

Fungibility: Attacks and Solutions

Scaling Bitcoin Milan
Adam Back & Matt Corallo

Why Fungibility?

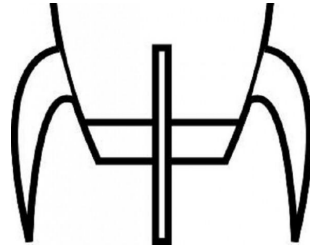
- Bitcoin, like cash is immediate and final payment
 - Fungibility practices have gotten so bad, that with some wallets, that it is worse than paypal.
 - Paypal does not freeze your funds if one of your customers' customers used silkroad!
- Everyone needs fungibility, or no one has it.
 - Your lack of fungibility impacts everyone else.
- Bitcoin's permissionlessness is critical to its users
 - For bitcoin to function for payment we need fungibility
 - If fungibility breaks down, merchants may start to consult blacklist services
 - Taint tracing services become permission brokers. No permission, no bitcoin :(
- Worst case fungibility collapse can lead to loss of confidence, price crash.

Types of Attacks

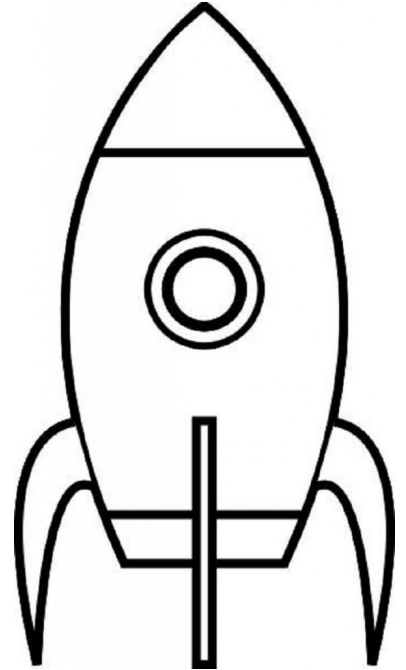
- Modern Attacks do backwards looking analysis
 - who received this, looking back up to 4 hops?
- Primarily Focused on Grouping Transactions/UTXOs from one Individual/Group by:
 - Transaction Flow Graph Analysis
 - Single-owner Inputs/Outputs, Address Reuse and Lack of Balance Privacy make this possible
 - Network Transaction Origin Identification - Where did the transaction come from
 - Transaction Features Identification wallet/service fingerprinting
 - Transaction Censorship

Scalability

- Often fungibility solutions help scalability



- Sometimes fungibility solutions are massive scalability wins



Transaction Graph Privacy: Address Reuse

- Don't Do It!
- Stealth Addresses and HD-style derivation

Transaction Graph Privacy: Input/Output Privacy



CoinJoin

- TumbleBit



Lightning (with Onion Routing, even!)

- Ring Signatures (Monero)




One Way Aggregatable Signatures

- ZCash



MimbleWimble




Transaction Graph Privacy: Balance Privacy

- Balance Discretization
- Confidential Transactions
-  MimbleWimble
- ZCash

Network Attacks

- BIP 37 (SPV Bloom Filters) largely gives up all privacy
 - Committed Bloom Filters may be a solution
- Connect-To-Everyone Attacks are common
 - Private Transaction Relay is hard - lots of changes recently to improve this
- Essentially no privacy against global passive adversaries (aka NSA)
- There is lots of research into how to do this better using mixnets

Transaction Features Identification (Wallet/Service Fingerprinting)

- Coin Selection
 - Change value
 - Reveal which UTXOs are in the same wallet
 - Fee selection
- Scripts Used
 -  Schnorr fixes this for some types of multisig
 -  MAST with hidden branches
 -  zkSNARK-based script systems
- Non-Script Transaction Features

Transaction Censorship

- Coins which are censored even by a small hashrate are less valuable
- Create a social cost to Transaction Censorship
- Push Transaction Selection away from pools
- Encrypted Transactions

Conclusions

- Second-Layer solutions are incredibly powerful here: not everyone sees everything
- Better scaling helps fungibility (in many ways, sometimes just because there are more users)
- Much work to do but many ways forward