CoinJoinXT

...and other techiques for deniable transfers

Adam Gibson

03 July 2018

Building On Bitcoin 2018

Outline

Motivation

Intrinsic fungibility and “deniability”

CoinJoinXT

Extending CoinJoin across multiple transactions

CoinJoin Unlimited

Amount correlation, moving off chain

Accompanying blogpost:

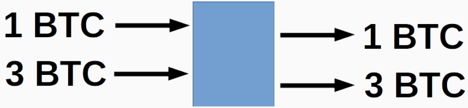
https://joinmarket.me/blog/blog/CoinJoinXT

Motivation

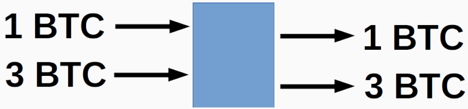
Fungible?

Intrinsic fungibility - satoshis are not watermarked

Who owns it?



Who owns it?



1 BTC

3 BTC

1 BTC

3 BTC

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)

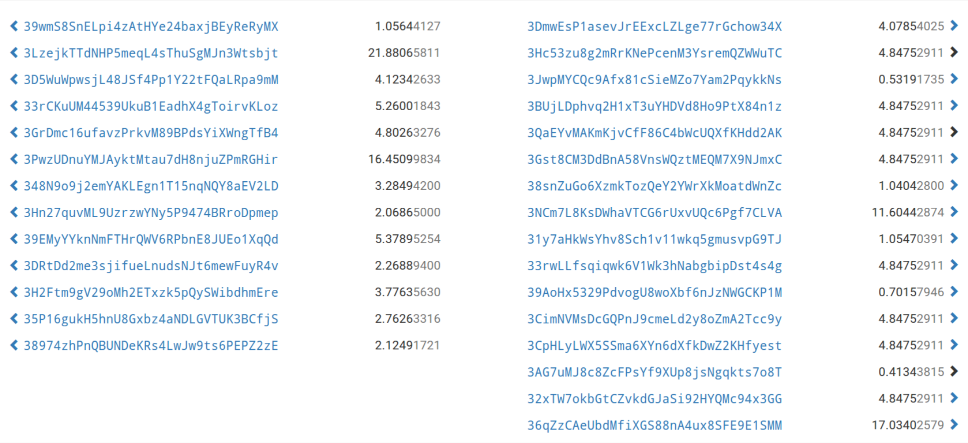
E Fake payment/Coinjoin - Alice owns everything

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

CoinJoin today[2]



39wmS8SnELpi4zAtHYe24baxjBEyReRyMX	1.05644127	3DmwEsP1asevJrEExcLZLge77rGchow34X	4.07854025
3LzejkTTdNHP5meqL4sThuSgMJn3Wtsbjt	21.88065811	3Hc53zu8g2mRrKNePcenM3YsremQZWWuTC	4.84752911
3D5WuWpwsjL48JSf4Pp1Y22tFQaLRpa9mM	4.12342633	3JwpMYCQc9Afx81cSieMZo7Yam2PqykkNs	0.53191735
33rCKuUM44539UkuB1EadhX4gToirvKLoz	5.26001843	3BUjLDphvq2H1xT3uYHDVd8Ho9PtX84n1z	4.84752911
3GrDmc16ufavzPrkvM89BPdsYiXWngTfB4	4.80263276	3QaEYvMAKmKjvCfF86C4bWcUQXfKHdd2AK	4.84752911
3PwzUDnuYMJAyktMtau7dH8njuZPmRGHir	16.45099834	3Gst8CM3DdBnA58VnsWQztMEQM7X9NJmxC	4.84752911
348N9o9j2emYAKLEgn1T15nqNQY8aEV2LD	3.28494200	38snZuGo6XzmkTozQeY2YWrXkMoatdWnZc	1.04042800
3Hn27quvML9UzrzwYNy5P9474BRroDpmep	2.06865000	3NCm7L8KsDWhaVTCG6rUxvUQc6Pgf7CLVA	11.60442874
39EMyYYknNmFTHrQWV6RPbnE8JUEo1XqQd	5.37895254	31y7aHkWsYhv8Sch1v11wkq5gmusvpG9TJ	1.05470391
3DRtDd2me3sjifueLnudsNJt6mewFuyR4v	2.26889400	33rwLLfsqiqwk6V1Wk3hNabgbipDst4s4g	4.84752911
3H2Ftm9gV29oMh2ETxzk5pQySWibdhmEre	3.77635630	39AoHx5329PdvogU8woXbf6nJzNWGCKP1M	0.70157946
35P16gukH5hnU8Gxbz4aNDLGVTUK3BCfjS	2.76263316	3CimNVMsDcGQPnJ9cmeLd2y8oZmA2Tcc9y	4.84752911
38974zhPnQBUNDeKRs4LwJw9ts6PEPZ2zE	2.12491721	3CpHLyLWX5SSma6XYn6dXfkDwZ2KHfyest	4.84752911
		3AG7uMJ8c8ZcFPsYf9XUp8jsNgqkts7o8T	0.41343815
		32xTW7okbGtCZvkdGJaSi92HYQMc94x3GG	4.84752911
		36qZzCAeUbdMfiXGS88nA4ux8SFE9E1SMM	17.03402579

Blockchain Analysis Heuristics

Heuristic 1

All inputs are co-owned.[1]

Heuristic 2

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

Blockchain Analysis Heuristics

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)

Blockchain Analysis Heuristics

Heuristic 0

Each utxo is unilaterally controlled.

Heuristic 1

All inputs are co-owned.[1]

Heuristic 2

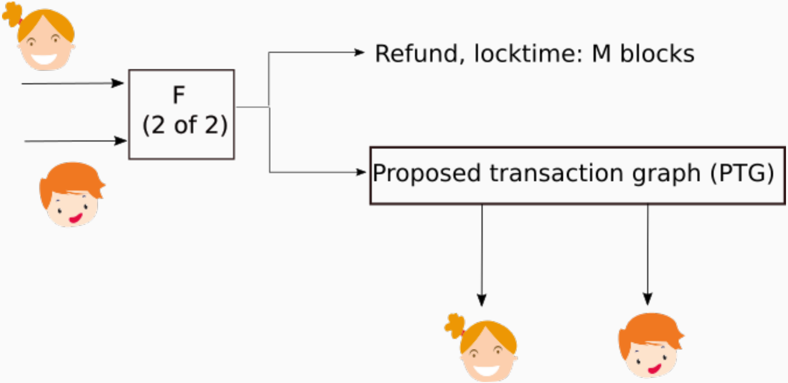
One-time use change addresses (and other change-related)

Heuristic 3

Transfer of control/ownership in one transaction implies payment

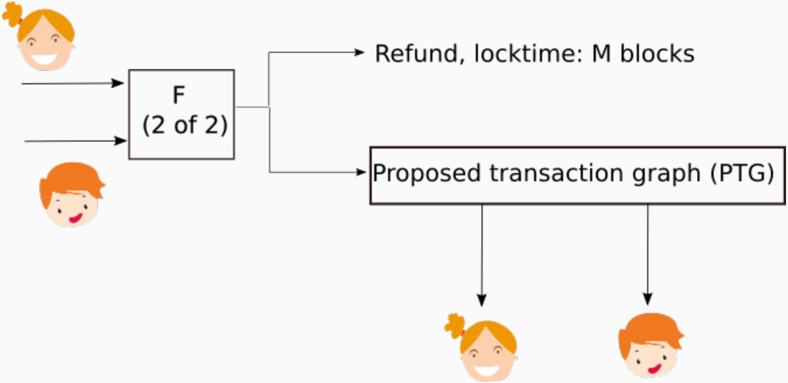
CoinJoinXT

CoinJoinXT - simplest case



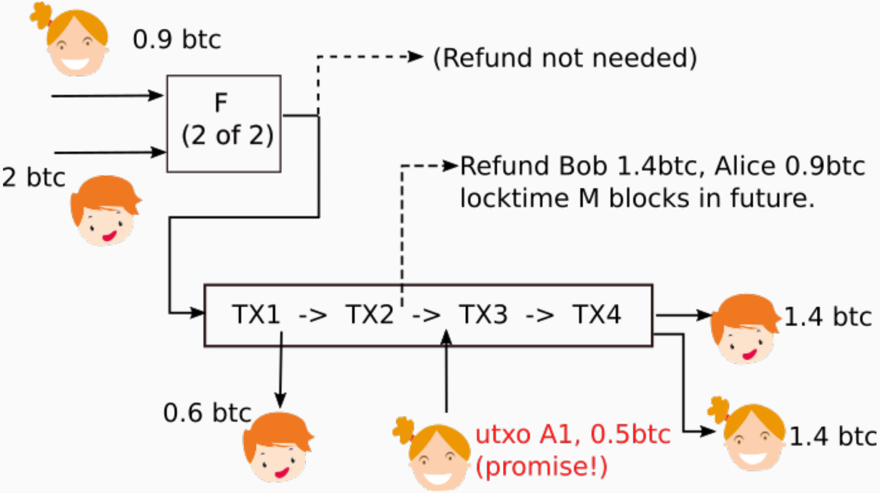
Sign first transaction last; we can do better!

CoinJoinXT - simplest case



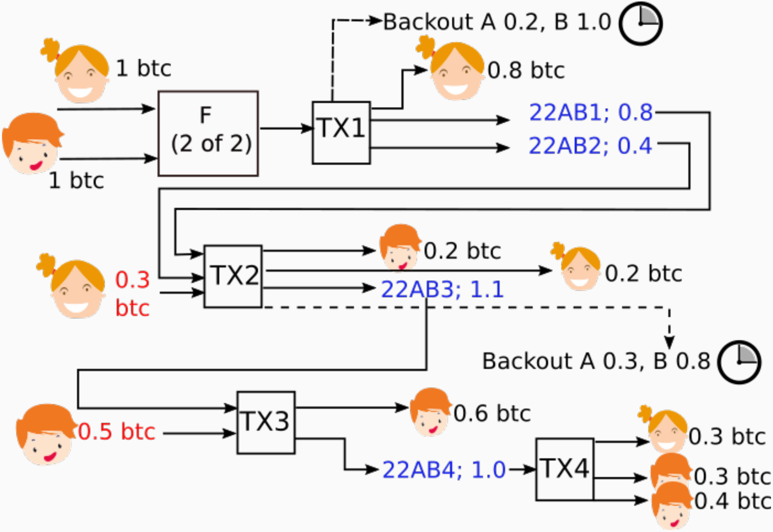
Sign first transaction last; we can do better!

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

Amount correlation problem

- CJXT still suffers from amount correlation in simplest form

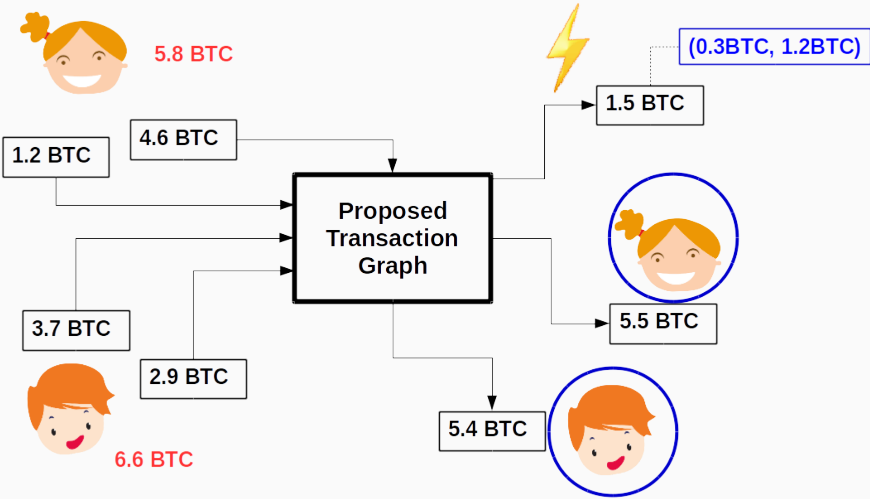
Amount correlation problem

- CJXT still suffers from amount correlation in simplest form
- Subset sum (exponential time? but not really)

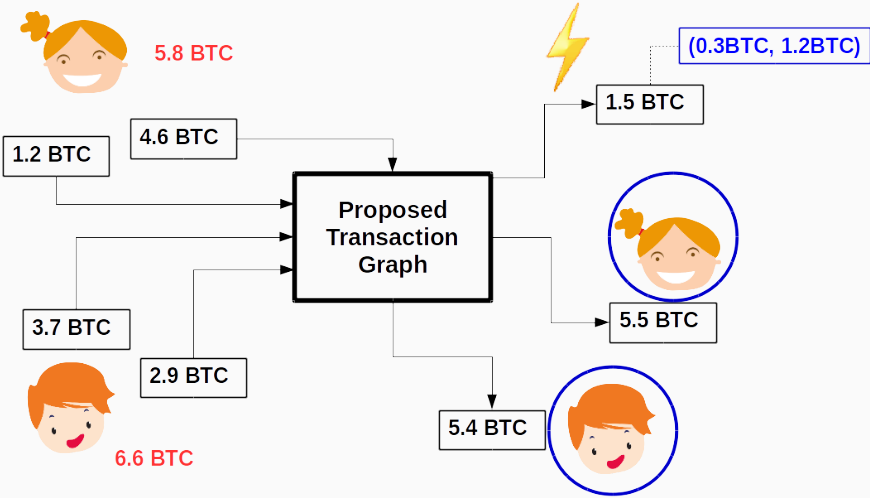
Amount correlation problem

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

Decorrelation via funding

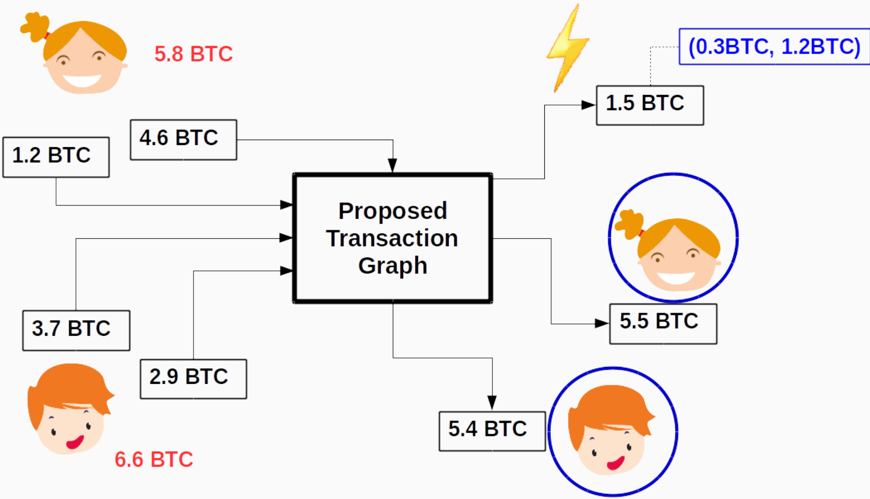


Decorrelation via funding



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": https://cseweb.ucsd.edu/ smeiklejohn/files/imc13.pdf
2. CoinJoin, Greg Maxwell: https://bitcointalk.org/index.php?topic=279249.0
3. BIP141 note on tx chains: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki#trust-free-unconfirmed-transaction-dependency-chain
4. Generic off-chain protocol patterns https://zmnscpxj.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