Anonymity vs. Privacy

Campbell R. Harvey
Duke University, NBER and
Investment Strategy Advisor, Man Group, plc

January 25, 2017
Setting

• Considerable misunderstanding of the terms anonymous and privacy
• Goal is to differentiate between the two and understand where bitcoin fits in

Definitions

• A transaction is “anonymous” if no one knows who you are.
• A transaction is “private” if what you purchased, and for what amount, are unknown
Definitions

- Public charitable gift
- Credit/debit card
- Campaign contribution
- Cash/barter
- Bitcoin

Campbell R. Harvey 2017
Definitions

- Cash/barter are most anonymous and private ways to transact
- A U.S. political campaign contribution is not anonymous and not private because all of the details are public record
Definitions

• Some transactions are private but not anonymous
• For example, you might see a person listed as donating to a charity – however, the amount the person donated is not listed.
Definitions

• Credit card transactions are not anonymous and they are not private
• Your information is fully available to the issuing bank, the merchant, the credit card network, and law enforcement – if subpoenaed.
Where does bitcoin fit?

• Bitcoin is anonymous but not private
• Identities are not revealed in the block chain – but every transaction is visible in the blockchain.
• Anonymity is attractive – but also a challenge for financial regulation that seeks to prevent money laundering
Where does bitcoin fit?

• What if you use a popular on-line wallet like Coinbase?
• In this case, you link your bitcoin to your identity. As a result, there is little difference in anonymity between using Coinbase and using a bank to transact.

Bitcoin Battle Heats Up as Coinbase Moves to Fight IRS Demand

Jeff John Roberts
Jan 17, 2017

Coinbase, the most well-known bitcoin exchange in the U.S., filed court papers last week to support a challenge to an IRS demand that the startup turn over information about millions of customers’ accounts. The IRS had cited a "suspicion [the group] includes U.S. taxpayers who are not complying with the law."
Where does bitcoin fit?

- To transact anonymously, you need to acquire bitcoin in a private transaction or do mining.
Deanonymization techniques

- Even if you privately obtained bitcoin, there are ways to deanonymize. This is called “transaction graph analysis”
  - Transactions that have more than one input address (means that it is likely that both input addresses controlled by the same person)
  - If one output address has never appeared in chain, it is like the “change” address which is linked to the same person doing the transaction
  - Examine the numerical precision. If there are two outputs, 5 BTC and 2.117 BTC, it is likely that the 5 is going to the recipient and the 2.117 is the “change” for the sender
Deanonymization techniques

• Deanonymization can be minimized by sending your bitcoins through a mixer or tumbler
  – Fee involved
  – You must trust the mixing firm
  – Transaction graphing can be used to identify coins that have been mixed – and this would be an obvious red flag for merchants accepting bitcoin
Deanonymization techniques

- Deanonymization can also take place outside of the block chain
  - Merchants publish QR codes and addresses
  - Addresses can be harvested from public forums (sometimes people leave a public address when they sign a posting)
  - Can be used for retroactive geolocation analysis, which potentially can trace where you spent your bitcoin during the day
Deanonymization techniques

- Deanonymization can also take place outside of the blockchain
  - IP addresses another source of information
  - Thousands of computers attached to the bitcoin network “announce” transactions (nodes)
  - If you had a network of nodes that allow you to link to all the nodes accepting incoming connections, you could potentially identify the first IP to broadcast a transaction
  - What about Tor? They use “onion routing” (i.e. onion DNS addresses that appear to be randomly generated that do not correspond to the same addresses via HTTP)
  - But Tor is not a great solution - see Biryukov and Pustogarov, “Bitcoin over Tor isn’t a good idea”. [http://arxiv.org/pdf/1410.6079v2.pdf](http://arxiv.org/pdf/1410.6079v2.pdf)
Summary

• Bitcoin less anonymous than cash
• It is possible to get bitcoin privately but even then there are possible ways to identify you