A Ten Minute Primer on Transaction Privacy

The Danger and Allure of Grafting Privacy-Enhancing Tech onto Transparent Systems

Brandon Goodell

Monero Research Lab, a workgroup at The Monero Project

February 27, 2019

Bitcoin has a transparent blockchain.

Can Bitcoin ever be private?

Bitcoin has a transparent blockchain.

Overheard: “Bitcoin will eventually be private with new technological developments (MimbleWimble, Confidential Transactions).”

Can Bitcoin ever be private?

Bitcoin has a transparent blockchain.

Overheard: “Bitcoin will eventually be private with new technological developments (MimbleWimble, Confidential Transactions).”

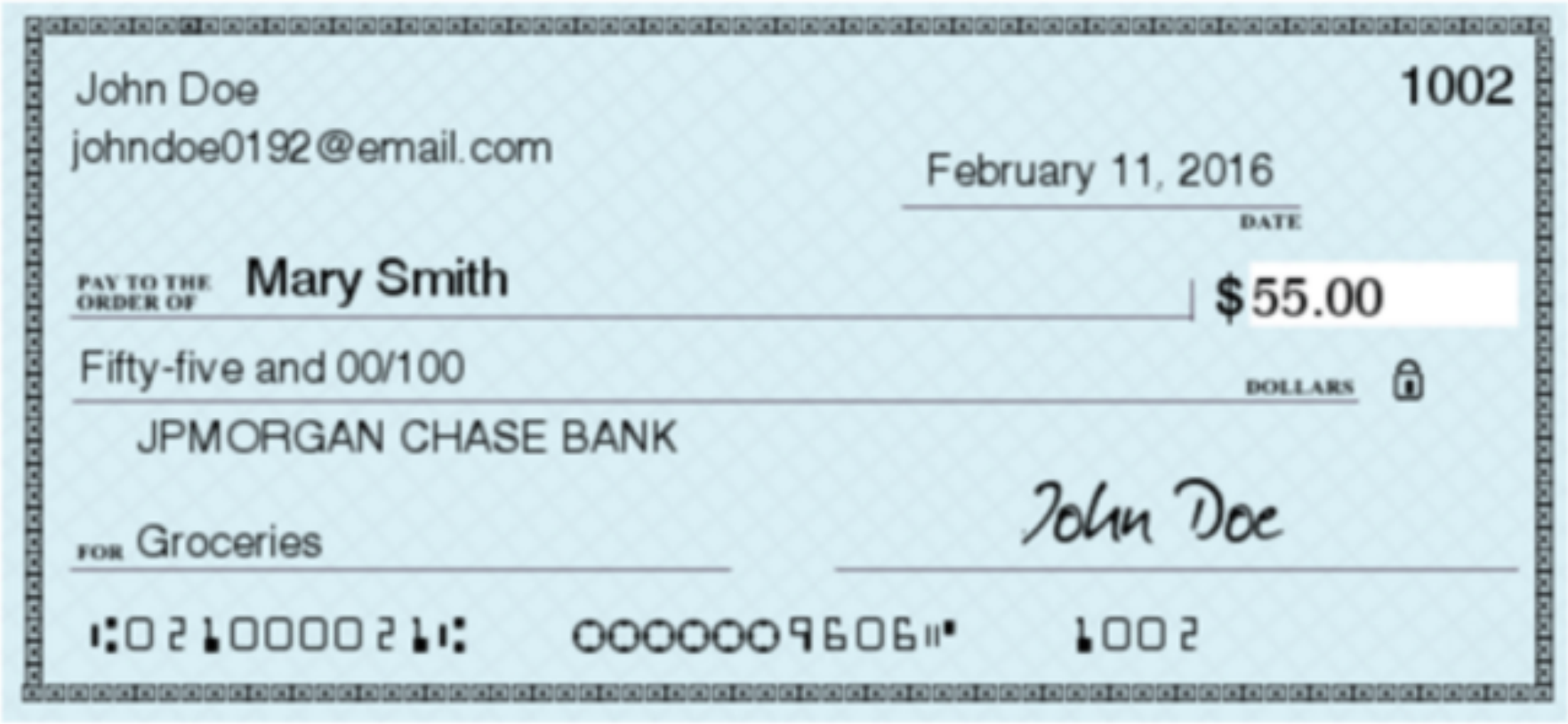
Great sentiment! Why is it wrong?

Transparent transactions

Mary sent John a check for $55 on 11 Feb 2016; none of the data is encrypted or secret.

Transparent transactions

Mary sent John a check for $55 on 11 Feb 2016; none of the data is encrypted or secret.



Confidentiality Fixes

Problems?

- Identities, account numbers... fix: one-time keys.

Confidentiality Fixes

Problems?

- Identities, account numbers... fix: one-time keys.
- Amount... fix: homomorphic commitments and range proofs (bulletproofs).

Confidentiality Fixes

Problems?

- Identities, account numbers... fix: one-time keys.
- Amount... fix: homomorphic commitments and range proofs (bulletproofs).
- Forgeable signature... fix: cryptographically secure signatures.

Confidentiality Fixes

Problems?

- Identities, account numbers... fix: one-time keys.
- Amount... fix: homomorphic commitments and range proofs (bulletproofs).
- Forgeable signature... fix: cryptographically secure signatures.
- Permissioned and censorship-sensitive.... fix: remove TTP, allow anyone to broadcast, and decentralize verification.

Confidentiality Fixes

Problems?

- Identities, account numbers... fix: one-time keys.
- Amount... fix: homomorphic commitments and range proofs (bulletproofs).
- Forgeable signature... fix: cryptographically secure signatures.
- Permissioned and censorship-sensitive.... fix: remove TTP, allow anyone to broadcast, and decentralize verification.
- Date... fix: dual key structures (paper in prep).

Mo fixes mo problems

- One-time keys can still be clustered... fix: sign with a whole ring of keys!

Mo fixes mo problems

- One-time keys can still be clustered... fix: sign with a whole ring of keys!
- Amounts... well, actually, we have that one pretty well locked down.

Mo fixes mo problems

- One-time keys can still be clustered... fix: sign with a whole ring of keys!
- Amounts... well, actually, we have that one pretty well locked down.
- Blockchain security with POW requires *ongoing burning of resources* (distributed, but still expensive)... fix: none yet. Proof of Stake, Space, Time, or Steak inherits problems.

Mo fixes mo problems

- One-time keys can still be clustered... fix: sign with a whole ring of keys!
- Amounts... well, actually, we have that one pretty well locked down.
- Blockchain security with POW requires *ongoing burning of resources* (distributed, but still expensive)... fix: none yet. Proof of Stake, Space, Time, or Steak inherits problems.
- TTP model remains: bank replaced with exchanges, and now mining centralization is also a threat.

TLDR: Beginning with a *transparent system* and then *grafting privacy tech on top* leads to a rabbit hole of more and more complicated problems... *assuming you were even successful in grafting!*

The only way to win is to not play by beginning with a *private system* first!