

Watchtower

e3b0c44298...	
6e340b9cff...	
96a296d224...	
709e80c884...	
df3f619804...	
8855508aad...	
...	...
...	...
...	...

How much does it cost?

(Size of Encrypted Blob + Size of Key)
(350 + 32)

X
Number of Updates
(1M)

X
Number of Channels
(30000)

=

11 TB
(always online server, watching the blockchain)

Observations

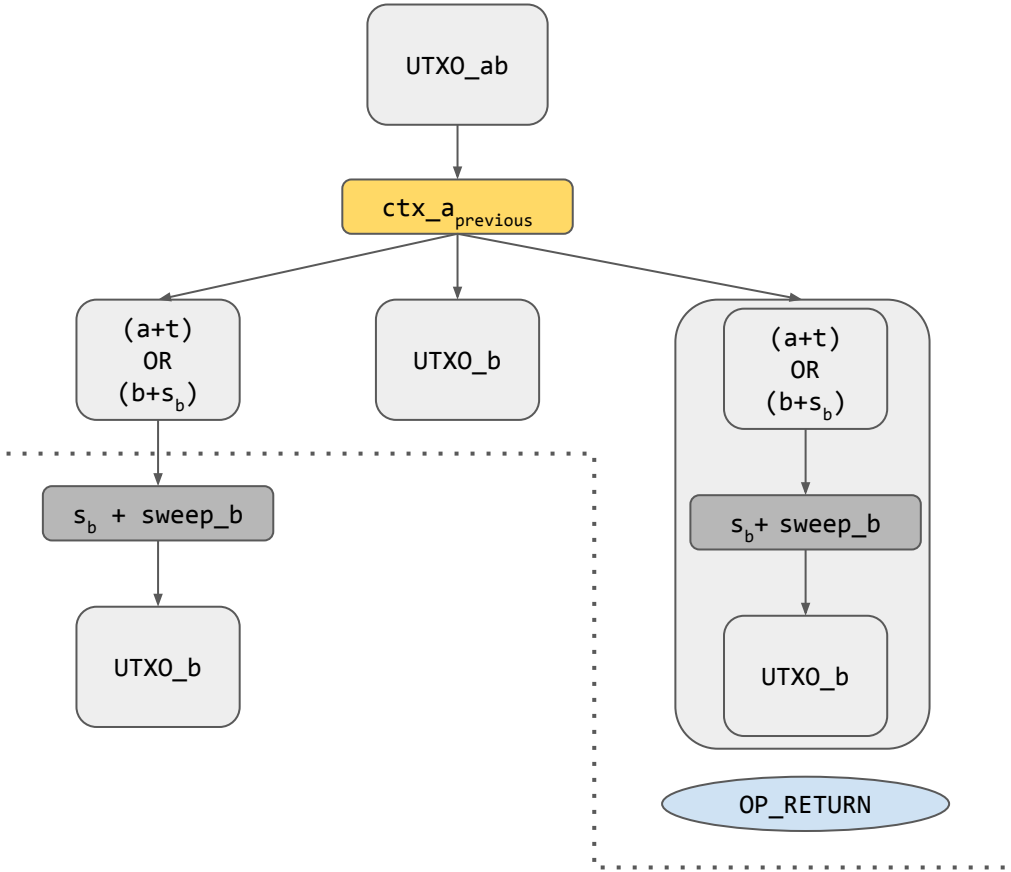
Cheater has to store cheating CTX(s)

Every CTX has a corresponding JTX

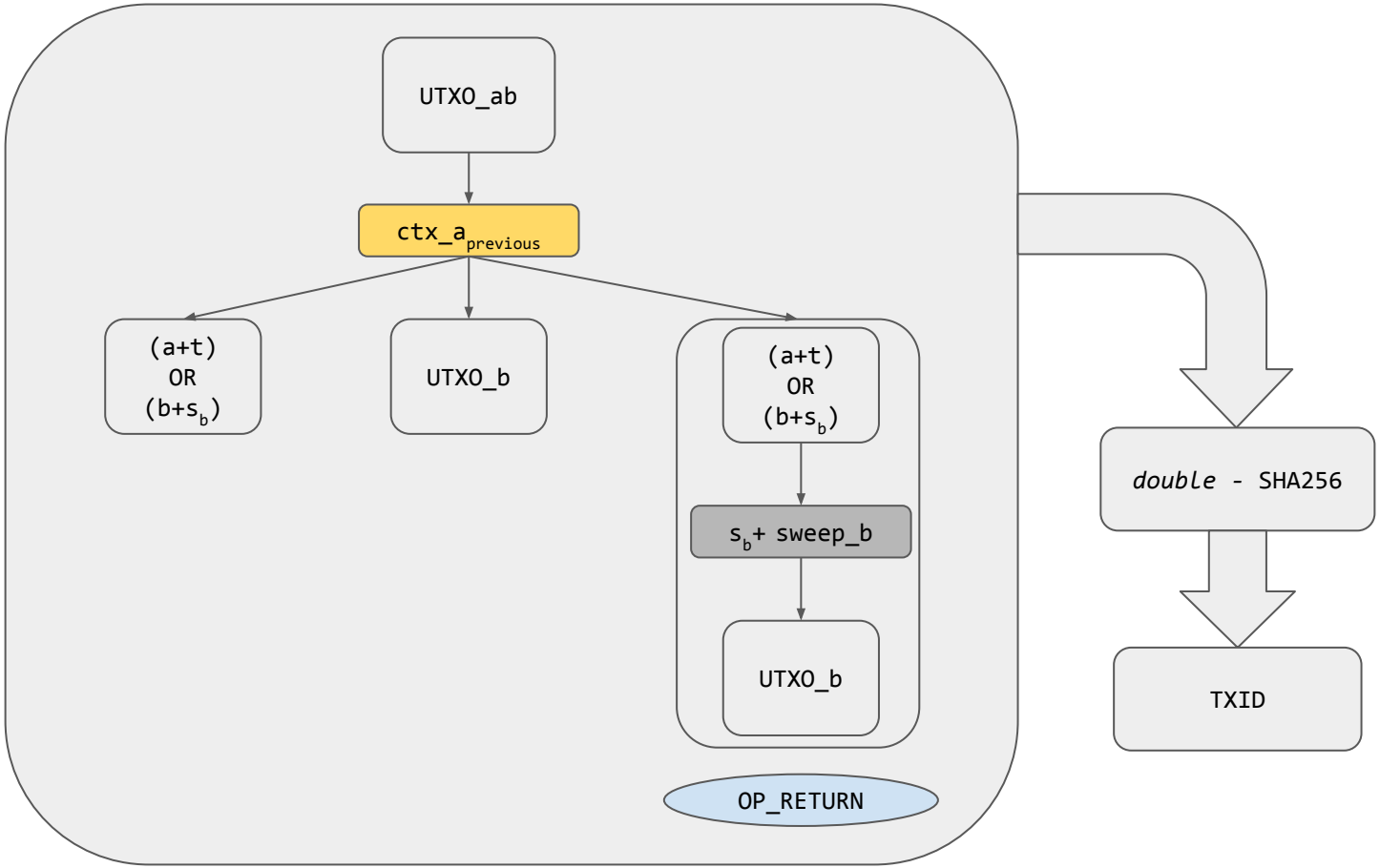
CTX has to be published on the blockchain

Store the corresponding JTX inside this CTX?

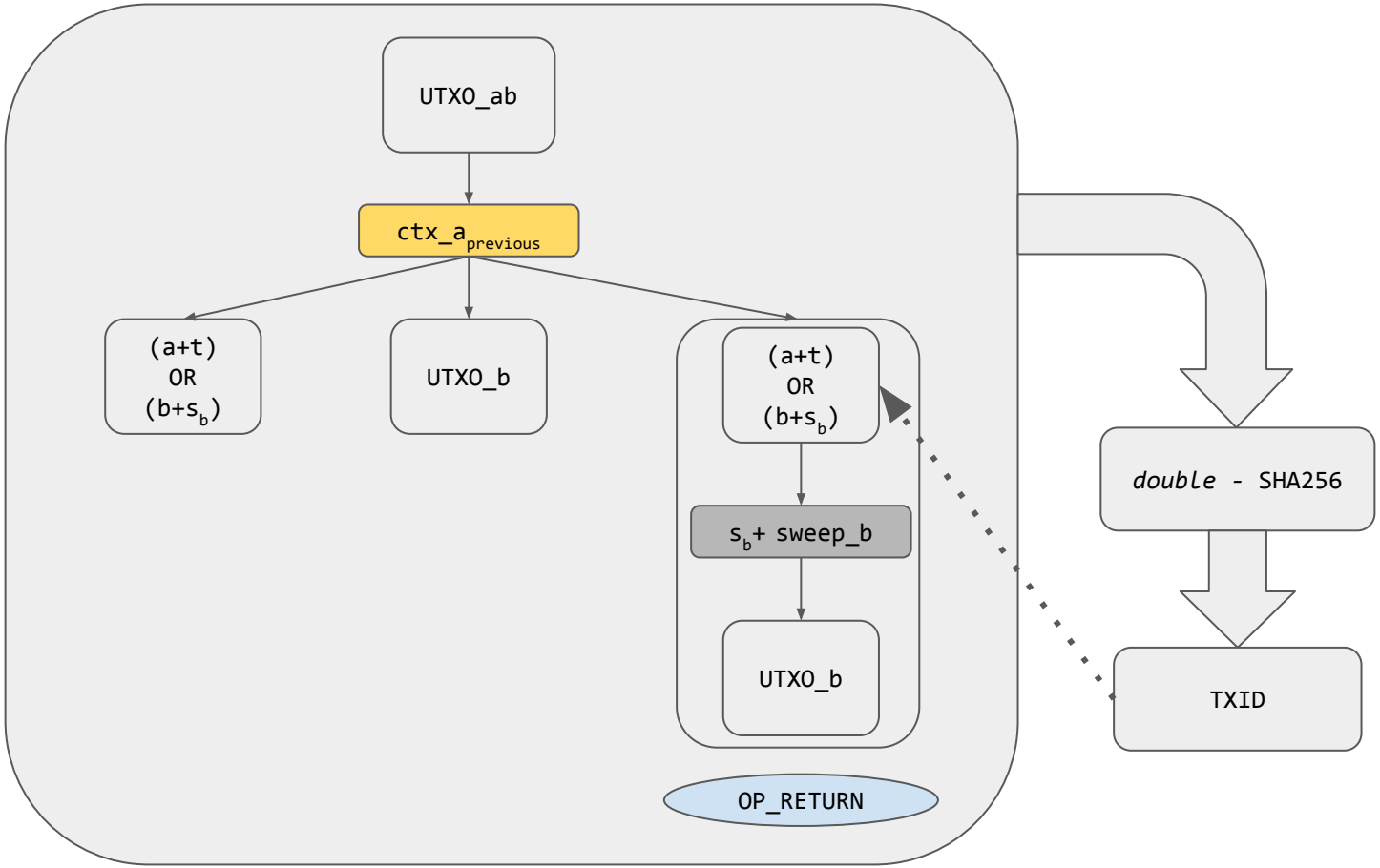
Can we store JTX inside CTX?



TXID

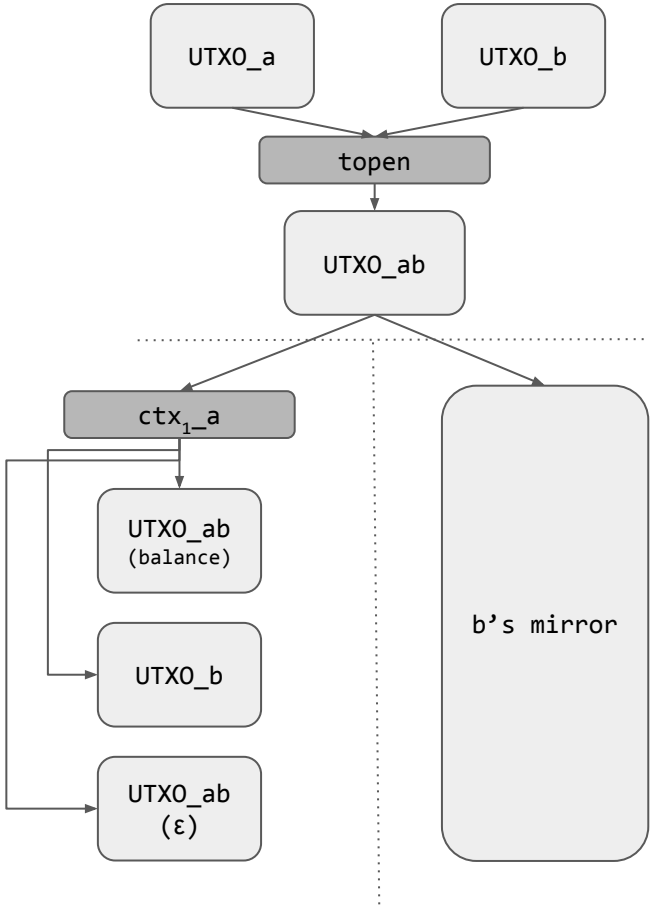

UTXO_ab
ctx_a previous
(a+t)
OR
(b+s_b)
UTXO_b
(a+t)
OR
(b+s_b)
s_b+ sweep_b
UTXO_b
OP_RETURN
double - SHA256
TXID

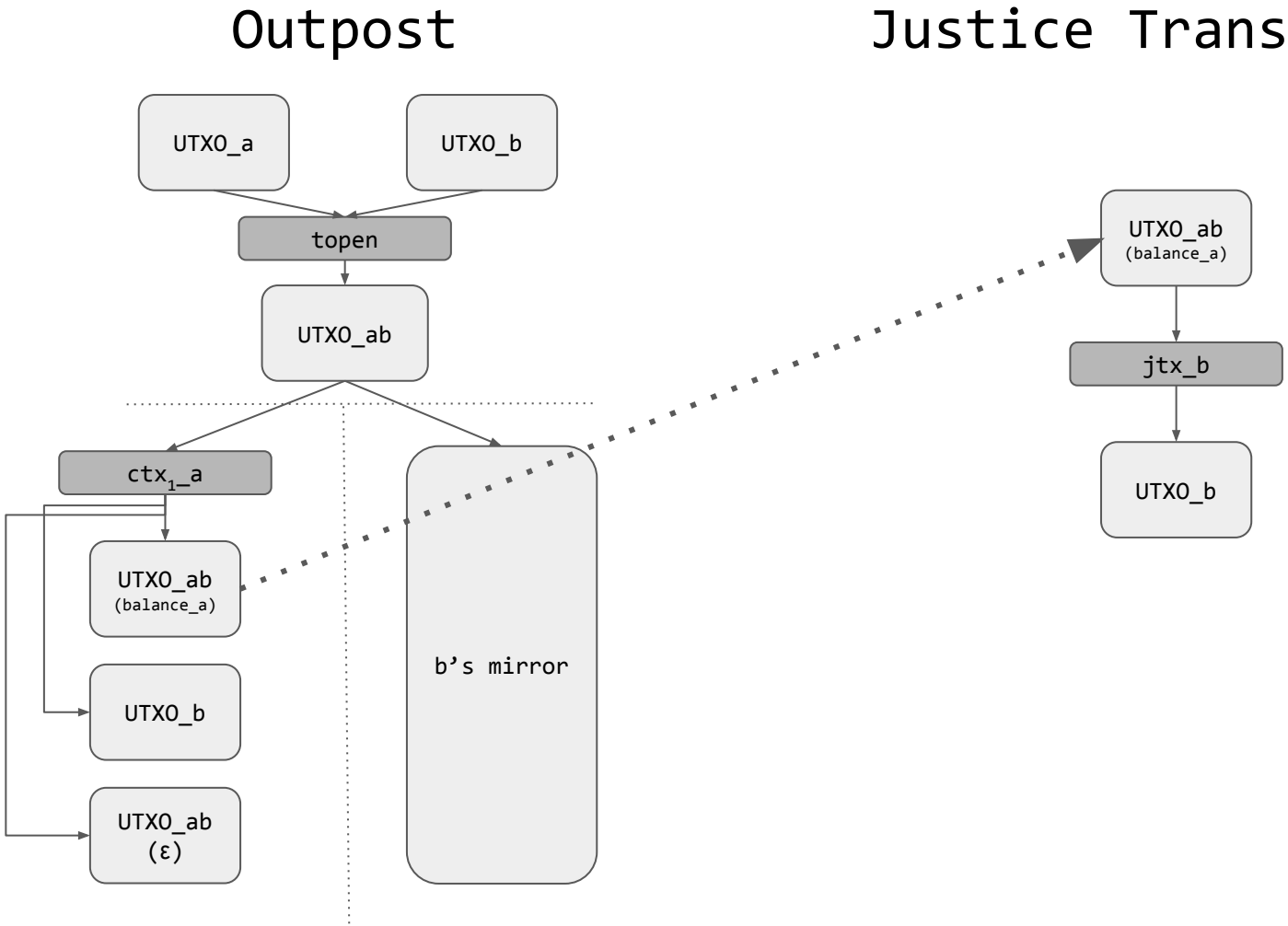
TXID makes it self-referential



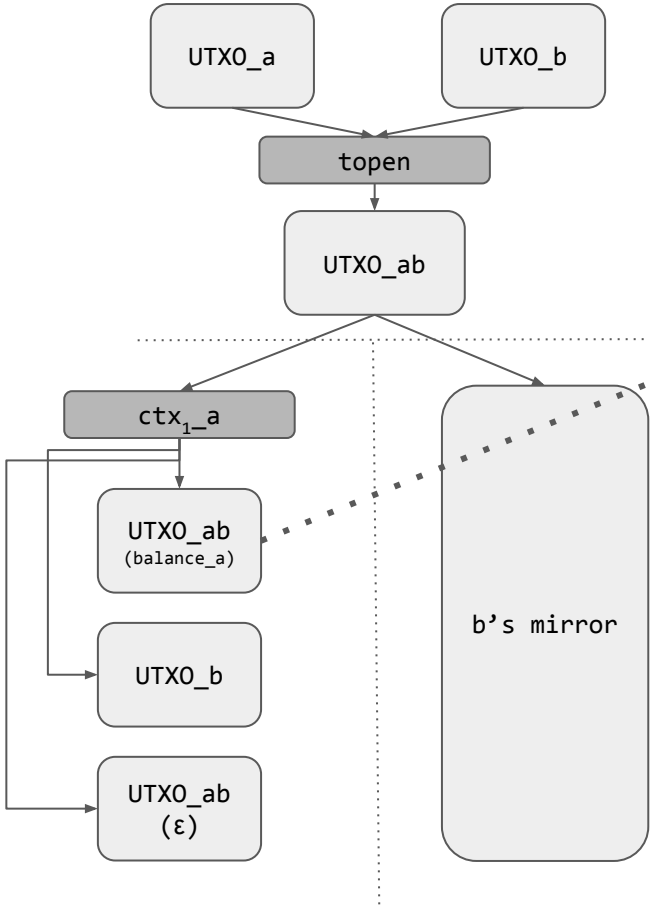
Outpost

Outpost

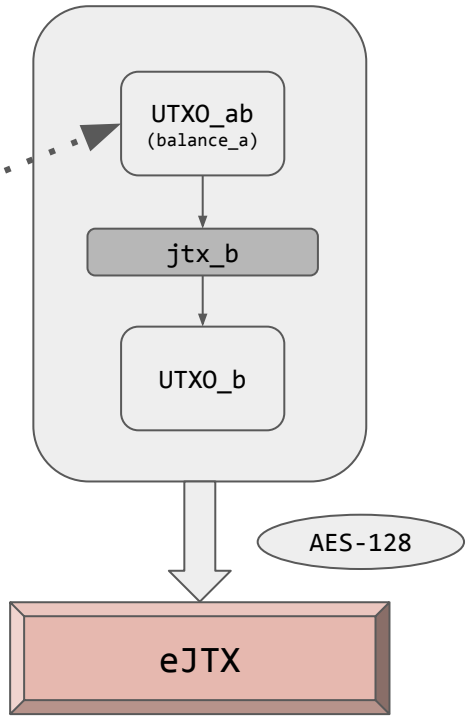

UTXO_a
UTXO_b
topen
UTXO_ab
ctx1_a
UTXO_ab
(balance)
UTXO_b
UTXO_ab
(ε)
b's mirror

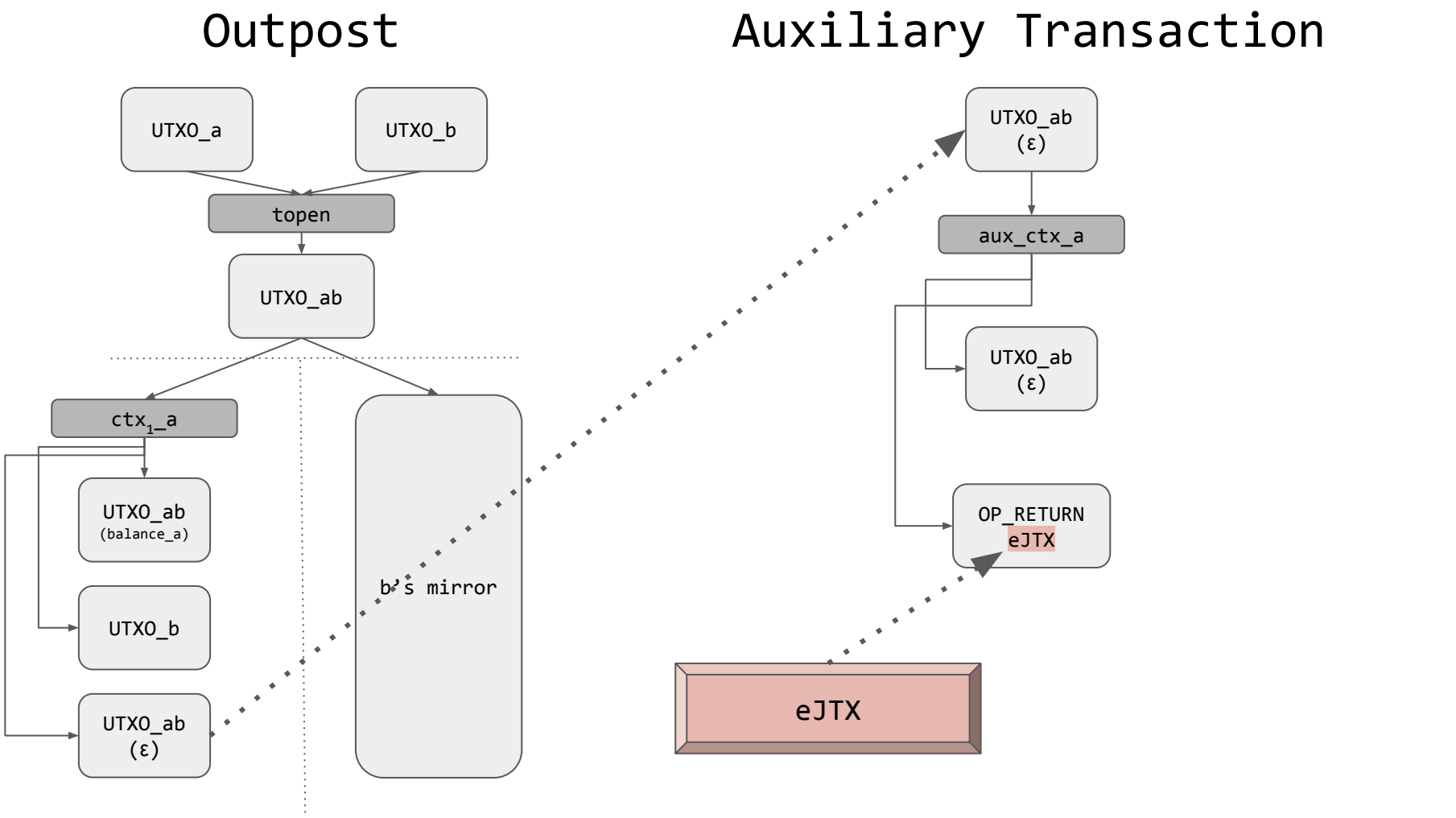

Outpost
Justice Transaction
UTXO_a
UTXO_b
topen
UTXO_ab
ctx1_a
UTXO_ab
(balance_a)
UTXO_b
UTXO_ab
(ε)
b's mirror
UTXO_ab
(balance_a)
jtx_b
UTXO_b

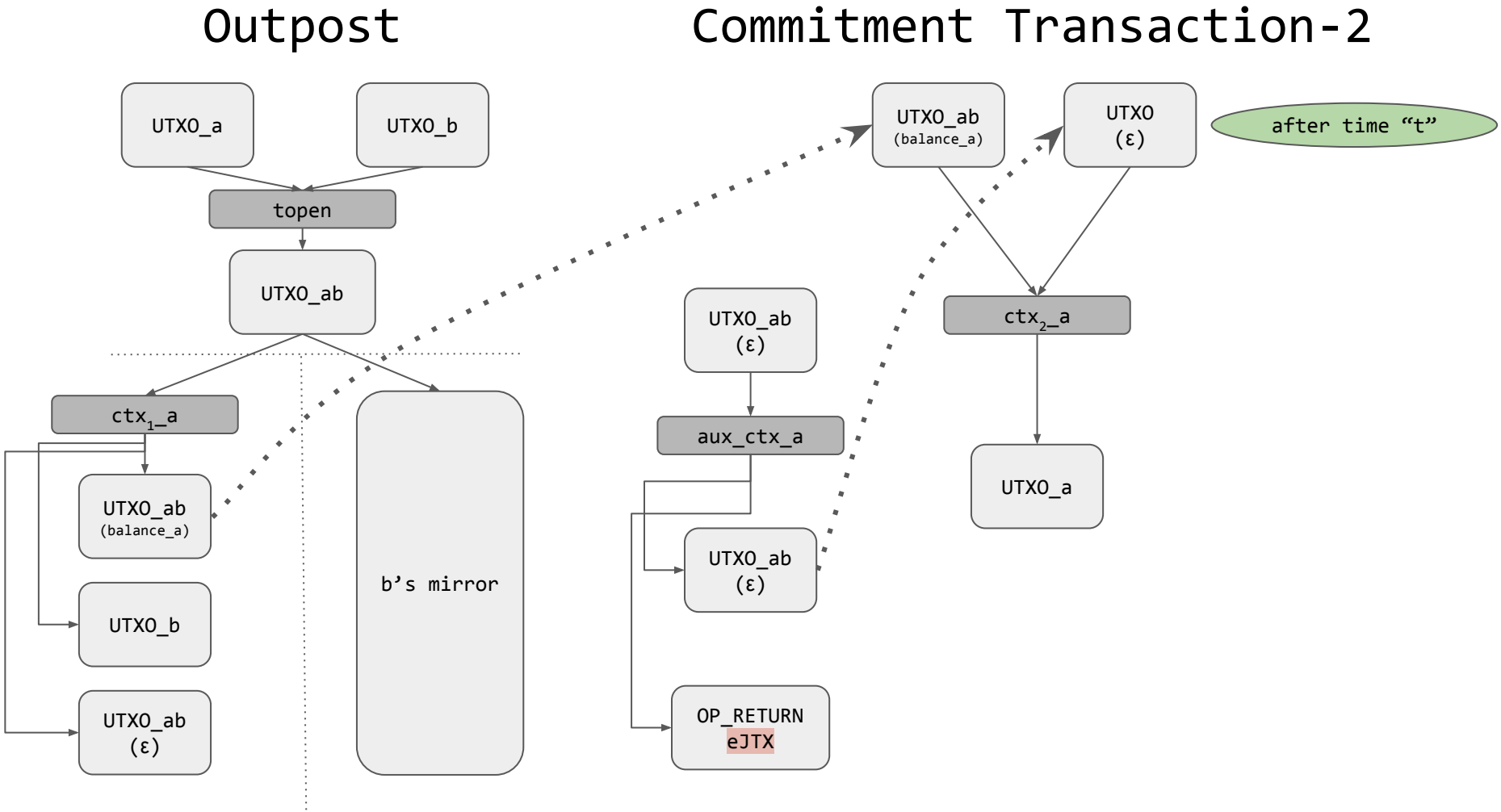
Outpost



Encrypted Justice Transaction




Outpost
Auxiliary Transaction
UTXO_a
UTXO_b
topen
UTXO_ab
ctx1_a
UTXO_ab
(balance_a)
UTXO_b
UTXO_ab
(ε)
b's mirror
UTXO_ab
(ε)
aux_ctx_a
UTXO_ab
(ε)
OP_RETURN
eJTX
eJTX


Outpost
Commitment Transaction-2
UTXO_a
UTXO_b
topen
UTXO_ab
ctx1_a
UTXO_ab
(balance_a)
UTXO_b
UTXO_ab
(ε)
b's mirror
UTXO_ab
(balance_a)
UTXO
(ε)
after time "t"
UTXO_ab
(ε)
ctx2_a
aux_ctx_a
UTXO_a
UTXO_ab
(ε)
OP_RETURN
eJTX

The money slide

Classic Lightning

	Per channel, with N updates	30k channels, 1M updates
Known Channel	N·size(ejtx) + 1·size(txid)	10.00 TB
Unknown Channel	N·size(ejtx) + N·size(txid))	11.45 TB

Outpost

Known Channel	size(key) + size(txid)	1.44 **MB** (WTF)
Unknown Channel	N·size(key) + N·size(txid)	1.44 TB

Note: size(key) << size(ejtx) i.e. 16 << 350

Outpost keeps Lightning’s key features

- Unilateral closure: broadcaster has to wait
    - Not cheating
    - Cheating

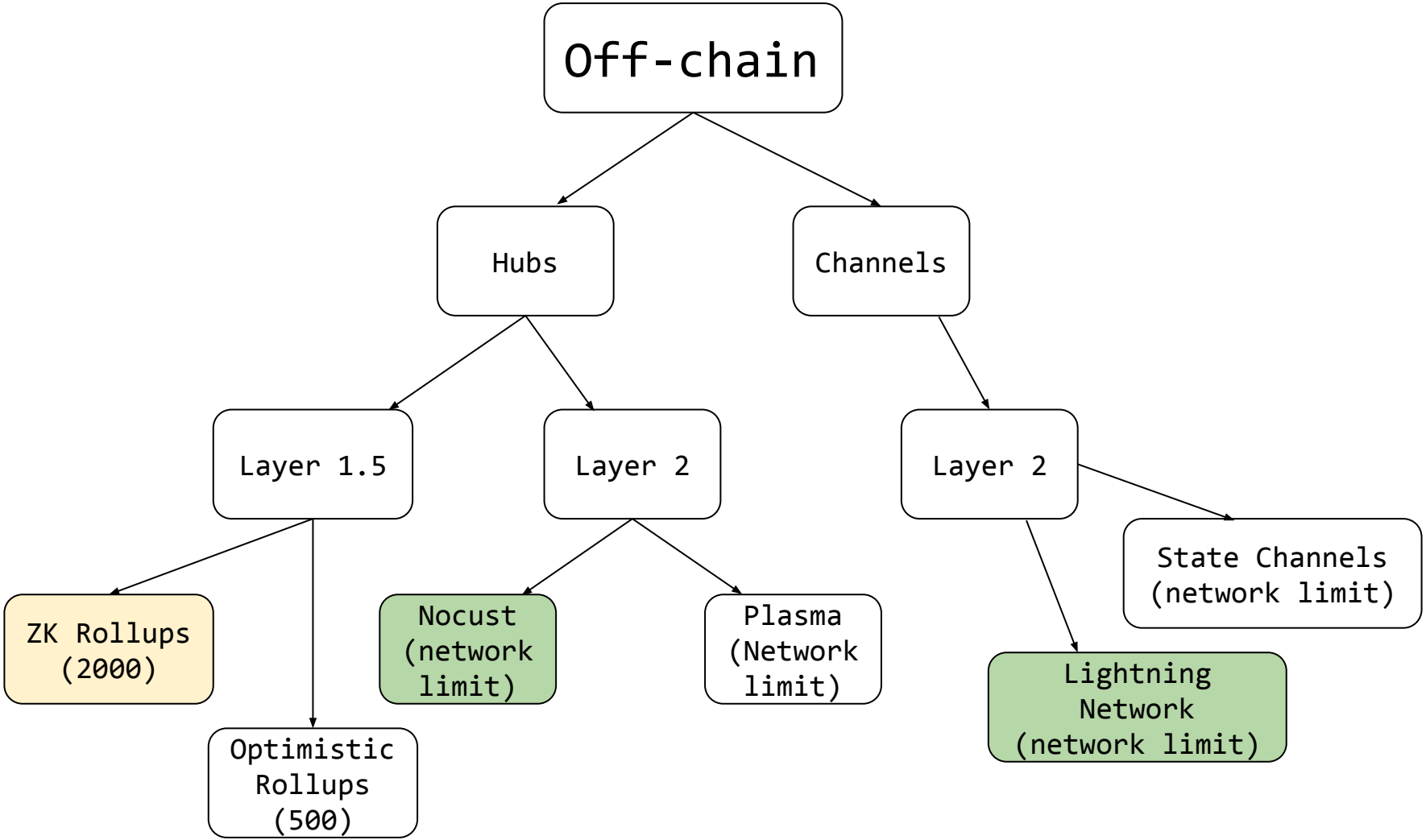
- Exchange revocation keys vs. AES-128 decryption keys

Limitations

- OP_RETURN limited to 80 bytes.
  - IsStandard ಠ_ಠ
  - Split aux_ctx into 2; P2SH Data-hash across them

- Bloat
  - Not on the blockchain (happy case)
  - On the blockchain, 3 txns vs 1 txn

- But
  - No changes to Bitcoin, whatsoever.


Off-chain
Hubs
Channels
Layer 1.5
Layer 2
Layer 2
ZK Rollups (2000)
Optimistic Rollups (500)
Nocust (network limit)
Plasma (Network limit)
State Channels (network limit)
Lightning Network (network limit)