1. The Ripple Network

The Ripple network is being adopted by banks, cross-border payment services, Bitcoin merchants and many others as their backbone network.

Verifiability is enforced through a public transaction ledger.

Huge Privacy Issues!

3. Linking Wallets: Hot and Cold Wallets

Using the connectivity in the Ripple network, we have defined two novel heuristics to link Ripple wallets controlled by the same user. [1]

![Heuristics to link Ripple wallets controlled by the same user](image)

4. Deanonymizing Ripple Users

Reconstructing gateways business:
- De-anonymized almost 50% payments previously unknown for Bitstamp
- DividendRippler, Dym, Chriswen and Devcoin gateways have the same owner

Deanonymizing our clustered graph:
- 78% total payments in the cluster
- More than $177 million payments volume

<table>
<thead>
<tr>
<th>Heuristic</th>
<th>Ripple</th>
<th>Bitcoin</th>
<th>Altcoins</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>425</td>
<td>64,808</td>
<td>3,113</td>
</tr>
<tr>
<td>H2</td>
<td>323</td>
<td>339,442</td>
<td>-</td>
</tr>
<tr>
<td>H3</td>
<td>2,483</td>
<td>690,878</td>
<td>-</td>
</tr>
<tr>
<td>Grouped</td>
<td>3,166</td>
<td>946,078</td>
<td>3,113</td>
</tr>
</tbody>
</table>

5. Discussion and Future Work

- Detected 68% of the wallets published by the 109 studied gateways
- Results confirmed by Ripple Labs and 2 contacted gateways
- Our work shows a privacy problem in the design of payment networks
- Privacy-preserving payments are necessary [2, 3, 4]
- Further deanonymization possible using a Ripple server:
  - Linking wallets in payments sent from the same IP address

References