(Technical) Blockchain Issues

Scalability

Privacy
(Anonymity)
(Technical) Blockchain Issues

Scalability

Privacy
(Anonymity)
(Technical) Blockchain Issues

**Scalability**

- Stanford
- MIT
- San Diego
- Berlin

**Privacy** (Anonymity)

- Transaction content
- Metadata (IP address of origin)

Stefanie Roos
Network Layer Anonymity

Mix Rather than Peel Onions
Network Layer Anonymity

Low latency
(<= 2s)

Tor

BITCOIN UPDATES WITH DANDELION:
THE TRANSACTION PRIVACY PROTOCOL

KOVRI
<table>
<thead>
<tr>
<th>Anonymity Protocol</th>
<th>Attack</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (Standard)</td>
<td>Internal attacker</td>
<td>30%</td>
</tr>
<tr>
<td>Low Latency (Tor)</td>
<td>Timing analysis</td>
<td>25%</td>
</tr>
</tbody>
</table>
Mixing

In-coming messages → M → Out-going messages

Encrypt Decrypt Shuffle
Mix Rather than Peel Onions

Mix Networks
## Problem

<table>
<thead>
<tr>
<th>Anonymity Protocol</th>
<th>Attack</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (Standard)</td>
<td>Internal attacker</td>
<td>30%</td>
</tr>
<tr>
<td>Low Latency (Tor)</td>
<td>Timing analysis</td>
<td>25%</td>
</tr>
<tr>
<td>Mixes</td>
<td>Any attack as long as not all mixes are malicious</td>
<td>0%</td>
</tr>
</tbody>
</table>
Mix Rather than Peel Onions

Research Challenges

RQ 1: Attack-resistant Mix Selection
RQ 2: Ensure T Satisfies Constraints

RQ 3: Design Cover Traffic Protocol
RQ 4: Denial of Service Detection
Research Challenges

Mix Rather than Peel Onions

RQ 1: Attack-resistant Mix Selection

RQ 2: Ensure T Satisfies Constraints

RQ 3: Design Cover Traffic Protocol

RQ 4: Denial of Service Detection
Research Challenges

RQ 1: Attack-resistant Mix Selection

RQ 2: Ensure T Satisfies Constraints

RQ 3: Design Cover Traffic Protocol

RQ 4: Denial of Service Detection
Research Challenges

Mix Rather than Peel Onions

RQ 1: Attack-resistant Mix Selection

RQ 2: Ensure T Satisfies Constraints

N1, N2: cover traffic

RQ 3: Design Cover Traffic Protocol

RQ 4: Denial of Service Detection
Research Challenges

- **Honest Malicious**
  - Mix Selection
  - Mixes
  - RQ 1: Attack-resistant Mix Selection

- **tr: transaction; Enc: encrypted**
  - Time T
  - RQ 2: Ensure T Satisfies Constraints

- **Enc(N1), N2: cover traffic**
  - Enc(tr) • S
  - RQ 3: Design Cover Traffic Protocol

- **Drops Claims to forward**
  - RQ 4: Denial of Service Detection

Mix Rather than Peel Onions

Stefanie Roos
Research Challenges

**Honest Malicious**

- **Mix Selection**
- **Mixes**

- **Network**

**RQ 1: Attack-resistant Mix Selection**

- **Enc(N1)**
- **Enc(N2)**

- **S**
- **Enc(tr)**

**N1, N2: cover traffic**

**Time T**

- **tr**
- **Enc(tr)**

**RQ 2: Ensure T Satisfies Constraints**

**RQ 3: Design Cover Traffic Protocol**

**Drops Claims to forward**

**RQ 4: Denial of Service Detection**

Stefanie Roos

Mix Rather than Peel Onions