Bitcoin privacy

Aljaz Ceru, November 2021

Importance of privacy

- Keeping your personal finances private
- Personal safety
- Avoiding censorship

Privacy

- Not a one solution problem
- Ongoing process
- Multiple approaches combined together

Basics

- Obtaining bitcoin
- Avoid address reuse
- Use lightning
- Coin control
- Online privacy

Obtaining bitcoin

- Buying bitcoin from an exchange
- Bitcoin ATMs
- P2P
- Earning bitcoin
- Mining

Address reuse

- You don’t want your hairdresser to know how much bitcoin you have
- You don’t want your employer to know what you spend your money on
- Single bitcoin address used for multiple transactions
    - Sender knows how much bitcoin you have and what are you spending it on
    - Linking together your purchases

Coin control

- Utxos with different privacy levels in one wallet
- Avoid spending multiple utxos for single transaction
- Dusting
- Depends on wallet software

Regaining privacy

- Coinjoin/PayJoin/JoinMarket
- Mixers/tumblers
  - usually involves a lot of trust
- Privacy focused wallets
  - Wasabi
  - Samurai
- Potential issues
  - Exchanges don’t like privacy

Lightning network

- Off chain payments are not permanently stored on chain
- Common analysis tools don’t work on lightning
  - Common input ownership heuristic
  - Address reuse
  - Change address detection
- Different threat model
  - Node privacy and security
  - Channel opening and closing transactions can be identified

Lightning node privacy

- Use utxos that are not kyc'd
- Use tor (or use cloud instances to avoid leaking home ip)
- Don't run other publicly available services on your node

Safety

- Exchanges and vendors get hacked
- Identifying your wallets from deposit/withdrawal addresses
- Bitcoiners make for great targets
  - Ledger hack
  - 5$ wrench attack