Teechain: Scalable Blockchain Payments using Trusted Execution Environments
Cryptocurrencies

- Most popular: Bitcoin

- Driving technology: Blockchain
  - Peer-to-peer transaction based ledger

- Transactions from and to addresses
The blockchain

- tx1: 1 BTC from A to B
- tx2: 4 BTC from C to D
- tx3: 2 BTC from C to E
- …
- tx255: 0.5 BTC from F to G
- tx256: 1.8 BTC from H to I
- tx257: 2 BTC from C to D
- …
- tx511: 0.8 BTC from F to G
- tx512: 2.5 BTC from H to I
- tx513: 2 BTC from C to D
- …
Shortcomings of Bitcoin

- Not scalable
- High fees
- Environmental issues
- Security vulnerabilities
Payment channels: Setup

Payment Channel

Bob

2 BTC

0 BTC

Alice

Alice gets: 0 BTC
Bob gets: 2 BTC
Payment channels: Payment

Payment Channel

Bob

New Camera

Alice

1.5 BTC

Alice gets: 0 BTC
Bob gets: 2 BTC

Alice gets: 1.5 BTC
Bob gets: 0.5 BTC
Payment channels: Problems

Alice gets: 0 BTC
Bob gets: 2 BTC

Alice gets: 1.5 BTC
Bob gets: 0.5 BTC

Payment Channel

2 BTC
0 BTC
Payment channels: Solutions

- Timelocks
- Lightning network
Teechain payment channels

- Establish trust relationship between users
- Protected channel state until termination
Establishing trust

- Shift root of trust to hardware using trusted execution environments (TEEs)
  - Intel SGX
    - Fully isolated
    - Encrypted memory
    - Remote attestation
Distributed trust
Establishing trust

- Users trust:
  - The blockchain
  - Own TEE (i.e. Intel)
  - Own environment
  - Remote TEE
  - Teechain code
Single channel: Deposit

Bob → TEE

2 BTC

TEE

Alice → TEE
Single channel: Mutual attestation

Bob

Alice

TEE

TEE

2

0

Attestation
Single channel: Opening a channel

Bob

Alice

Channel ID: 42
Public keys

Settlement address: 1F4K...

Settlement address: 1DrH...
Single channel: Deposit approval

Bob  TEE  2

Approve my deposit

Deposit approved

TEE  0  Alice

Approve my deposit
Single channel: Deposit association

Associate Deposit 1

Bob

Private key of Deposit 1

Alice

<table>
<thead>
<tr>
<th>ID</th>
<th>DEPOSIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>42</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>DEPOSIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>42</td>
<td>1</td>
</tr>
</tbody>
</table>
Single channel: Payment

Bob

Pay Alice 1.5 BTC

Bob

TEE

Pay 1.5 BTC

Alice

TEE

<table>
<thead>
<tr>
<th>ID</th>
<th>DEPOSIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>42</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID</th>
<th>DEPOSIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>42</td>
<td>1</td>
</tr>
</tbody>
</table>
Single channel: Settlement
Single channel: Settlement

Bob: 0.5 BTC

Alice: 1.5 BTC

Alice gets: 1.5 BTC
Bob gets: 0.5 BTC

Channel 42

Settle

TEE

TEE

0.5

1.5
Payment chains

- Goals:
  - Atomicity
  - Robustness against nodes ejecting
Payment chains: Lock (1)

- Check:
  - Channel idle
  - Enough funds available

- Create `chainSettleTx`
Payment chains: Sign (2)

- Sign chainSettleTx
Payment chains: PromiseA (3)

- Promise to not settle pre-payment
- Distribute chainSettleTx
Payment chains: PromiseB (4)

- Promise to correctly settle post-payment
- Update internal channel balances to post-payment
Payment chains: Update (5)

- Delete chainSettleTx
Payment chains: Release (6)

- Release the lock
Chain payment atomicity

- PromiseA transitions nodes to post-payment settling
Neutralize channels via chains

Surplus: 2 BTC

Channel difference: 0 BTC
Fault tolerance

- Persistent storage
- Backup chains
# Performance

<table>
<thead>
<tr>
<th>Single channel performance</th>
<th>Throughput (tx/s)</th>
<th>Latency (ms ± stddev)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lightning Network</td>
<td>1’000</td>
<td>387 ± 31</td>
</tr>
<tr>
<td>Teechain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• No fault tolerance</td>
<td>111’000</td>
<td>86 ± 4.4</td>
</tr>
<tr>
<td>• Chain replication</td>
<td>33’000</td>
<td>123 ± 1.2</td>
</tr>
<tr>
<td>• Persistent storage</td>
<td>9.9</td>
<td>185 ± 0.3</td>
</tr>
<tr>
<td>Remote attestation and channel creation</td>
<td>N/A</td>
<td>2’100 ± 420</td>
</tr>
</tbody>
</table>
## Performance

<table>
<thead>
<tr>
<th>Two channel (chain) performance</th>
<th>Latency (ms ± stddev)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lightning Network</td>
<td>0.91 ± 0.115</td>
</tr>
<tr>
<td>Teechain</td>
<td></td>
</tr>
<tr>
<td>• No fault tolerance</td>
<td>2.28 ± 0.10</td>
</tr>
<tr>
<td>• Chain replication</td>
<td>3.3 ± 0.15</td>
</tr>
<tr>
<td>• Persistent storage</td>
<td>3.5 ± 0.11</td>
</tr>
<tr>
<td>UK1 -&gt; UK2 with chain replication</td>
<td>0.22 ± 0.05</td>
</tr>
</tbody>
</table>
Security

- Secure channel setup (Diffie Hellman key exchange)
- Monotonically increasing counters against replay attacks
- Introducing hardware risks
  - Spectre adaptations
  - Side-channel attacks
Limitations

- Hardware constraints
- Performance highly dependent on fault tolerance
- Potential loss of funds