CoinJoinXT

...and other techniques for deniable transfers

Adam Gibson
03 July 2018

Building On Bitcoin 2018
Motivation
Intrinsic fungibility and “deniability”

CoinJoinXT
Extending CoinJoin across multiple transactions

CoinJoin Unlimited
Amount correlation, moving off chain

Accompanying blogpost:
https://joinmarket.me/blog/blog/CoinJoinXT
Motivation
Intrinsic fungibility - satoshis are not watermarked
Who owns it?

1 BTC → [ ] → 1 BTC
3 BTC → [ ] → 3 BTC
Who owns it?

A Alice pays Bob 1 coin with 4 coins, Alice gets 3 change
B ”CoinJoin” - Alice pays Alice 1, Bob pays Bob 3
C Alice pays Bob 2 (!) - Alice pays 3, gets 1, Bob pays 1, gets 3
D Alice pays Bob 4 coins (in 2 outputs for some reason)
E Fake payment/Coinjoin - Alice owns everything
F Alice pays Bob 3 coins and Carol 1 coin
G Alice pays 3, Bob pays 1, Carol receives 3, David receives 1
H Alice and Bob pay Carol 4 coins
<table>
<thead>
<tr>
<th>Address</th>
<th>Value</th>
<th>Hash</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>39wm8SnELpi4zAtHYe24baxjBEyReRyMX</td>
<td>1.05644127</td>
<td>3DmWesP1asevJrEEcLZLge77rGchow34X</td>
<td>4.07854025</td>
</tr>
<tr>
<td>3LzejKTTdNHP5meqL4sThuSgMj3Wtsbjt</td>
<td>21.88065811</td>
<td>3Hc53zu8g2mRrKNePcM3YsremQZwWuTC</td>
<td>4.84752911</td>
</tr>
<tr>
<td>3D5WuwpwjsjL48JSf4Pp1Y22tFQaLRpa9MM</td>
<td>4.12342633</td>
<td>3JwpYMCqC9Afx81cSieMzo7Yam2PqykKNs</td>
<td>0.53191735</td>
</tr>
<tr>
<td>3rCKuUM44539UkuB1EadhX4gToirvKLoz</td>
<td>5.26001843</td>
<td>3BUjLDphvq2H1xT3uYHDVD8Ho9PtX84n1z</td>
<td>4.84752911</td>
</tr>
<tr>
<td>3GrDmc16ufavzPrkvM89BPdsYiXWngTfB4</td>
<td>4.80263276</td>
<td>3QaEYvMAKmKjvCFF86C4bwCUQfKHdd2AK</td>
<td>4.84752911</td>
</tr>
<tr>
<td>3PwzUDnuYMJAyktMtau7dH8njuZPmRgtGh</td>
<td>16.45099834</td>
<td>3Gst8CM3DdBnA58VnsWqzTMcM7X9JmxC</td>
<td>4.84752911</td>
</tr>
<tr>
<td>348N9o9j2emYAKLEg1T15nqNQY8aEV2LD</td>
<td>3.28494200</td>
<td>38snZUG6xZmKTozQeY2YWRXkMoatdWnZc</td>
<td>1.04042800</td>
</tr>
<tr>
<td>3Hn27quvML9UrzWYNy5P9474BRRdPmep</td>
<td>2.06865000</td>
<td>3NCm7L8ksDwaVTCG6rUXvUQc6Pgf7CLVA</td>
<td>11.60442874</td>
</tr>
<tr>
<td>39EMyYYknNmFTHrQWV6RPbne8JEUeo1XqQd</td>
<td>5.37895254</td>
<td>31y7aHKwsYvhS8ch1v11wkwq5gmsu6vG9TJ</td>
<td>1.05470391</td>
</tr>
<tr>
<td>3DRtDd2me3sjfueLnudsNJt6mewFuyR4v</td>
<td>2.26889400</td>
<td>33rWLLfsqiqwK6V1W3hNabgbipDst4s4g</td>
<td>4.84752911</td>
</tr>
<tr>
<td>3H2Ftm9gV29oMh2ETxzk5pQySWibdhmEre</td>
<td>3.77635630</td>
<td>39AoHxs532PdvugU8woXbf6nJznWNGCKPM</td>
<td>0.70157946</td>
</tr>
<tr>
<td>3SP16gukH5hnU8Gxbz4aNDLGVTK3BCfjS</td>
<td>2.76263316</td>
<td>3CmNVMsDcGQPnJ9cmeLd2y8oZmA2Tcc9y</td>
<td>4.84752911</td>
</tr>
<tr>
<td>38974ZhPnQBUNDEKRs4LwJw9ts6PEPZzE</td>
<td>2.12491721</td>
<td>3CPHLYW5SSma6XYn6xFK6Z2KHFyest</td>
<td>4.84752911</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3A67UJM8c8ZcfPsfY9FXUp8jsNqkts7o8T</td>
<td>0.41343815</td>
</tr>
<tr>
<td></td>
<td></td>
<td>32xTw7Qkb6CZvkdGJaSi92HYQmc94x36G</td>
<td>4.84752911</td>
</tr>
<tr>
<td></td>
<td></td>
<td>36qZzCAeUbdMfiXGS88nA4ux85FE9E1SM</td>
<td>17.03402579</td>
</tr>
</tbody>
</table>
Heuristic 1
All inputs are co-owned.\(^1\)

Heuristic 2
One-time use change addresses (and other change-related)
Heuristic 0
Each utxo is unilaterally controlled.

Heuristic 1
All inputs are co-owned.¹

Heuristic 2
One-time use change addresses (and other change-related)
Heuristic 0
Each utxo is unilaterally controlled.

Heuristic 1
All inputs are co-owned.¹

Heuristic 2
One-time use change addresses (and other change-related)

Heuristic 3
Transfer of control/ownership in one transaction implies payment
CoinJoinXT
CoinJoinXT - simplest case

Sign first transaction last; we can do better!
CoinJoinXT - simplest case

Sign first transaction last; we can do better!
CoinJoinXT - add a promise

Bob takes no risk of funds loss in case Alice double spends A1.
CoinJoinXT - example

Boundary may be unclear to attacker
CoinJoin Unlimited
CJXT still suffers from amount correlation in simplest form
• CJXT still suffers from amount correlation in simplest form
• Subset sum (exponential time? but not really)
Amount correlation problem

- CJXT still suffers from amount correlation in simplest form
- Subset sum (exponential time? but not really)
- Another approach - combine with
Decorrelation via funding

Proposed Transaction Graph

5.8 BTC
1.2 BTC

4.6 BTC

3.7 BTC

2.9 BTC

6.6 BTC

(0.3BTC, 1.2BTC)

1.5 BTC

5.5 BTC

5.4 BTC
Decorrelation via funding

No valid subsets at funding time
Decorrelation via funding

No valid subsets at funding time
Even *after* close, no subsets if spending off-chain occurred
Thank you

Blog post on this topic: https://joinmarket.me/blog/blog/CoinJoinXT

Contact info:

waxwing (freenode IRC, reddit)
@waxwing__ (twitter)
https://github.com/AdamISZ

gpg: 4668 9728 A9F6 4B39 1FA8 71B7 B3AE 09F1 E9A3 197A
References
References

1. Meiklejohn et al ”A Fistful of Bitcoins”:

2. CoinJoin, Greg Maxwell:
   https://bitcointalk.org/index.php?topic=279249.0

3. BIP141 note on tx chains:

4. Generic off-chain protocol patterns
   https://zmnsclpxj.github.io/offchain/generalized.html

5. On-chain contracting for privacy
   https://gist.github.com/AdamISZ/a5b3fcdd8de4575dbb8e5fba8a9bd88c

6. Simple CoinJoinXT example code
   https://github.com/AdamISZ/CoinJoinXT-POC