Crypto News?

Anonymity

Who owns bitcoin?

- Regular people, early adopters, governments, exchanges
- How do they retain ownership over these coins?
  - Recall private vs. public keys from last week
- How do they relinquish coins?
  - Recall how users must sign unspent transaction outputs in order to claim and spend them

How are private keys generated?

- Ideally, private keys are generated randomly and locally
  - Why would this help with privacy/anonymity?
- Services exist to do this for you, or you can do it yourself
  - Are these services trustworthy? Hard to tell

What happens if you use an exchange to store funds?

- Most exchanges require some form of identification for legal reasons
  - These exchanges then manage private and public keys on behalf of your legal identity, so when you send coins from an address, the exchange has a record that you did that
- Depending on the exchange's residence country, governments may subpoena personal and/or financial data of users
  - Can't just use a foreign exchange to get around this completely
  - Just because two governments don't cooperate to subpoena now doesn't mean they won't in the future
- Buying a cryptocurrency for fiat and exchanging cryptocurrencies are all taxable transactions in the U.S.
  - By law, you are required to submit a report detailing crypto exchanges on your taxes, therefore decreasing anonymity of exchanges
  - We will come back to the idea of "cashing out" later

How does bitcoin’s structure contribute to anonymity

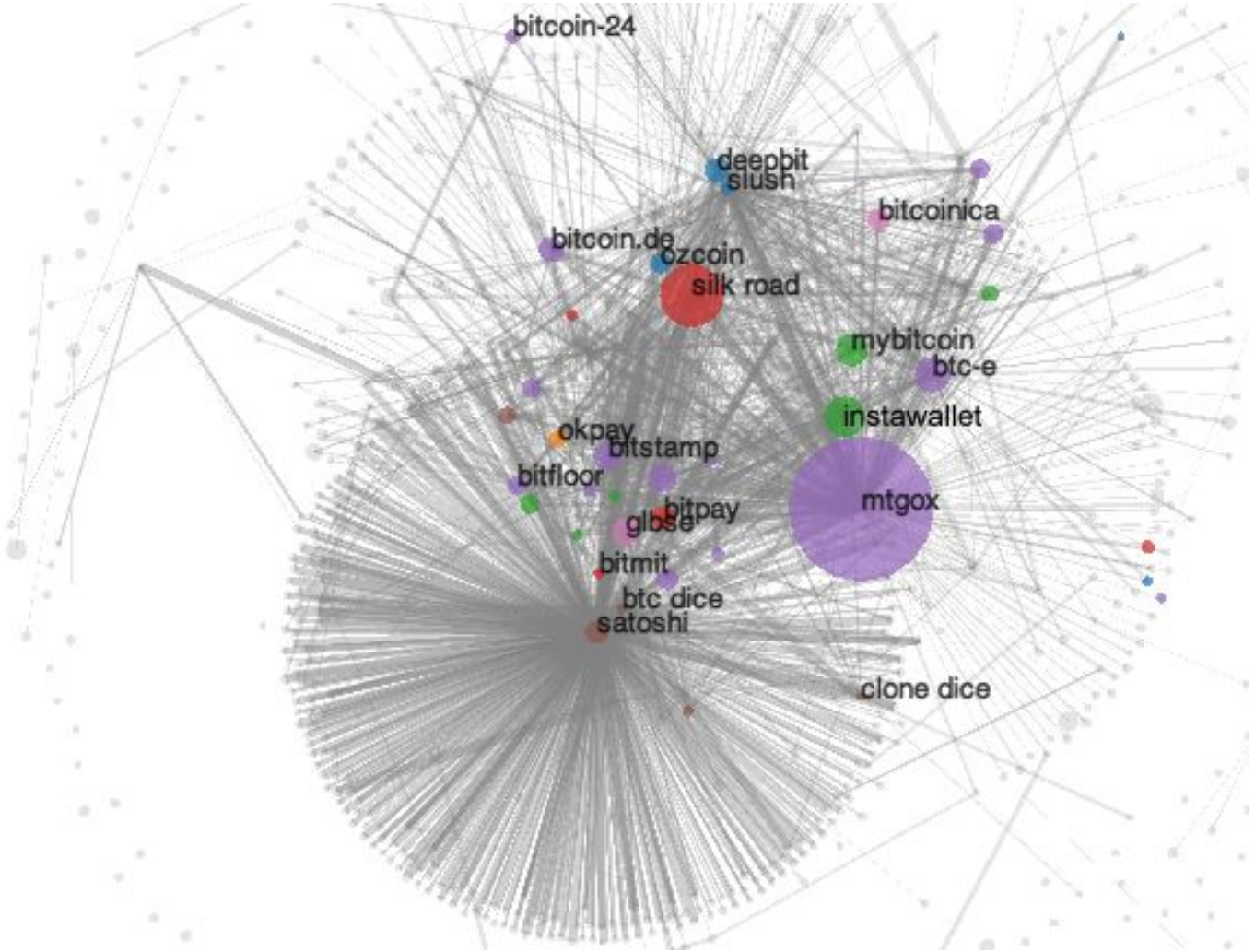
- The blockchain does not store any personal info
  - Only addresses are included on the blockchain, not private keys, emails, names, or any other personally identifying information
- For all intents and purposes, anyone can create an “unlimited” number of addresses to send coins to
  - How does this contribute to anonymity?
  - We can “roll” coins to multiple addresses that we own, no one has to know we own them

How are people usually tracked down?

- Not using multiple addresses
  - If the change from every transaction is sent back to the same address, then it is very easy to link many transactions (illegal or not) back to one identity, since that identity is the only one in charge of the private key to that particular address
- Side channels
  - If payments from address x are only between 8 and 11 PM EST, then the person is probably on the east coast of the United States, etc
  - Hacked exchanges could reveal user IP logs, which can expose elements of location of users

How are people usually tracked down?

- Blockchain Analysis
  - There is a whole field of study leveraged by the FBI called “blockchain analysis,” in which the FBI (or any government agency) will draw graphs of transactions between addresses in order to track the flow of bitcoin from point A to point B — this works surprisingly well in deanonymizing users on the network
- Cashing Out
  - When a user goes to convert crypto back into fiat, they can deanonymize themselves if they are not careful
  - Converting back to fiat electronically usually requires a bank account or wire transfer
  - What if you sell your crypto for literal cash?


bitcoin-24
deepbit
slush
bitcoinica
bitcoin.de
ozcoin
silk road
mybitcoin
btc-e
instawallet
okpay
bitstamp
bitfloor
bitpay
mtgox
bitmit
btc dice
satoshi
clone dice

Silk Road

anonymous marketplace

How to avoid detection?

- One of the most well-known cases of Bitcoin anonymity is Silk Road
- Silk Road was an illegal marketplace that was only accessible via the Tor network from 2011 until it was shutdown in 2013
- How did they incorporate anonymity into their site?
  - Two main ways:
    - Tor
    - Bitcoin mixing

The Tor Project

- Tor is a web browser designed for anonymous web surfing by obfuscating web traffic
- How does Tor achieve this?
  - Onion protocol — multi-layer encryption
- What is one major problem with the onion protocol for anonymity?
  - Exit nodes can be compromised

Bitcoin mixing

- Recall the idea of chains of digital signatures
  - If a coin goes from person A to person B, then it is very easy to trace
- We can “mix” bitcoins by scrambling these chains of digital signatures
  - Suppose person A wants to pay person B anonymously
  - Instead of person A directly paying person B, person A can pay a third entity who owns a large amount of bitcoin, and that third entity can send a different unspent output to person B
- Problems?
  - Trust
  - Blockchain Analysis — pool of addresses owned by third entity will be a “hotspot” for transactions of a particular type

How do other cryptocurrencies achieve anonymity?

- Zcash
  - Zcash is a cryptocurrency geared towards anonymity by using zk-SNARKs
  - zk-SNARKs allow nodes to verify transactions without needing to know the start or end address, or the amount of money being sent
  - Problem? Trusted Setup
- Monero
  - Monero gears itself towards anonymity by using ring signatures
  - In a nutshell, ring signatures allow transaction outputs “hide” among other transaction outputs via stealth addresses
  - Problem? Opaque blockchain, rings of size 0, Temporal Analysis
- Dash
  - Achieves anonymity via PrivateSend, in which master nodes mix coins when user A wants to send to user B
  - Problem? Centralized

Project 2

- Project 2 is due on Friday, March 9th, at 11:59 PM, deadline is Monday March 12th at 11:59 PM for 15% penalty
- Project consists of receiving a list of transactions, and then validating each transaction in the list as if you were a node on Bitcoin's network
- You will have to keep track of inputs and outputs as well as a UTXO pool, as we discussed last week in the Wallets & Transactions slides
- As always, we have office hours on Tuesdays at 2 in Startup Shell, but can meet outside if need be

Summary

- Bitcoin is not inherently anonymous
- Private keys should never be generated using personal information
- Exchanges keep track of users, any fiat to crypto transaction (or vice versa) carries significant risk of deanonymization
- Tor and Bitcoin mixing are two ways to hide your identity with Bitcoin
- Some other coins attempt to address anonymity explicitly

Questions?