Payment Channels
Designing Secure Watchtowers

Zeta Avarikioti
Can cryptocurrencies scale?

7 tx/s  
20 tx/s  
65,000 tx/s
Payment Channels
Payment Channels
Payment Channels

Funding transaction

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></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

<table>
<thead>
<tr>
<th>Alice</th>
<th>1</th>
<th>5btc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>1</td>
<td>4btc</td>
</tr>
</tbody>
</table>
Payment Channels

Funding transaction

Alice sends 3btc

Alice
5btc

Bob
4btc

Alice
2btc

Bob
7btc
Payment Channels

Funding transaction

Alice sends 3btc

Bob sends 6btc
Lightning Channels

- Funding
- Commitment
- Dispute period

Revocation
Attack

Funding

Commitment

Dispute period
Why be a Watchtower?
Why be a Watchtower?

Assuming rational parties and watchtowers...

- Will a party commit fraud? ✗
- Will a watchtower get paid? ✗
- Will a party commit fraud? ✓
- Will a watchtower get paid? ✓
- Will a party commit fraud? ...
- Will a watchtower get paid? ✗
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?

## Premiums

<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
Bitcoin

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

Penalty 1
Published by B

Reclaim
Published by W

Collateral
On-chain

σ

a

σAB

a+b

σBW

σ

b

σ

a+b

σBW

σ

σW

σBW

σ

σW

σ

σBW

σ

σW
Cerberus Channels

Funding
On-chain

\[ \#\sigma_A \]
\[ a \]
\[ \#\sigma_B \]
\[ b \]

Commitment
(1)
Published by A

\[ \sigma_{AB} \]
\[ \sigma_A \wedge \Delta t \vee \sigma_{AW} \]
\[ a \]
\[ (\sigma_B \wedge \Delta t) \vee \sigma_{BW} \]
\[ b \]

Commitment
(i)
Published by A

\[ (\sigma_A \wedge \Delta t) \vee \sigma_{AW} \]
\[ a_i \]
\[ (\sigma_B \wedge \Delta t) \vee \sigma_{BW} \]
\[ b_i \]

Revocation
Published by B, W

\[ \sigma_A \wedge \Delta t \vee \sigma_{BW} \]

Commitment
(i+1)
Published by A

\[ (\sigma_A \wedge \Delta t) \vee \sigma_{AW} \]
\[ a_{i+1} \]
\[ (\sigma_B \wedge \Delta t) \vee \sigma_{BW} \]
\[ b_{i+1} \]

Penalty 1
Published by B

\[ \sigma_B \wedge \Delta t \]

Collateral
On-chain

\[ \#\sigma_W \]
\[ c \]

Reclaim
Published by W

\[ \sigma_{BW} \]
\[ c \]

\[ \sigma_{BW} \]
\[ c \]

\[ \sigma_W \]
\[ c \]
Cerberus Channels

Funding
On-chain

Commitment (1)
Published by A

Revocation
Published by B, W

Commitment (i)
Published by A

Penalty 1
Published by B

Commitment (i+1)
Published by A

Penalty 2
Published by B

Collateral
On-chain

Reclaim
Published by W

Fundamentals of Channels
Fundamentals of Channels

Funding

Commitment

Dispute period
Fundamentals of Channels
Time = CryptoMoney!

Asynchronous channels?
Be proactive, not reactive
Be proactive, not reactive
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
Privacy preserving
Alice/Bob cannot publish a previous transaction
Brick Architecture

(1) Update

(2) Consistent Broadcast

(3) Execute
Incentives

 EFFECTS

➔ 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?
