Payment Channels
Designing Secure Watchtowers

Zeta Avarikioti
Can cryptocurrencies scale?

- Bitcoin: 7 tx/s
- Ethereum: 20 tx/s
- VISA: 65,000 tx/s
Payment Channels
Payment Channels
Payment Channels

Funding transaction

```
<table>
<thead>
<tr>
<th>Pay to the order of</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>5btc</td>
</tr>
<tr>
<td>Bob</td>
<td>4btc</td>
</tr>
</tbody>
</table>
```
Payment Channels

Funding transaction

Alice  5btc

Bob   4btc

5 —— 4
Payment Channels

Funding transaction

Alice sends 3btc

5 btc

4 btc

2 btc

7 btc
Payment Channels

Funding transaction

Alice sends 3btc

Bob sends 6btc

5  4  2  7  8  1
Lightning Channels

Funding
Commitment
Dispute period
Revocation
Watchtowers

- Funding
- Commitment
- Dispute period
- Revocation
Why be a Watchtower?
### Why be a Watchtower?

Assuming rational parties and watchtowers…

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Will a party commit fraud?</td>
<td>✗</td>
</tr>
<tr>
<td>Will a watchtower get paid?</td>
<td>✗</td>
</tr>
<tr>
<td>Will a party commit fraud?</td>
<td>✓</td>
</tr>
<tr>
<td>Will a watchtower get paid?</td>
<td>✓</td>
</tr>
<tr>
<td>Will a party commit fraud?</td>
<td>✗</td>
</tr>
</tbody>
</table>

...
Why be a Watchtower?

<table>
<thead>
<tr>
<th>Watchtowers →</th>
<th>Active</th>
<th>Inactive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parties ↓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Fraud</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Why be a Watchtower?

<table>
<thead>
<tr>
<th>Watchtowers →</th>
<th>Active</th>
<th>Inactive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parties ↓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fraud</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Fraud</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Why be an active Watchtower?

Collateral
→ UTXO-based (Unspent Transaction Output)
→ Transaction: consumes & produces UTXOs
→ Multi-signatures: $\sigma_{AB}$
→ Timelocks: $\Delta t$
Lightning Channels

Funding
On-chain

Commitment
(1)
Published by A

Commitment
(i)
Published by A

Commitment
(i+1)
Published by A

Revocation
Published by B, W

\#σ_A

σ_{AB}

a + b

a

σ_B

b

(σ_A ∩ Δt) ∨ σ_{AB}

σ_{AB}

a_i

σ_B

b_i

(σ_A ∩ Δt) ∨ σ_{AB}

σ_B

a_{i+1}

σ_B

b_{i+1}
Cerberus Channels

- **Funding**: On-chain
  - #σ_A
  - a
  - b

- **Commitment (1)**: Published by A
  - σ_{AB}
  - a + b
  - (σ_A ∩ Δt) ∨ σ_{AW}
  - a
  - σ_{BW}
  - b

- **Commitment (i)**: Published by A
  - (σ_A ∩ Δt) ∨ σ_{AW}
  - a_i
  - σ_{BW}
  - b_i

- **Commitment (i+1)**: Published by A
  - (σ_A ∩ Δt) ∨ σ_{AW}
  - a_{i+1}
  - σ_{BW}
  - b_{i+1}

- **Revocation**: Published by B, W
  - σ_B
  - a_i + b_i

- **Penalty 1**: Published by B
  - c + b_i
  - σ_B

- **Collateral**: On-chain
  - #σ_W
  - c

- **Reclaim**: Published by W
  - σ_{BW}
  - c
  - σ_W
  - c
Cerberus Channels

- **Funding**: On-chain
  - $\#\sigma_A \rightarrow a$
  - $\#\sigma_B \rightarrow b$

- **Commitment (1)**
  - Published by A
  - $\sigma_{AB} \rightarrow a + b$
  - $(\sigma_A \land \Delta t) \lor \sigma_{AW}$

- **Commitment (i)**
  - Published by A
  - $\sigma_{AW} \rightarrow a_i$
  - $(\sigma_A \land \Delta t) \lor \sigma_{BW}$

- **Commitment (i+1)**
  - Published by A
  - $\sigma_{BW} \rightarrow b_{i+1}$
  - $(\sigma_B \land \Delta t) \lor \sigma_{BW}$

- **Revocation**
  - Published by B, W
  - $\sigma_B \rightarrow a_i + b_i$

- **Penalty 1**
  - Published by B
  - $\sigma_B \rightarrow c + b_i$

- **Reclaim**
  - Published by W
  - $\sigma_{BW} \rightarrow c$
  - $\sigma_B \rightarrow c$
Cerberus Channels

Funding
On-chain

Commitment (1)
Published by A

Commitment (i)
Published by A

Commitment (i+1)
Published by A

Reclaim
Published by W

Penalty 1
Published by B

Penalty 2
Published by B

Collateral
On-chain

Commitment
Published by A

Revocation
Published by B,
W

Cerberus Channels: Incentivizing Watchtowers for Bitcoin.

Fundamentals of Channels
Fundamentals of Channels

- Funding
- Commitment
- Dispute period
Fundamentals of Channels

- Funding
- Commitment
- Dispute period
  ➔ Eclipse
  ➔ Censor
  ➔ Congestion
Time = Cryptocurrency!
Time = CryptoMoney!

Asynchronous channels?
Be proactive, not reactive
Be proactive, not reactive

Funding

Close

Signatures of Alice & Bob
OR
Signatures of \( \frac{2}{3} \) WT & (Alice or Bob)
Challenges

1) Consensus is costly
2) Privacy is important
3) Incentives are critical
Consistent Broadcast

- O(n) communication complexity for state updates
- Verification of consensus between Alice & Bob
- No liveness guarantees, if Alice & Bob both misbehave
- Consensus needed only for closing, if there is a dispute
Encrypted State

➔ Privacy preserving

➔ Alice/Bob cannot publish a previous transaction
Brick Architecture

(3) Execute

(1) Update

(2) Consistent Broadcast

H(     )
Incentives

➔ Unilateral channel for fees:
   Repeated game lifts fair exchange impossibility

➔ Collateral for anti-bribing:
   Reduction to fair-exchange
   WT Committee size ↑ → per WT collateral ↓
Brick Advantages

- Asynchronous channels
- Security even under L1 failure
- Privacy
- Incentive-compatible
- Embarrassingly parallel
- Linear communication

Thank you!

Questions?
