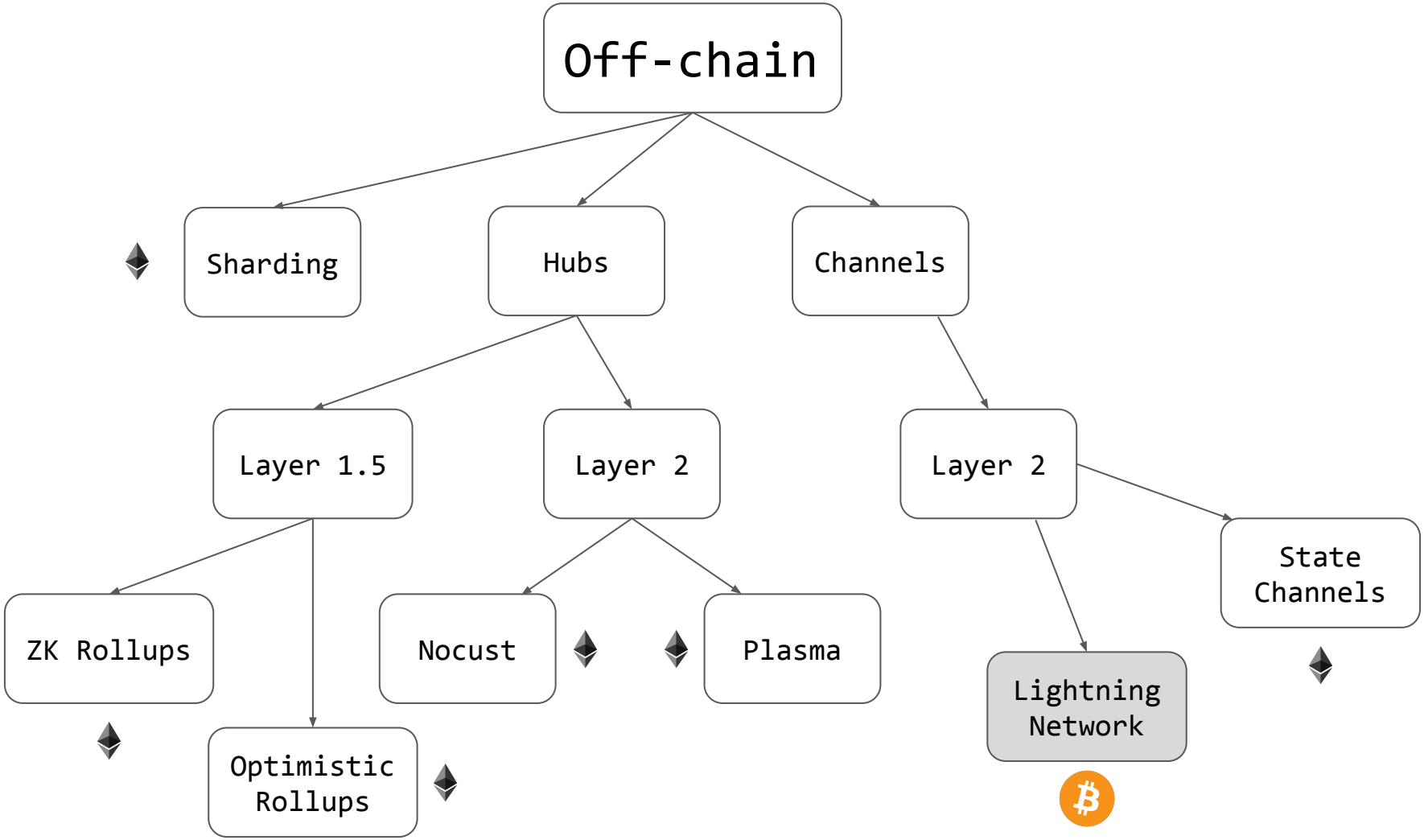
Layer-1 Blockchains have low throughput

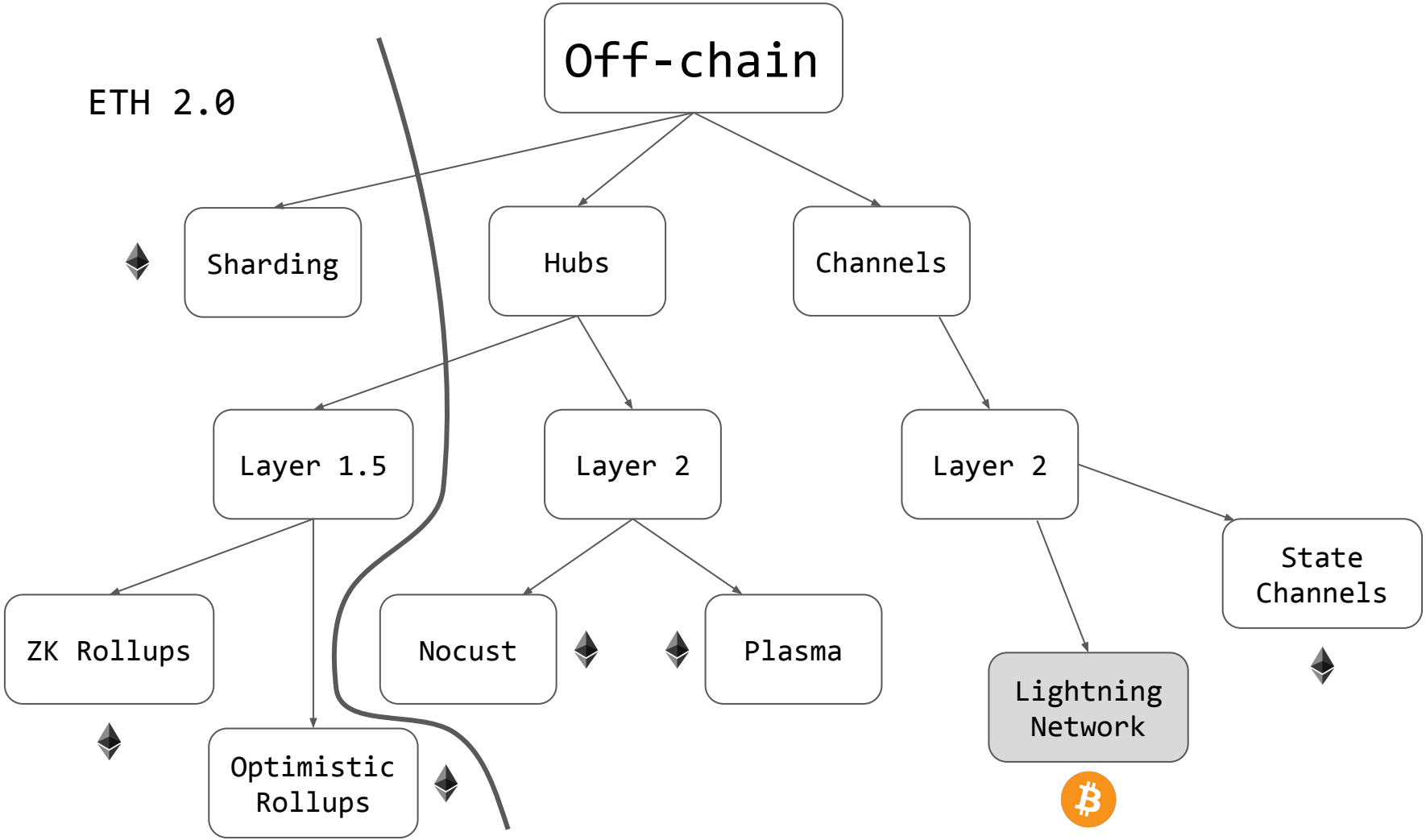
Bitcoin ~ 7 tps

Ethereum(1.0) ~ 15 tps

Channels

Moar Throughput!!!


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


Off-chain
ETH 2.0
Sharding
Hubs
Channels
Layer 1.5
Layer 2
Layer 2
ZK Rollups
Nocust
Plasma
State Channels
Lightning Network
Optimistic Rollups

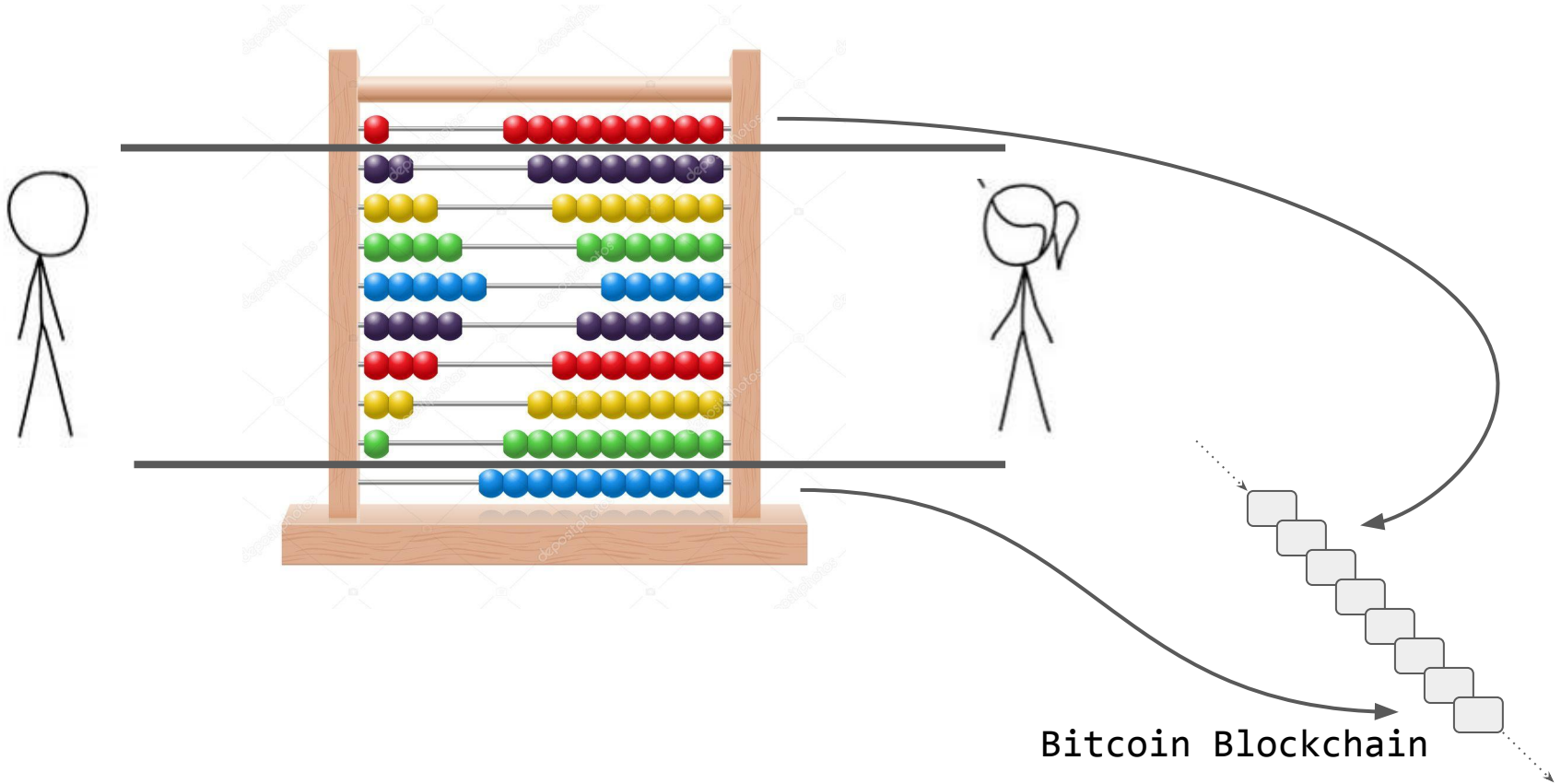
Layer-2: Payment channels

- Bitcoin - constrained smart contracts

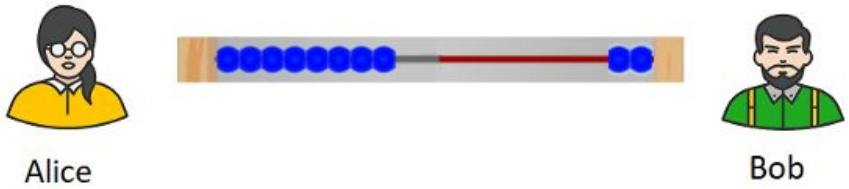
Payment Channels (and Networks)

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

Payment Channels

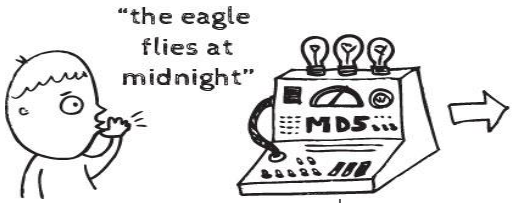


Connecting Channels



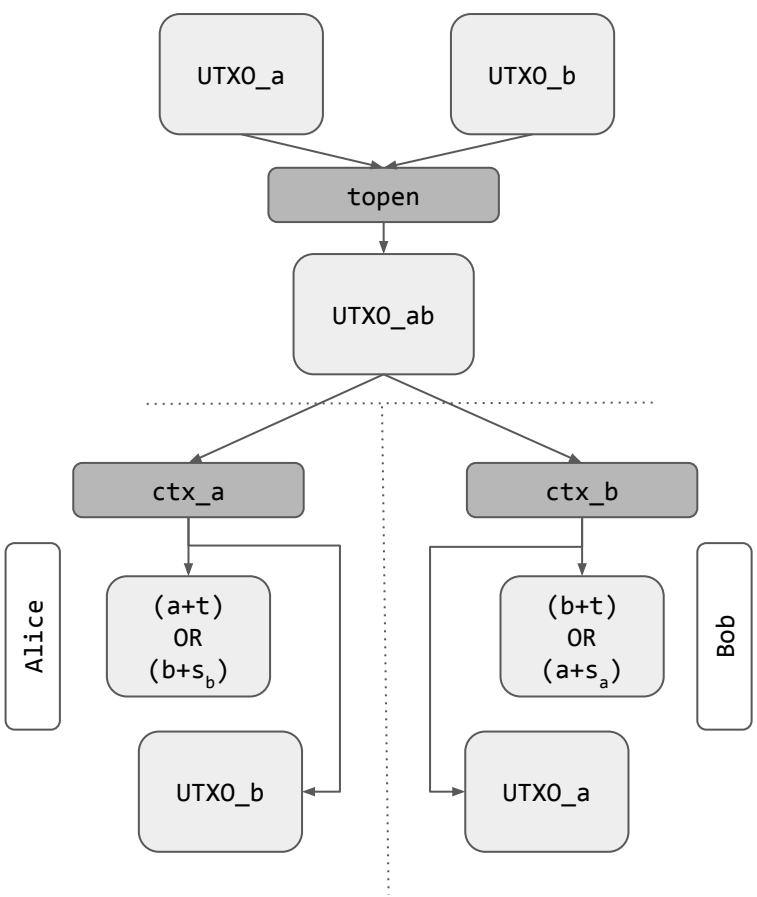
Bitcoin Primitives

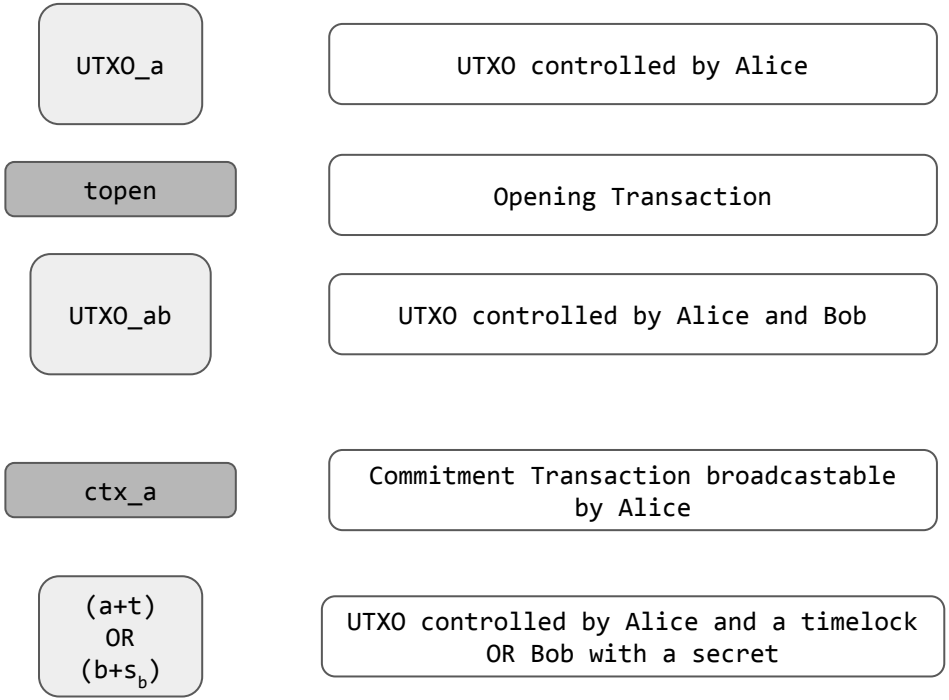
- UTXO - Unspent Transaction Output
- Multi-signature
- Cryptographic Hash Function
- Timelocks



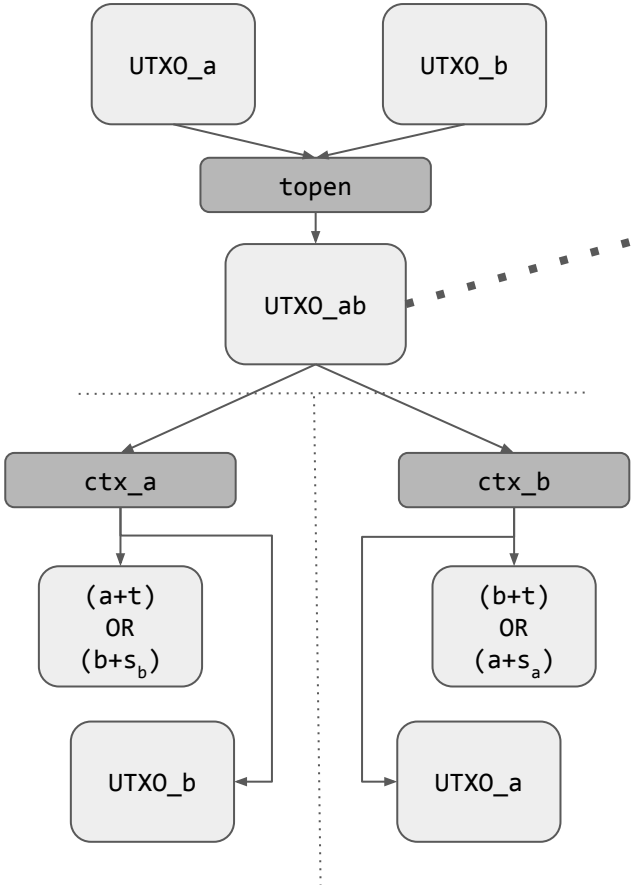
Hashed Timelocked Contracts

Lightning Channel

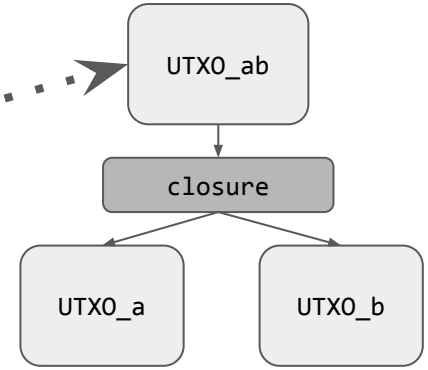




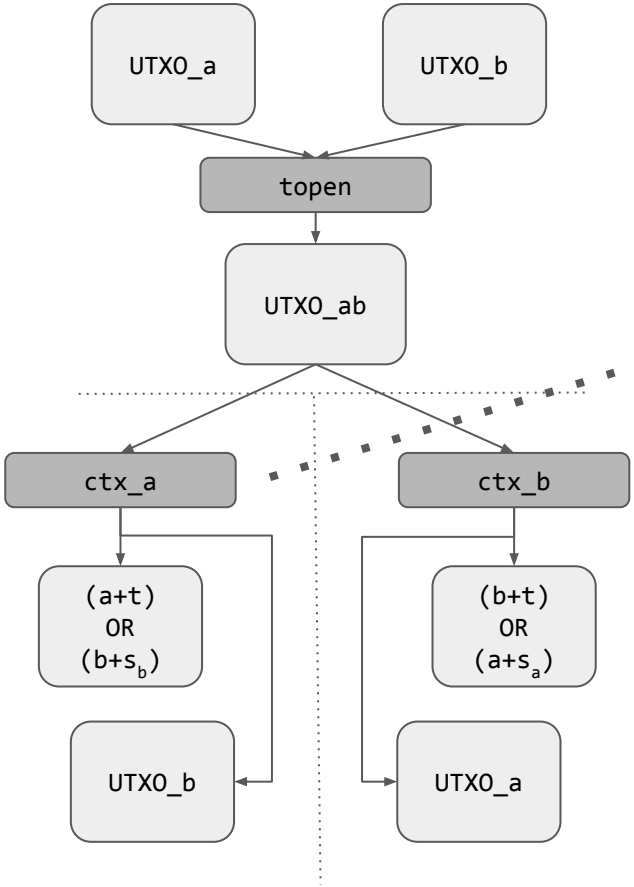
Lightning Channel



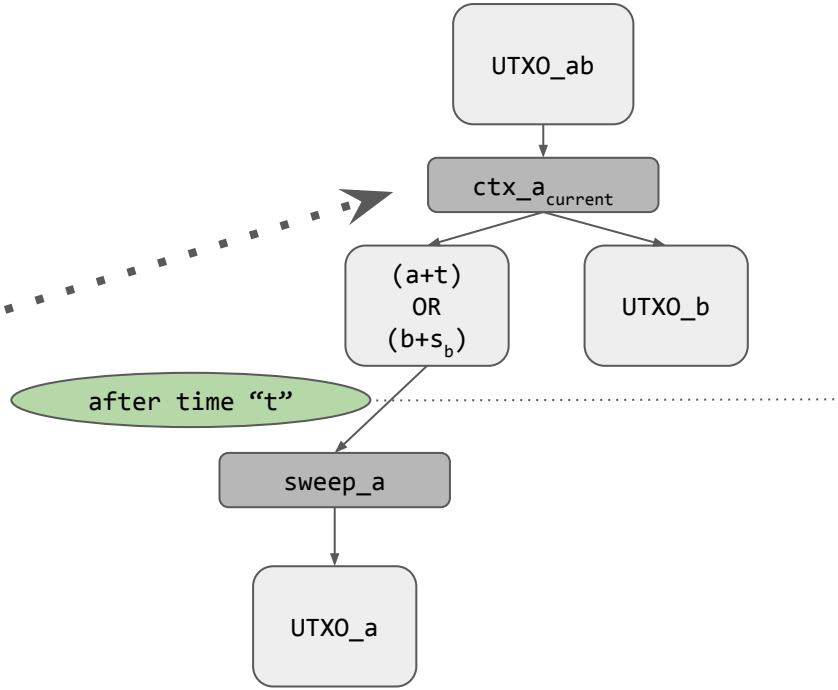
Bilateral Closure



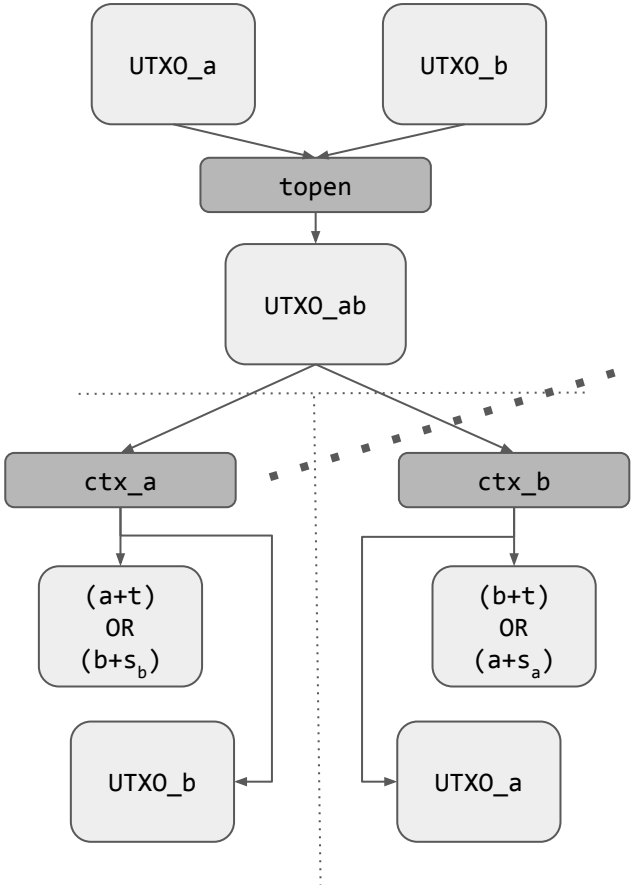
Lightning Channel



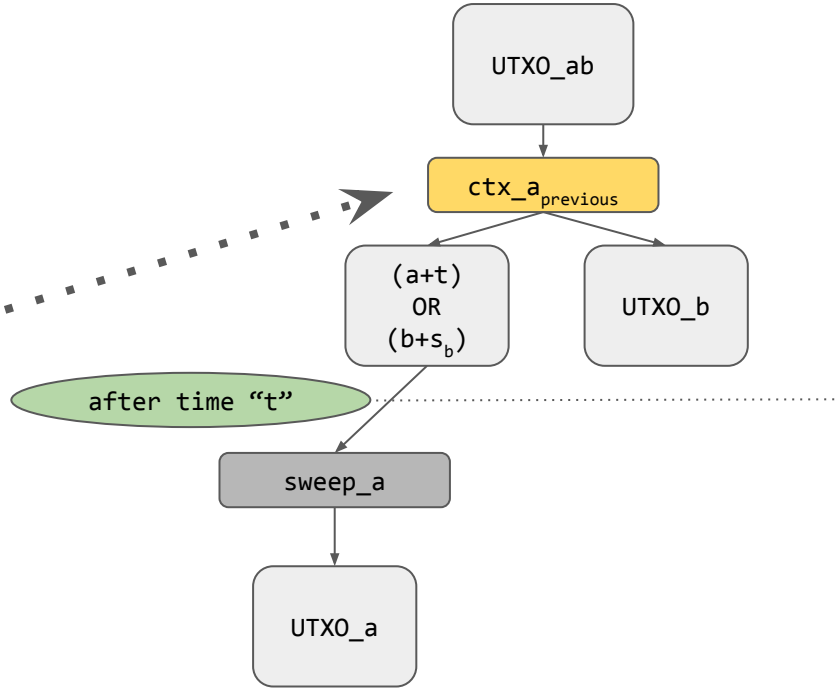
Unilateral Closure



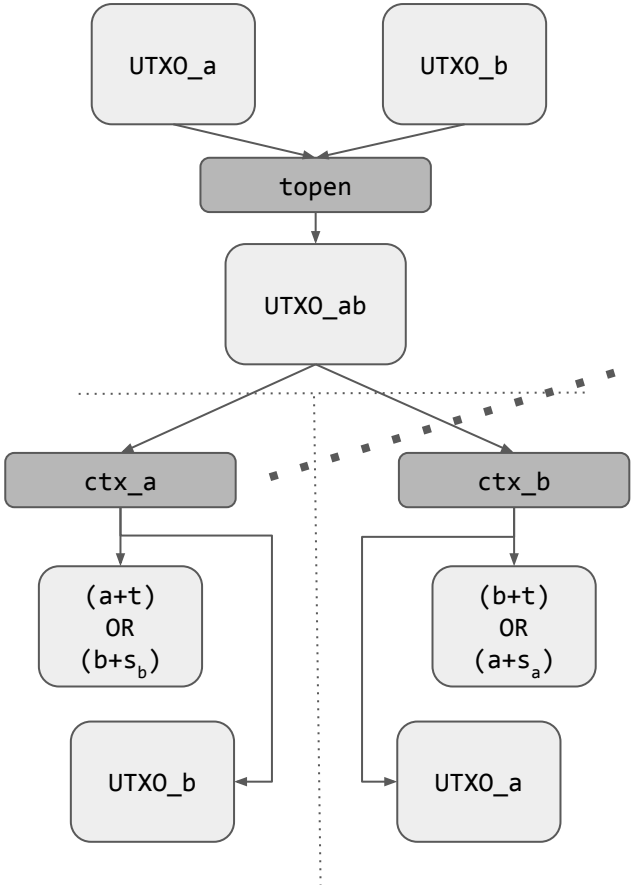
Lightning Channel



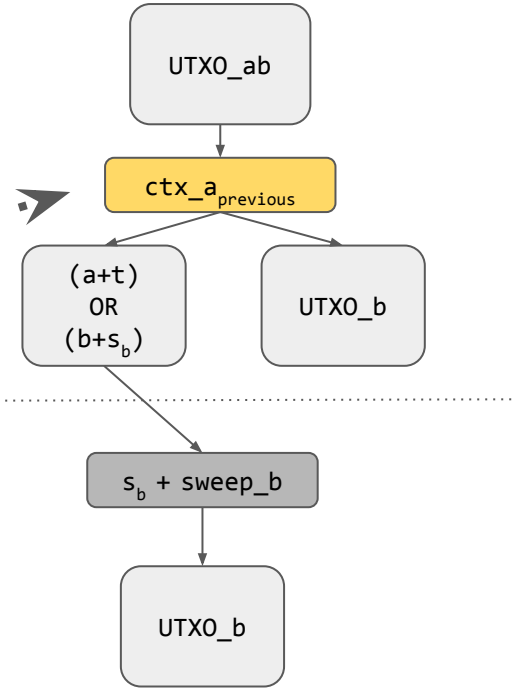
Cheating Closure



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
```

Some Engineering Details

BOLT - Basis of Lightning Technology 😀
BOLT(s) 1-11 (handshake, routing, invoices, etc.)

Multiple Implementations

- LND - Golang
- Eclair - Scala
- C-Lightning - C

- Rust-lightning - Rust
- ??? - C++

Miner Extractable Value

OMG!!!

Ethereum/Bitcoin/Others

Malicious/Rational Miner

Modification

Inclusion

Inspect & Include

Ordering

Exclusion

Ethereum

Malicious/Rational Miner

~~Modification~~

~~Inclusion~~

Inspect & Include ☠☠☠

Ordering ☠☠☠

Exclusion ☠☠☠

Bitcoin

Malicious/Rational Miner

~~Modification~~

~~Inclusion~~

Inspect & Include

Ordering

Exclusion

Bitcoin

Malicious/Rational Miner

~~Modification~~

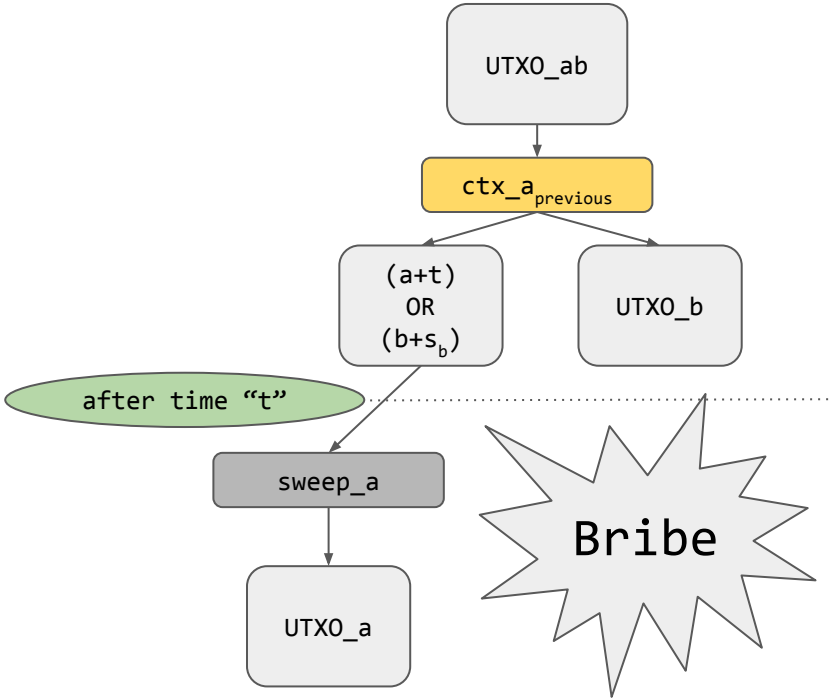
~~Inclusion~~

Inspect & Include (???)

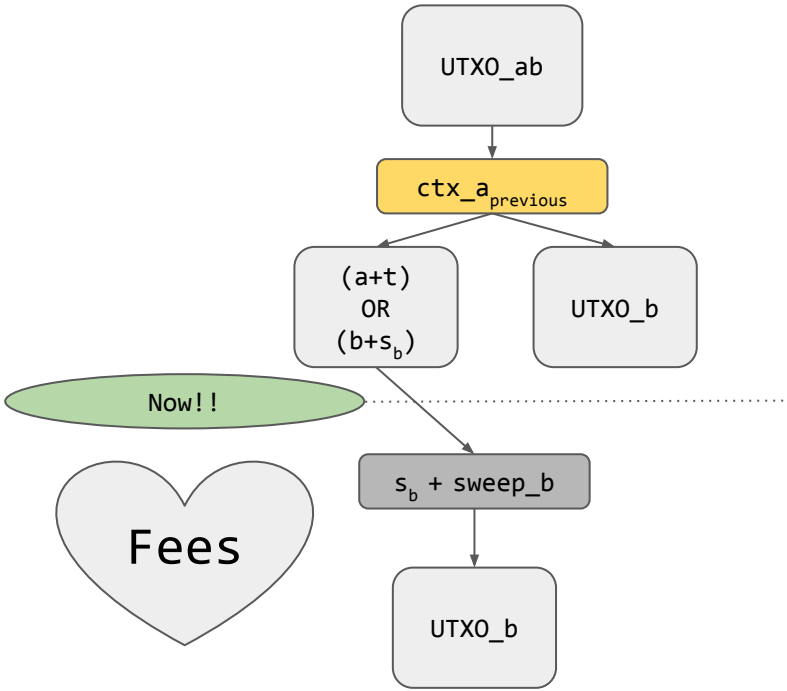
Ordering (???)

Exclusion ☠☠☠

Cheating Closure



Justice Transaction



TXN-1: Mine Now! - Take f in Fees

TXN-2: Mine Later! - Take b in Bribe

TXN-1: Mine Now! - Take f in Fees

TXN-2: Mine Later! - Take b in Bribe

But

TXN-1: Mine Now! - Take f in Fees

TXN-2: Mine Later! - Take b in Bribe

But

TXN-1 or TXN-2, not both
TXN-1 is valid now
TXN-2 is valid only after T blocks

Let’s say you wait...

What is the probability of mining block T+1?

Hashrate of a miner!!

Our Insight

Profit and mining probability are connected

Strong miners: $p > f/b$

Weak miners: $p < f/b$

All miners are strong

One strong miner refuses the bribe: $x.f + (1-x).p.b$

$x.f + (1-x).p.b < p.b$ …because $p > f/b$ and $x > 0$

One miner is weak

One weak miner refuses the bribe

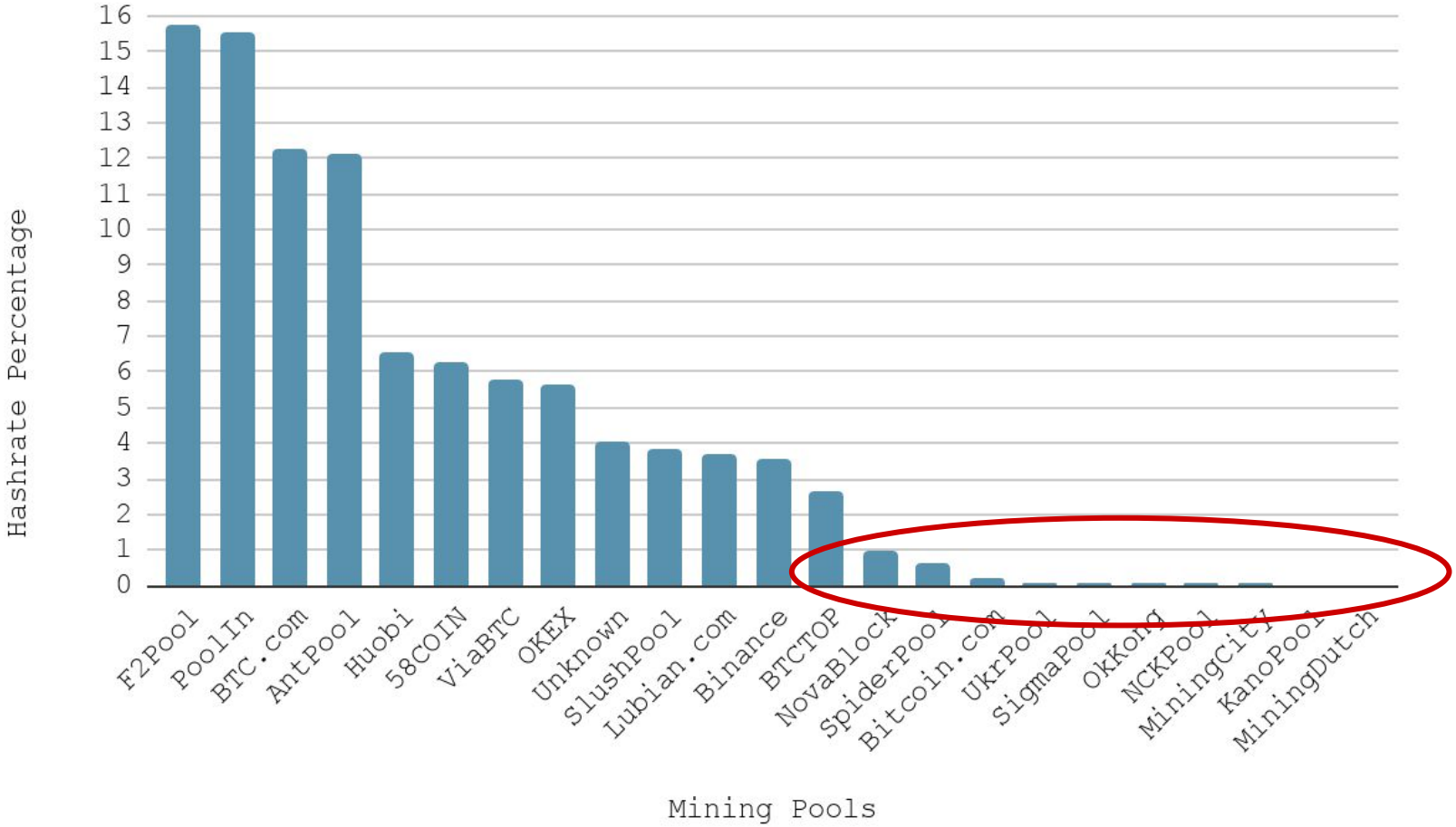
Outcome-1: [T+1] $p.b < f$

Outcome-2: [0,1,2...T] f (with some probability)

Outcome-2's **attempt** doesn't preclude Outcome-1

At $T > \frac{\log \frac{f}{b}}{\log(1 - p_w)}$ the game is safe at T = 0

Typically, $f/b = 0.01$


Hashrate Percentage
16
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
0
F2Pool
PoolIn
BTC.com
AntPool
Huobi
58COIN
ViaBTC
OKEX
Unknown
SlushPool
Lubian.com
Binance
BTCTOP
NovaBlock
SpiderPool
Bitcoin.com
UkrPool
SigmaPool
OkKong
NCKPool
MiningCity
KanoPool
MiningDutch
Mining Pools

Where?

Lightning Channels have $f/b = 0.01$ and $T = 144$

We recommend:
$T = 212$ based on weak miners hashrate
(changes over time)

Where?

Lightning Channels have $f/b = 0.01$ and $T = 144$

We recommend:
$T = 212$ based on weak miners hashrate
(changes over time)

Atomic Swaps, Covenants, Vaults, etc.