CS1699: Blockchain Technology and Cryptocurrency

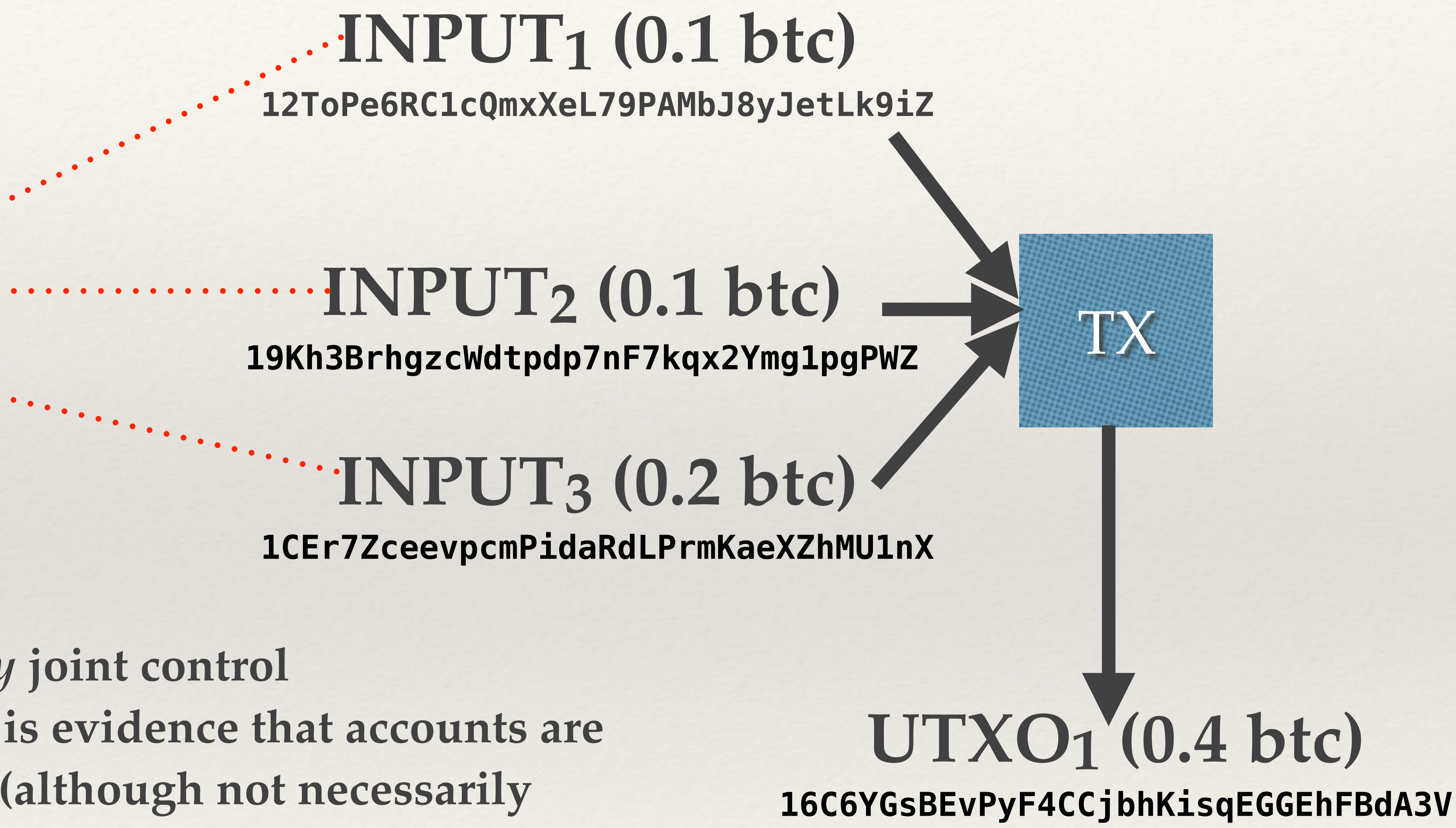
13. Improving the Anonymity of Bitcoin

Bill Laboon

Previously…

- Bitcoin is pseudonymous, NOT anonymous
- Operating under the assumption that anonymity is good (*anonymity* = *pseudonymity* + *unlinkability*)
- Trivial for anyone to follow transactions
- Steps can be taken to improve anonymity!

Linking



INPUT$_1$ (0.1 btc)

12ToPe6RC1cQmxXeL79PAMbJ8yJetLk9iZ

INPUT$_2$ (0.1 btc)

19Kh3BrhgzcWdtpdp7nF7kqx2Ymg1pgPWZ

INPUT$_3$ (0.2 btc)

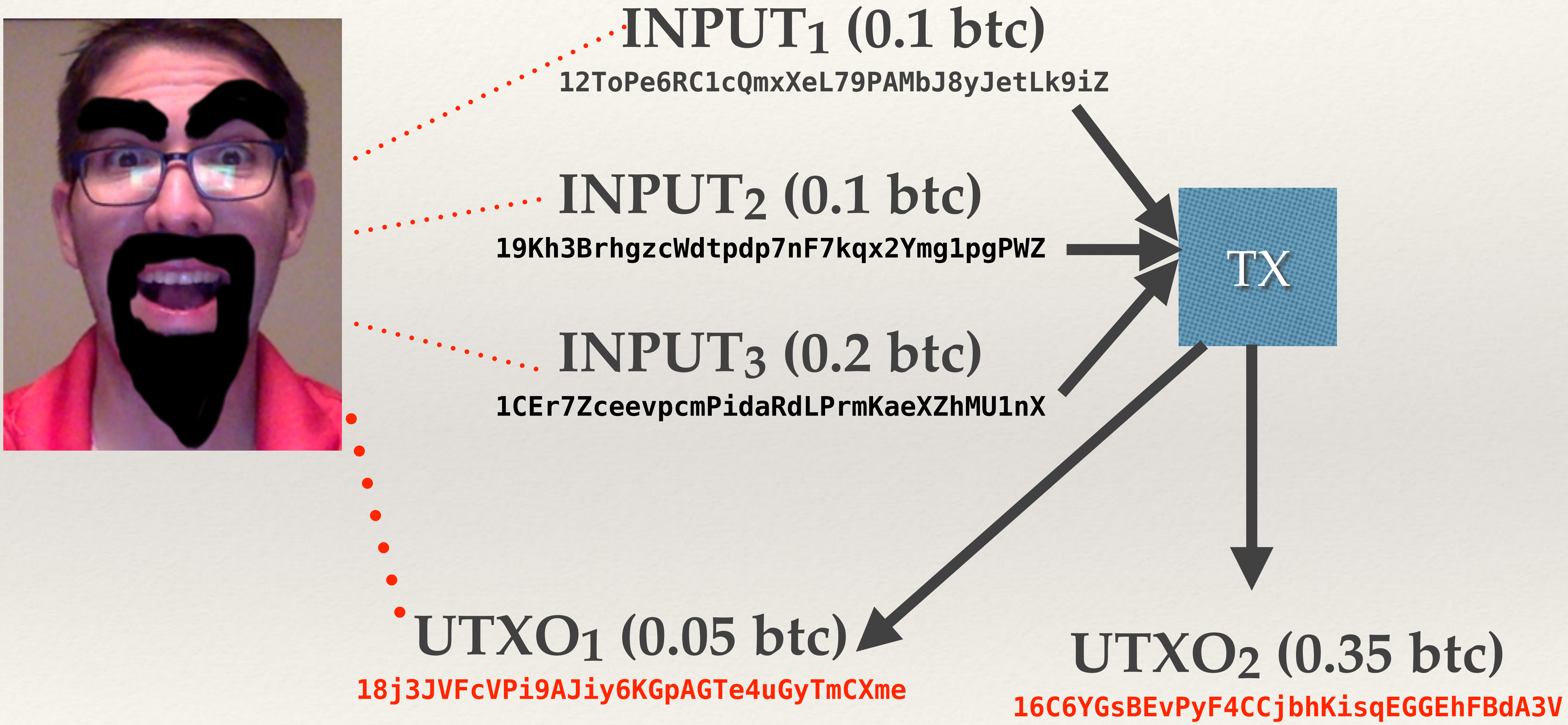
1CEr7ZceevpcmPidaRdLPrmKaeXZhMU1nX

UTXO$_1$ (0.4 btc)

16C6YGsBEvPyF4CCjbhKisqEGGEhFBdA3V

Joint inputs *imply* joint control
Shared spending is evidence that accounts are somehow linked (although not necessarily the same same person)

Linking - Change Addresses



INPUT$_1$ (0.1 btc)

12ToPe6RC1cQmxXeL79PAMbJ8yJetLk9iZ

INPUT$_2$ (0.1 btc)

19Kh3BrhgzcWdtpdp7nF7kqx2Ymg1pgPWZ

INPUT$_3$ (0.2 btc)

1CEr7ZceevpcmPidaRdLPrmKaeXZhMU1nX

TX

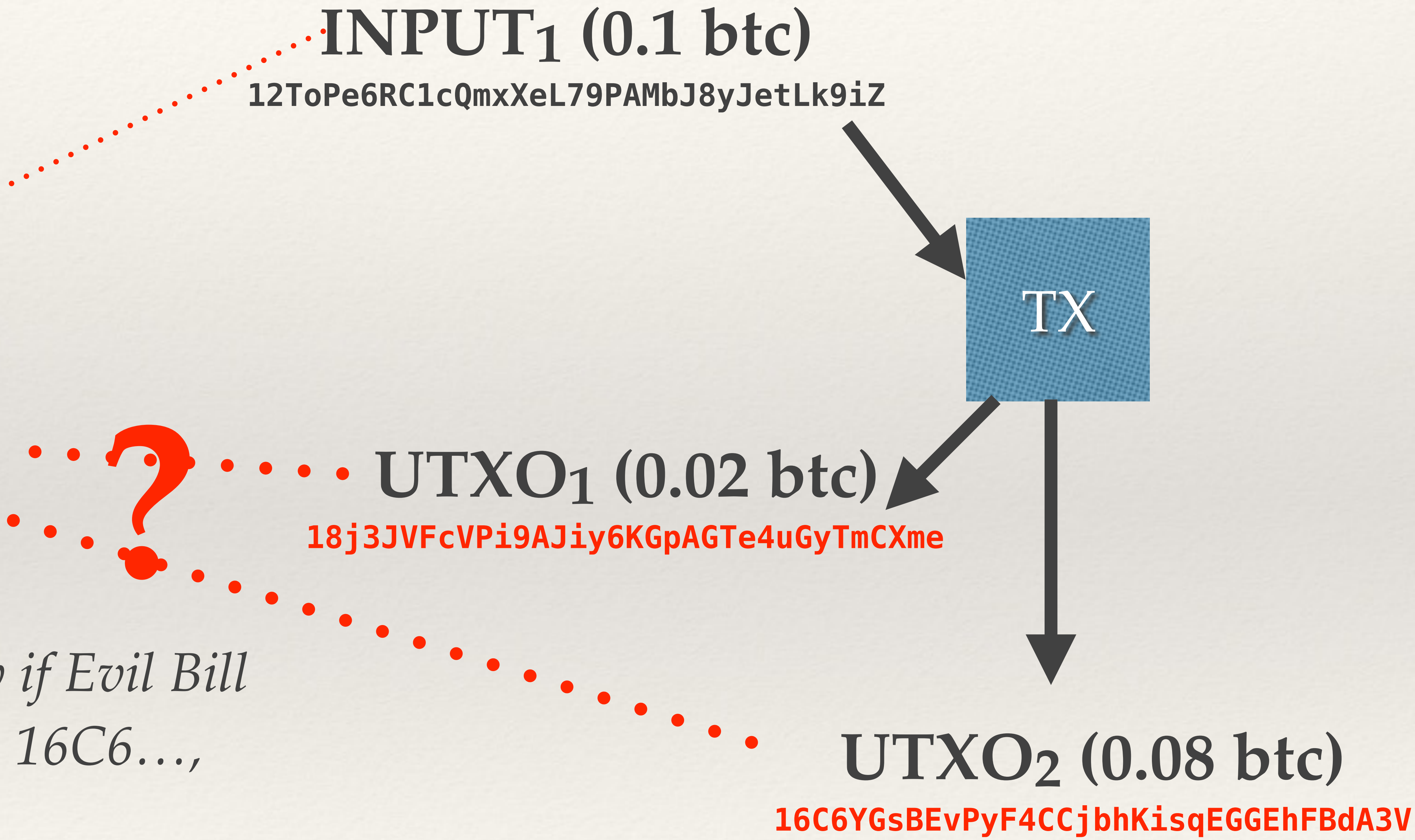
UTXO$_1$ (0.05 btc)

18j3JVFcVPi9AJiy6KGpAGTe4uGyTmCXme

UTXO$_2$ (0.35 btc)

16C6YGsBEvPyF4CCjbhKisqEGGEhFBdA3V

0.08 BTC or 0.02 BTC Payment?



INPUT$_1$ (0.1 btc)

12ToPe6RC1cQmxXeL79PAMbJ8yJetLk9iZ

TX

?

UTXO$_1$ (0.02 btc)

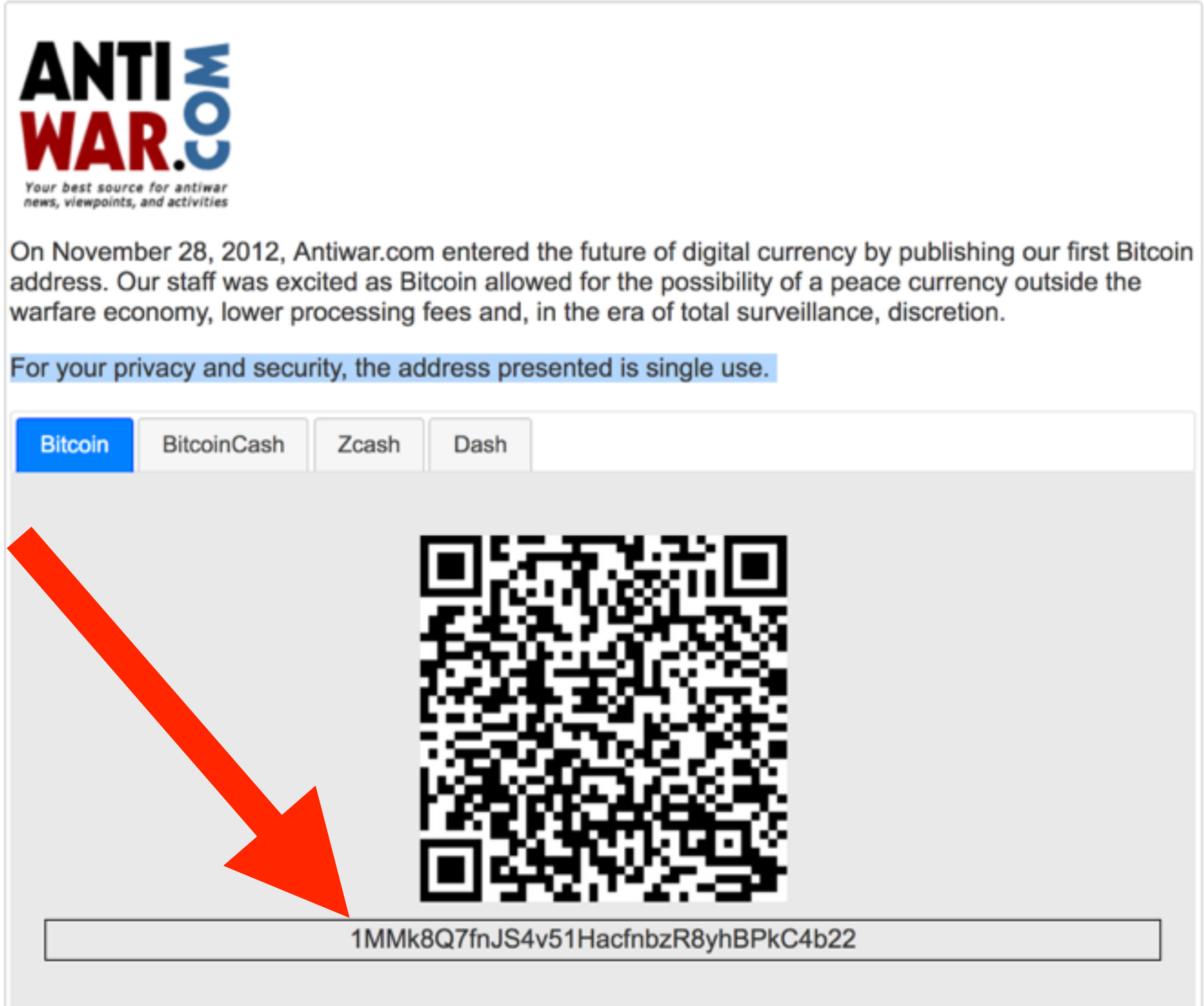
18j3JVFcVPi9AJiy6KGpAGTe4uGyTmCXme

UTXO$_2$ (0.08 btc)

16C6YGsBEvPyF4CCjbhKisqEGGEhFBdA3V

No way to know if Evil Bill controls 18j3…, 16C6…, both, or neither!

Avoid Address Re-Use



ANTI WAR.COM
Your best source for antiwar news, viewpoints, and activities

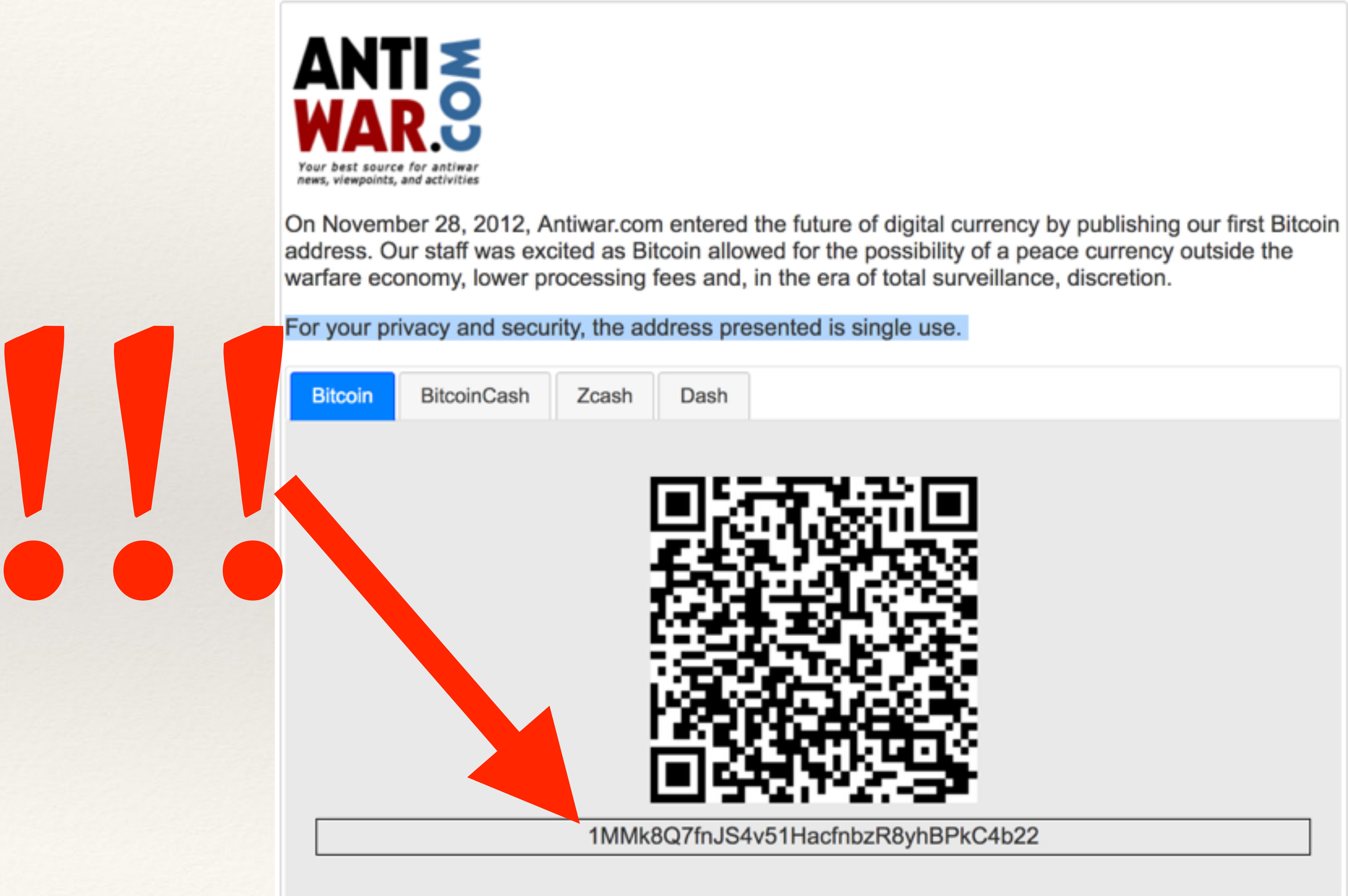
On November 28, 2012, Antiwar.com entered the future of digital currency by publishing our first Bitcoin address. Our staff was excited as Bitcoin allowed for the possibility of a peace currency outside the warfare economy, lower processing fees and, in the era of total surveillance, discretion.

For your privacy and security, the address presented is single use.

Bitcoin
BitcoinCash
Zcash
Dash

1MMk8Q7fnJS4v51HacfnbzR8yhBPkC4b22

Avoid Address Re-Use



ANTI WAR.COM

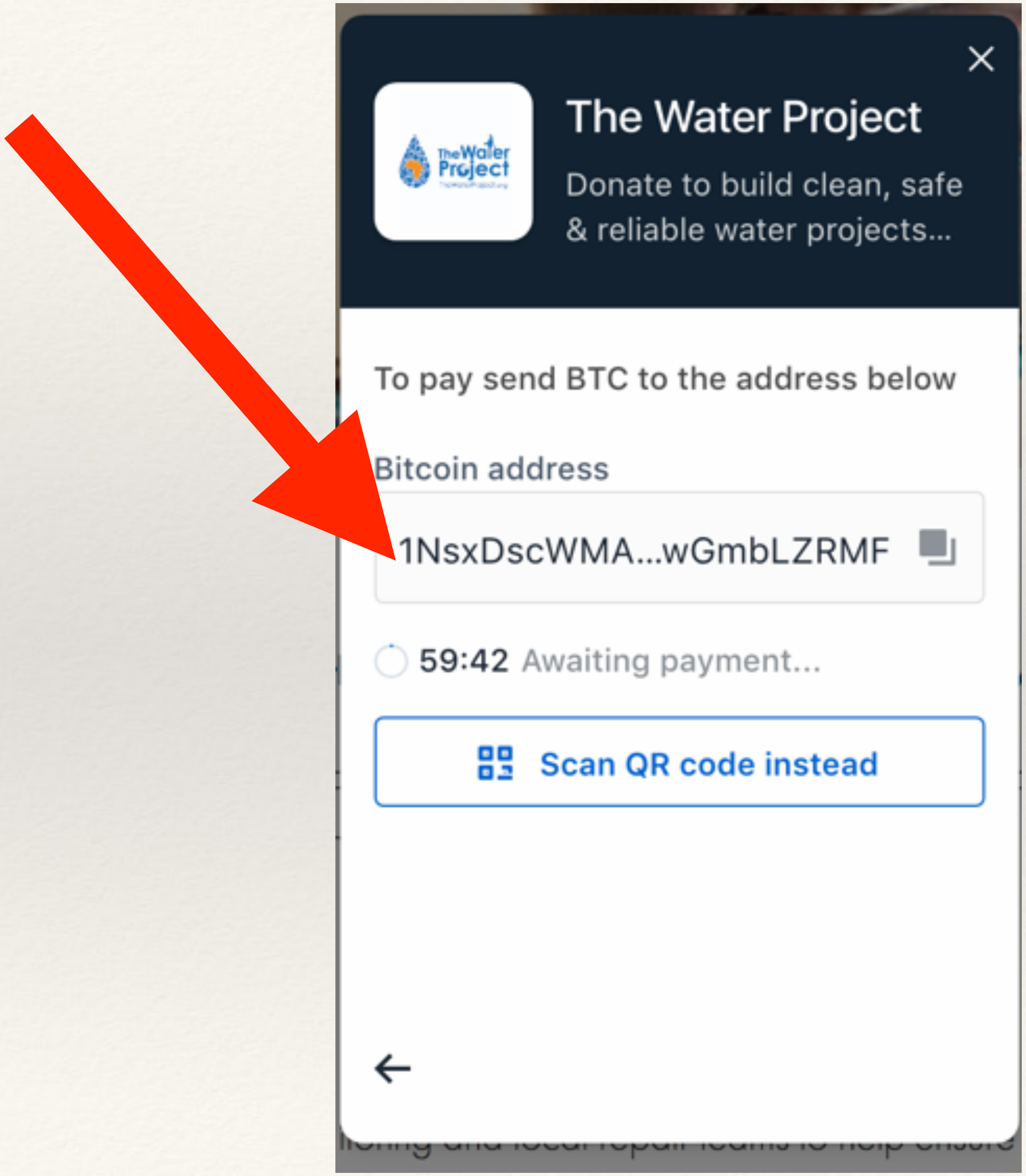
Your best source for antiwar news, viewpoints, and activities

On November 28, 2012, Antiwar.com entered the future of digital currency by publishing our first Bitcoin address. Our staff was excited as Bitcoin allowed for the possibility of a peace currency outside the warfare economy, lower processing fees and, in the era of total surveillance, discretion.

For your privacy and security, the address presented is single use.

1MMk8Q7fnJS4v51HacfnbzR8yhBPkC4b22

Avoid Address Re-Use



The Water Project

Donate to build clean, safe & reliable water projects...

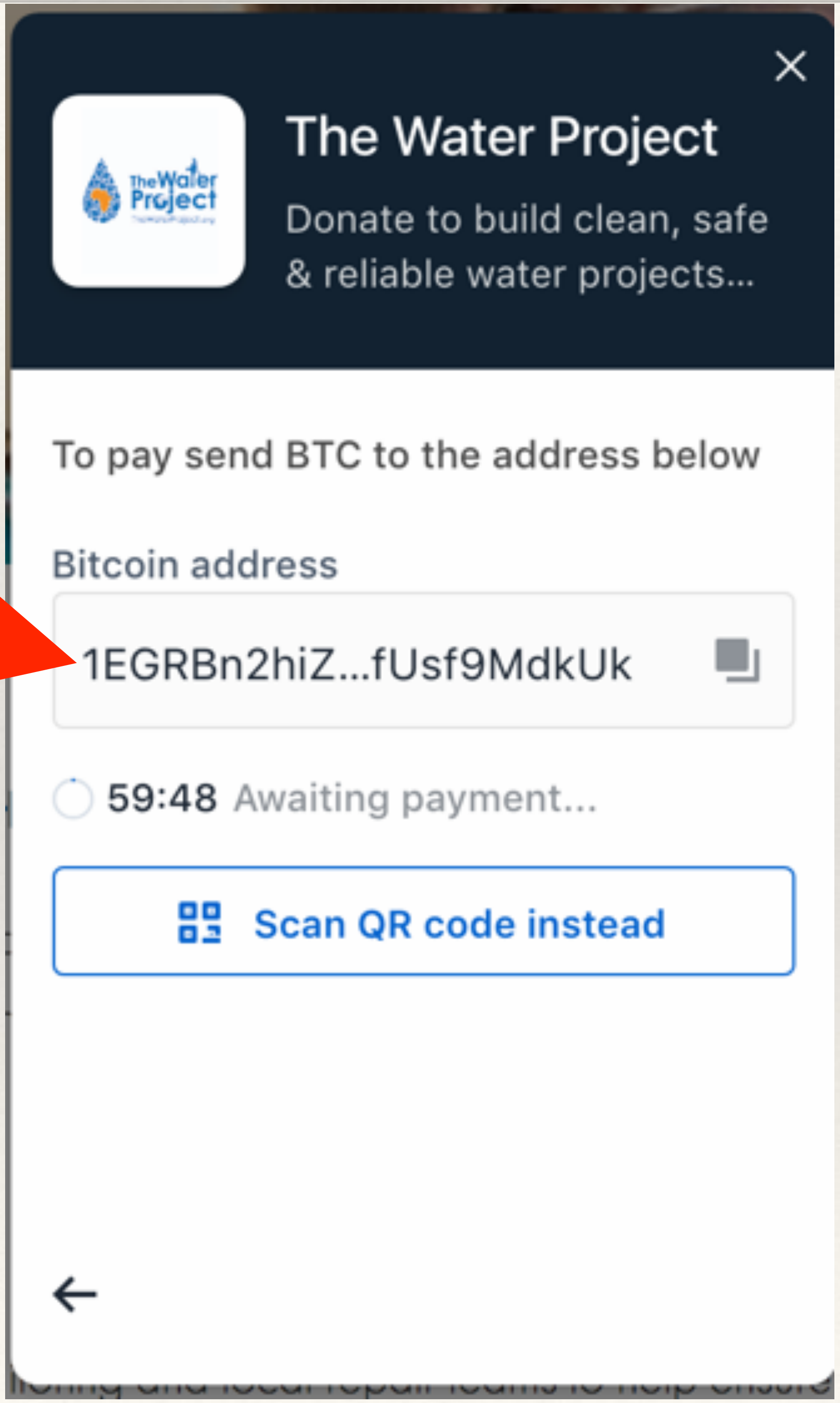
To pay send BTC to the address below

Bitcoin address

1NsxDscWMA...wGmbLZRMF

59:42 Awaiting payment...

Avoid Address Re-Use



The Water Project

Donate to build clean, safe & reliable water projects...

To pay send BTC to the address below

Bitcoin address

1EGRBn2hiZ...fUsf9MdkUk

59:48 Awaiting payment...

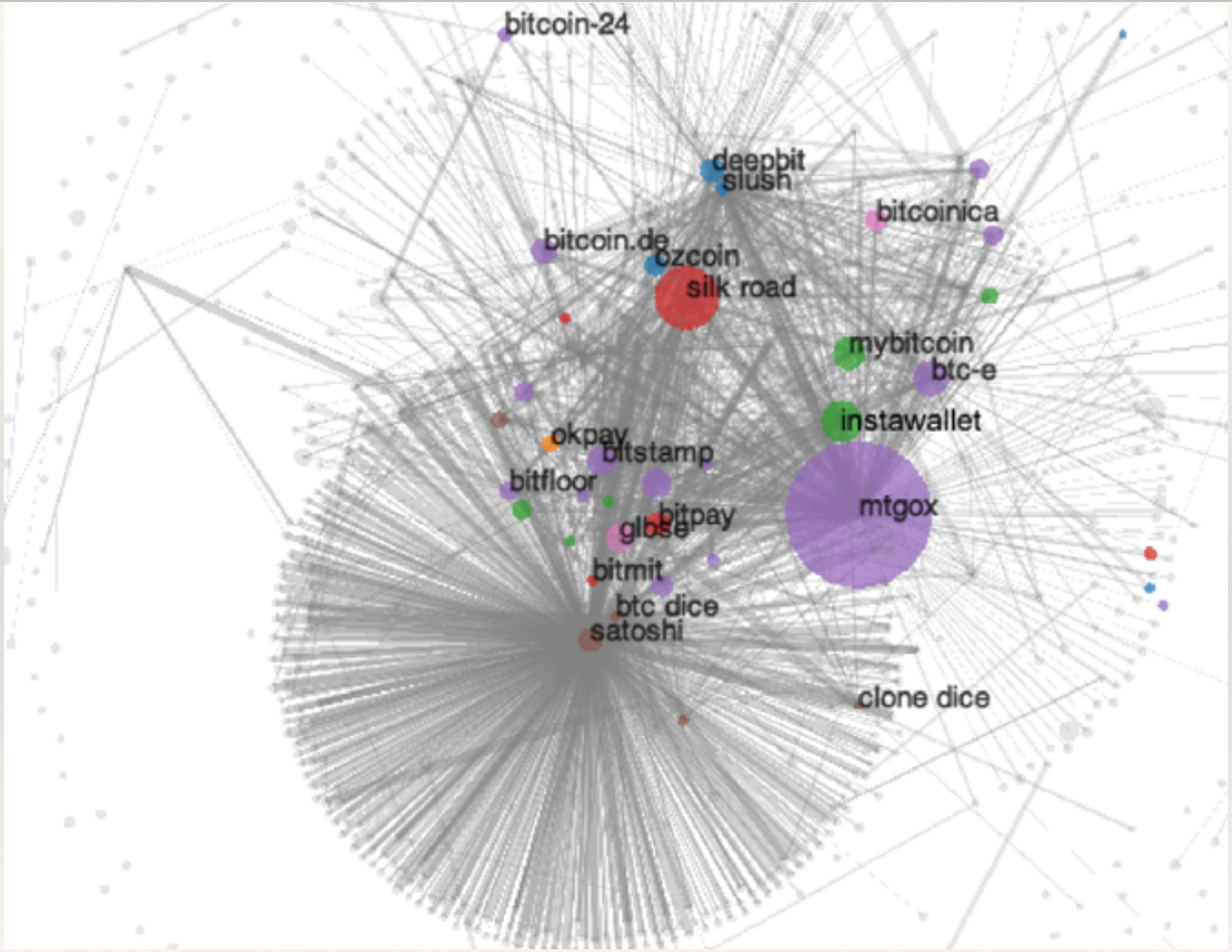
Idioms of Use

- Change addresses tend to be fresh addresses
- Shared spending implies a single identity
- Verification via re-identification attacks
- See paper: Reid and Harrigan's "An Analysis of Anonymity in the Bitcoin System" https://arxiv.org/pdf/1107.4524.pdf
- See paper: Seikeljohn *et al.* , "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names" https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf

Real-World IDs : TXs/Addresses

- If you can *link* part of a cluster to a real-world identity, you now know *much* more about that cluster and that real-world identity!
- Ways to do it:
  - Directly transacting.
  - Via service providers.
  - Carelessness (posting address in forum)
- Note: Anonymization tends to get worse over time (as researchers discover better deanonymization techniques)

Transaction Graph Analysis



"[B]lue nodes are mining pools; orange are fixed-rate exchanges; green are wallets; red are vendors; purple are (bank) exchanges; brown are gambling; pink are investment schemes; and grey are uncategorized." -Seikeljohn 2013

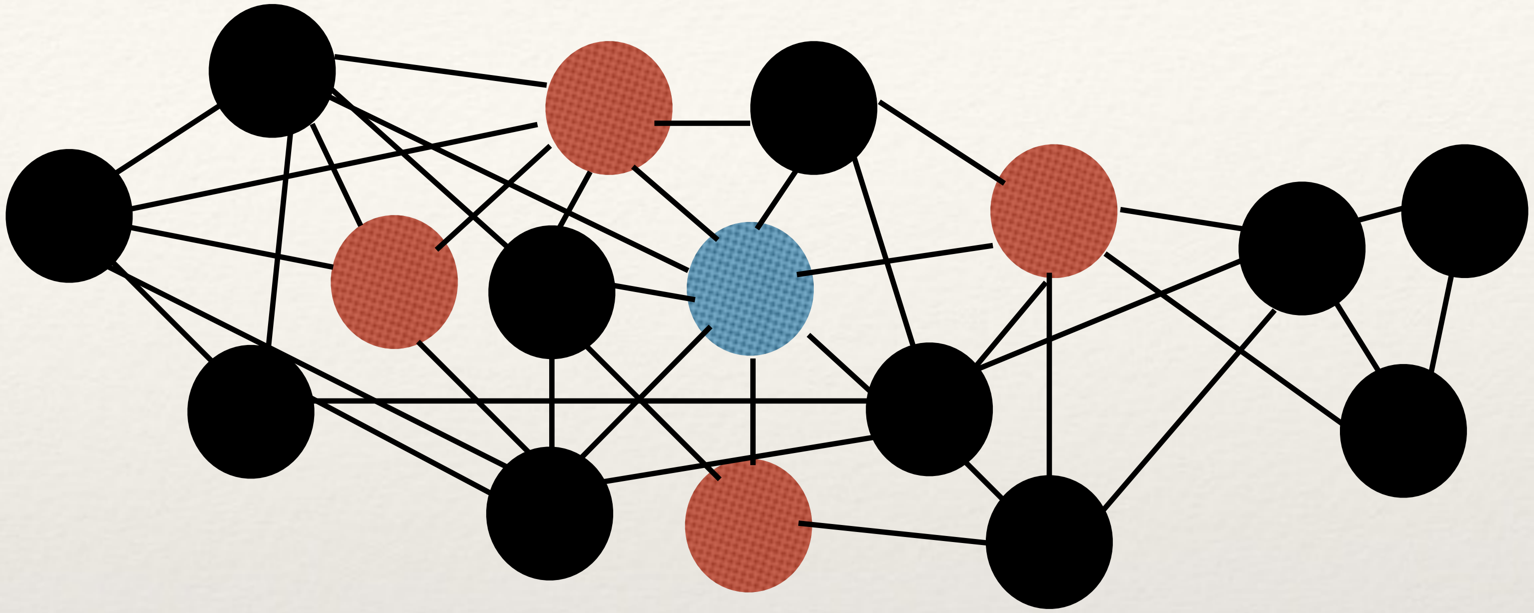
Network-Level Deanonymization

- We have seen how we can use the blockchain to create a transaction graph and analyze it in order to deanonymize
- But we can also use the Bitcoin network itself!
- Seminal work here was done by Dan Kaminsky at Black Hat 2011 in his talk “Black Ops of TCP/IP”. See slide deck here https://www.slideshare.net/dakami/black-ops-of-tcpip-2011-black-hat-usa-2011

Nuts and Bolts of Network-Level Deanonymization

Red = spies

Blue = tx source



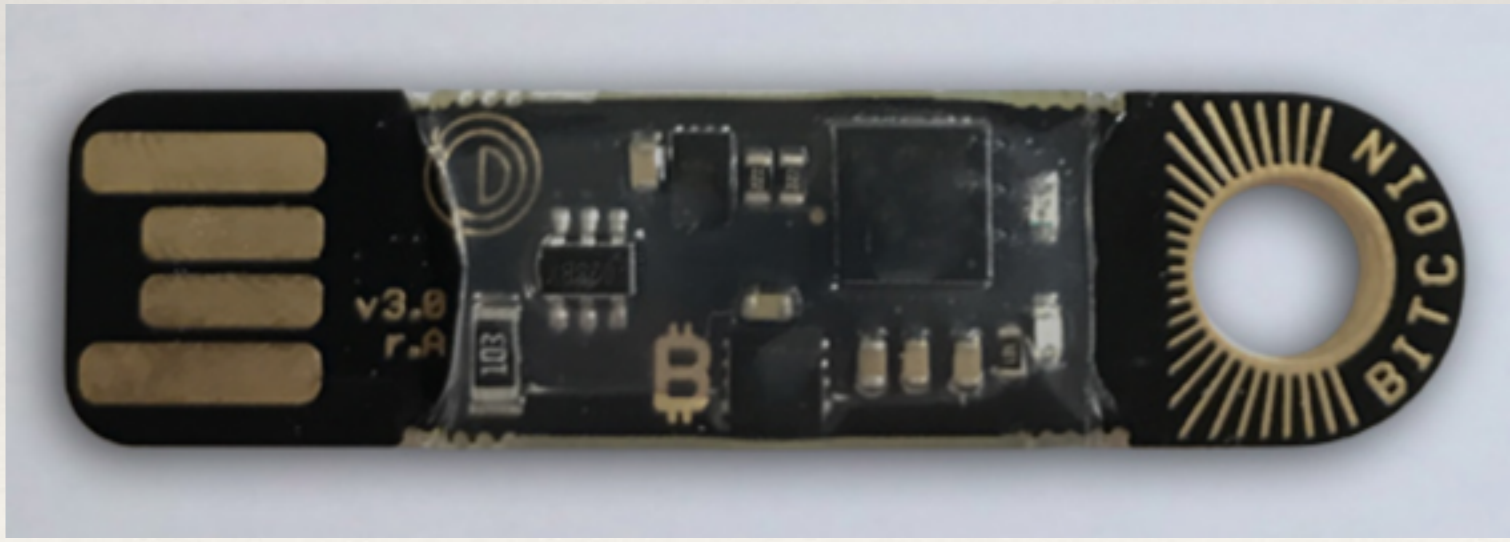
"[T]he first node to inform you of a transaction is probably the source of it." -Kaminsky

Avoiding Network-Level Deanonymization

- Need to hide your IP (using Tor or similar service)
- However, Tor:
  - Can be blocked (see Biryukov *et al.*, "Deanonymisation of clients in Bitcoin P2P network")
  - Is very slow and not well-suited to running on the Bitcoin network

Offline Transfers

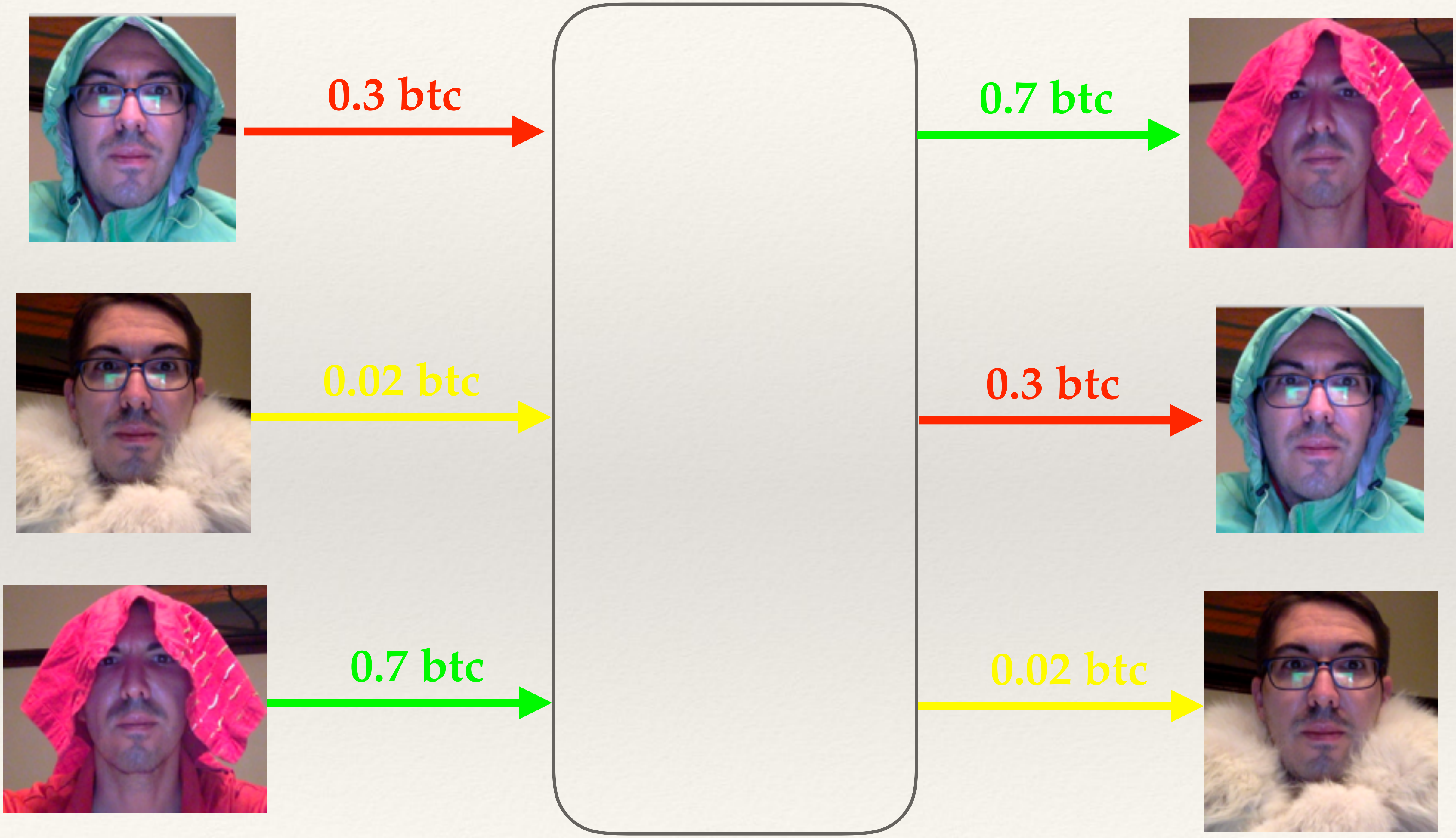
- Harder, but possible!
- See OpenDime



Mixers

- Want to improve anonymity, need to improve anonymity set
- Exchanges are theoretically good, but often have KYC or other requirements
- Dedicated mixing services

Transaction Should Be Equal



0.3 btc

0.02 btc

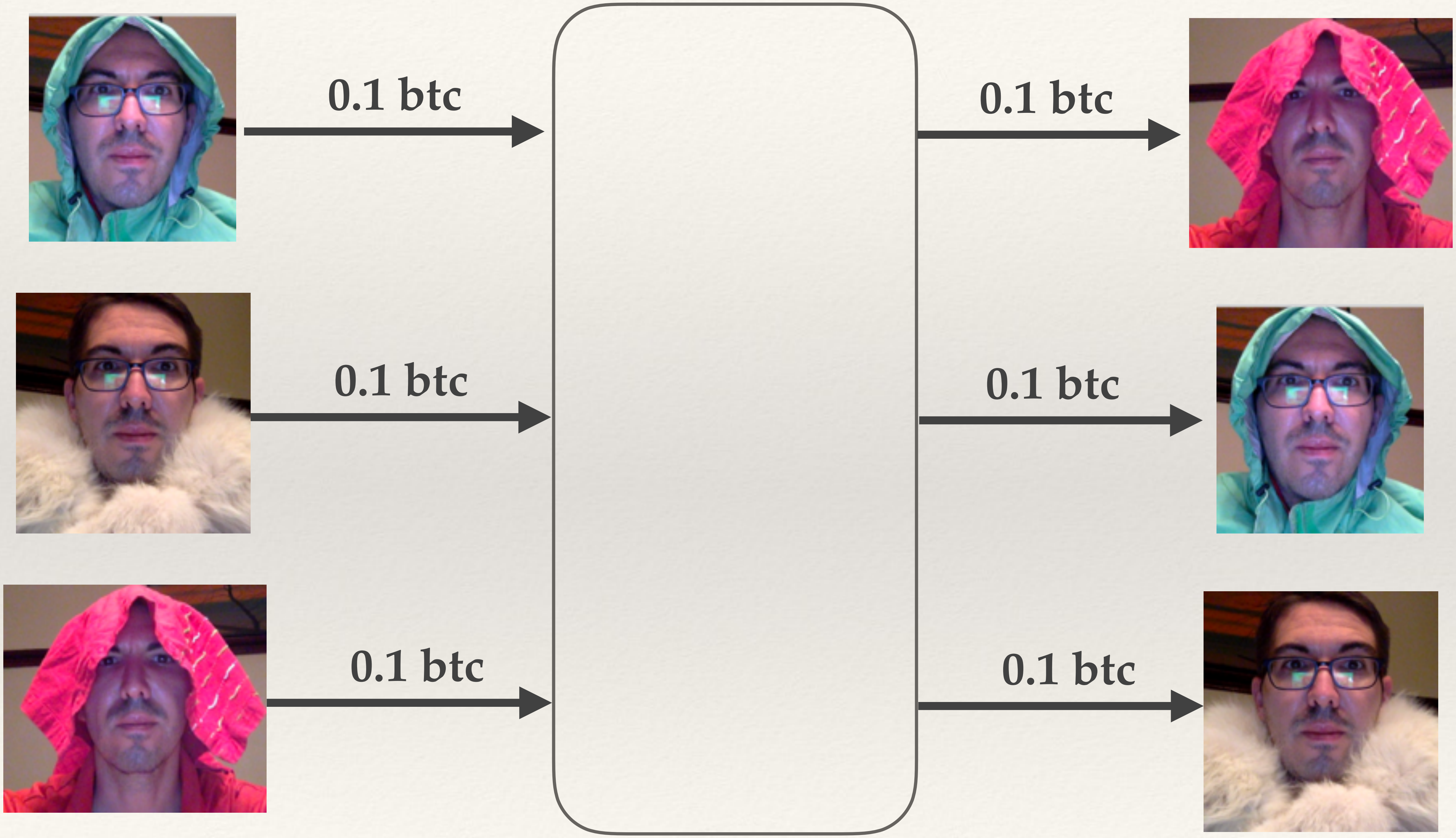
0.7 btc

0.7 btc

0.3 btc

0.02 btc

Mixer, Chunk Size = 0.1 btc



0.1 btc

0.1 btc

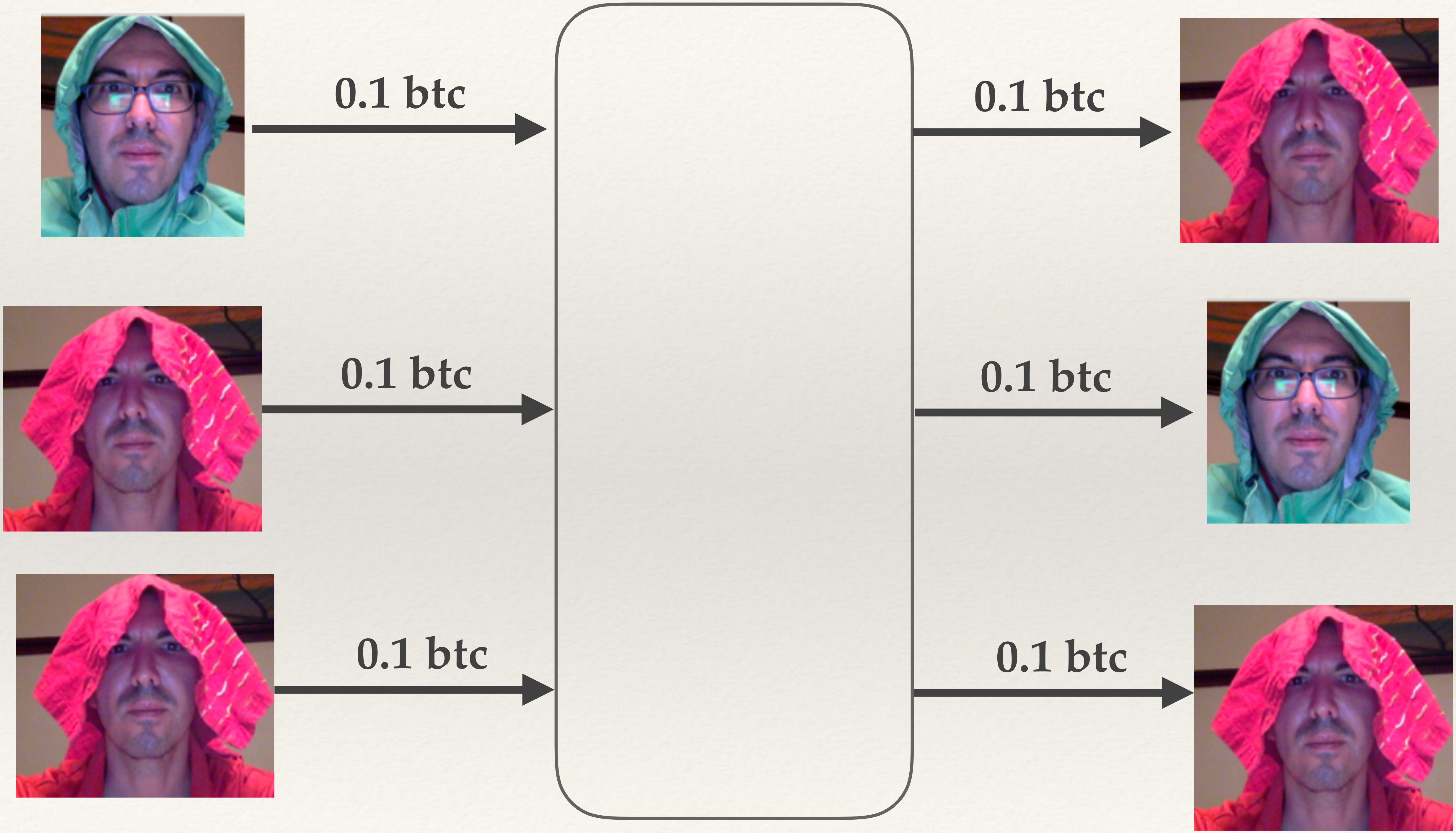
0.1 btc

0.1 btc

0.1 btc

0.1 btc

Chunk Size Optimization



0.1 btc

0.1 btc

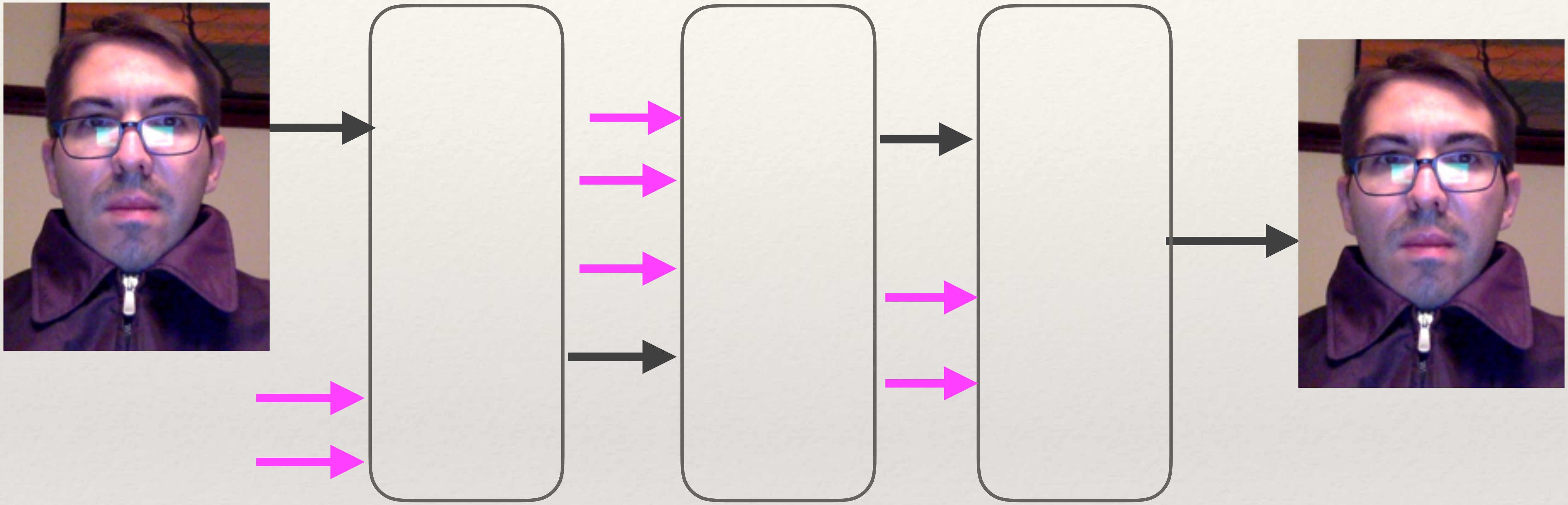
0.1 btc

0.1 btc

0.1 btc

0.1 btc

Multi-Mix



→ Jacket Bill’s bitcoin

→ Other people’s bitcoin

Should You Trust a Mixer?

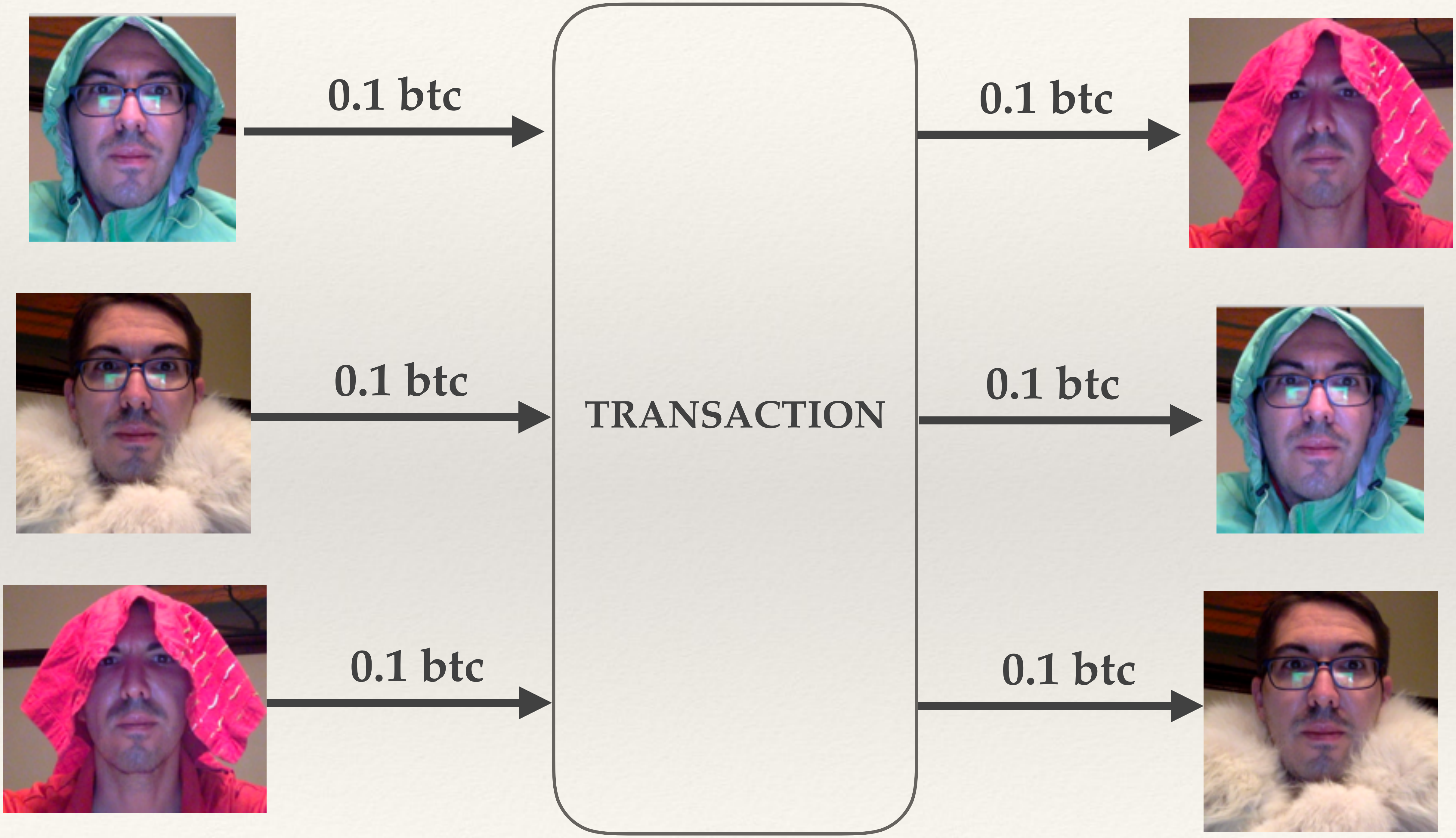
- You need to trust them with your bitcoin, even if momentarily
- Many, many, many scams
- Network effect difficulty - need to have large number of people using same mixer for high anonymity set (different mixers, different chunk sizes)
- Turns out tracking is possible since few (if any?) mixers follow best practices (see Bonneau et al., "Anonymity for Bitcoin with accountable mixes" http://wws.princeton.edu/system/files/research/documents/Felten_Mixcoin.pdf)

CoinJoin

- “Single-transaction mixing”

  1. Find peers who want to mix
  2. Exchange input/output addresses
  3. Construct transaction
  4. Send the transaction around. Each peer signs after verifying their output is present.
  5. Broadcast the transaction

CoinJoin



0.1 btc

0.1 btc

0.1 btc

TRANSACTION

0.1 btc

0.1 btc

0.1 btc

Problems with CoinJoin

1. Trivially vulnerable to Denial-of-Service attacks
2. Hard to defend against bad actors in a decentralized system
3. Possible to leak data via side channels with poor implementation

See "Weak Privacy Guarantees for SharedCoin Mixing Service" by Kristov Atlas http://www.coinjoinsudoku.com/advisory/

Privacy-Focused Altcoins

- **ZCash** - zk-SNARKS (zero-knowledge Succinct Non-Interactive Argument of Knowledge proofs); anonymity by choice (reduces the size of anonymity set!)
- **Monero** - Ring signatures, RingCT (Ring Confidential Transactions), stealth addresses
- **Grin** - Mimblewimble protocol