Layer-1 Blockchains have low throughput

Bitcoin ~ 7 tps

Ethereum(1.0) ~ 15 tps
Channels

Moar Throughput!!!
Off-chain

ETH 2.0

Sharding

Layer 1.5

Layer 2

Layer 2

Channels

Hubs

Lightning Network

State Channels

ZK Rollups

Optimistic Rollups

Nocust

Plasma
Layer-2: Payment channels

- Bitcoin - constrained smart contracts
- Duplex Micropayment Channels (ETH contribution)
- Lightning Channels
- Eltoo Channels (ETH alumni)
Payment Channels

Bitcoin Blockchain
Connecting Channels
Bitcoin Primitives

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

Hashed Timelocked Contracts
Lightning Channel

- **UTXO_a**
- **UTXO_b**

**topen**

- **UTXO_ab**

**ctx_a**
- (a+t)
- OR
- (b+s_b)

**UTXO_b**

**ctx_b**
- (b+t)
- OR
- (a+s_a)

**UTXO_a**

**Alice**

- Commitment Transaction broadcastable by Alice

**Bob**

- UTXO controlled by Alice and a timelock
- OR Bob with a secret

**Opening Transaction**

- UTXO controlled by Alice and Bob

- UTXO controlled by Alice
Lightning Channel

UTXO_a

utoken

UTXO_ab

ctx_a

(a+t)

OR

(b+s_b)

UTXO_b

ctx_b

(b+t)

OR

(a+s_a)

UTXO_a

Bilateral Closure

UTXO_ab

closure

UTXO_a

UTXO_b
Lightning Channel

- UTXO_a
- UTXO_b

- `topen`

- UTXO_ab

- `ctx_a`
  - (a+t)
  - OR
  - (b+s_b)

- UTXO_b

- `ctx_b`
  - (b+t)
  - OR
  - (a+s_a)

- UTXO_a

Unilateral Closure

- UTXO_ab

- `ctx_a_current`
  - (a+t)
  - OR
  - (b+s_b)

- UTXO_b

- `sweep_a`

- UTXO_a

`after time “t”`
Lightning Channel

UTXO_a

UTXO_b

topen

UTXO_ab

ctx_a

ctx_b

(a+t) OR (b+s_b)

UTXO_b

Cheating Closure

UTXO_ab

ctx_a

previous

(a+t) OR (b+s_b)

UTXO_b

after time “t”

sweep_a

UTXO_a
Lightning Channel

UTXO_a

UTXO_b

topen

UTXO_ab

ctx_a

(a+t)
OR
(b+s_b)

UTXO_b

UTXO_ab

ctx_b

(b+t)
OR
(a+s_a)

UTXO_a

Justice Transaction

UTXO_ab

ctx_a_{previous}

(a+t)
OR
(b+s_b)

UTXO_b

s_b + sweep_b

UTXO_b
# 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!!!
Malicious/Rational Miner

- Modification
- Inclusion
- Inspect & Include
- Ordering
- Exclusion

Ethereum/Bitcoin/Others
Malicious/Rational Miner

Ethereum

Modification

Inclusion

Inspect & Include ☠☠☠

Ordering ☠☠☠

Exclusion ☠☠☠
Malicious/Rational Miner

Bitcoin

Modification

Inclusion

Inspect & Include (???)

Ordering (???)

Exclusion ☠☠☠
Cheating Closure

(a+t) OR (b+s_b)

ctx_a_previous

UTXO_ab

UTXO_b

ctx_a_previous

UTXO_ab

UTXO_b

Bribe

UTXO_a

Fees

s_b + sweep_b

UTXO_b

after time “t”

Now!!
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: \( x.f + (1-x).p.b \)

\[ x.f + (1-x).p.b < p.b \quad \text{...because} \quad p > f/b \quad \text{and} \quad x > 0 \]
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, $f/b = 0.01$
Where?

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

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