Fungibility & Scalability

Adam Back

fungibility/privacy

- fungibility: all important cash property (all coins equal & interchangeable)
- mostly Bitcoin has fungibility without privacy
- via decentralised mining (someone will process your transaction)
- though pseudonym based and change vs payment ambiguity
- helped by other mechanisms (coinJoin, coinSwap, mergeAvoidance)
- types of Bitcoin privacy:
- unlinkability privacy (who is paying who)
- balance privacy (how much BTC owned)
- transaction value privacy (how much did you pay)

fungibility and scale - not all negative

- fungibility related mechanisms increase number of transactions
- and increase size of transactions, may increase UTXO size
- however some mechanisms reduce number of transactions
- and reduce UTXO size

fungibility mechanisms - one-use address

one-use addresses

- obscures who is paying who vs single reused address
- obscures wallet balance (balance split across multiple addresses)
- fragmentation as wallet split into many addresses
- increases number of transactions, size of transaction (more inputs)
- increases UTXO size
- only moderate effectiveness
- improve with merge avoidance (multiple tx instead of multiple input tx)

fungibility mechanisms - coinJoin / coinSwap

- improvement over one-use address
- shared input addresses across multiple wallets
- need amount ambiguity
- need to coordinate with other spenders
- some spenders maybe privacy hostile
- p2p in wallet or via coinJoin server
- trustless: cant steal only stall

fungibility mechanisms - confidential transactions

confidential transactions

- privacy for balance and transaction value
  - undisclosed values with homomorphic addition & range proof ZKP
- indirectly some privacy improvement - change more ambiguous
- can send 0-value transactions to others
- coinJoin simpler: any transaction set can be coinJoin ambiguous
- transaction size maybe 6x bigger (5x with new improvement)
- but replaces multiple transactions, makes these redundant:
  - merge avoidance, balance privacy, value privacy plus smaller UTXO
- hard to evaluate average reclaimed overhead due to privacy

fungibility mechanisms - linkable ring-sig

linkable ring-sig

- sender chosen mix-set, better than coinJoin
- values must match in set, ring-sig approves spend
- linkable ring-sig prevents double-spend, side-effect: not UTXO compactable
- overhead: ring-sig size linear in mix-set size
- saving: less reliant on one-use addr for reducing linkability?

fungibility mechanism - zeroCoin/zeroCash

- hides sender and recipient
- not UTXO compactable
- zeroCash hides values, zeroCoin has coin-denomination mix-set
- EZC value hiding zeroCoin variant
- zeroCoin big (30-40kB transactions), zeroCash better (300byte)
- CPU expensive zeroCash & novel crypto & key setup trapdoor
- otherwise zeroCash is ideal fungibility solution

fungibility mechanism - encrypted transaction

(time-lock) encrypted transaction - fungibility without privacy

- also called “committed transaction” use of commitment and time-lock
- two phase validation by miners, elides policy information
- in second phase keys are revealed and transaction must be approved
- block is invalid if it does not 2nd-stage validate pending transactions
- time-lock decryption prevents DoS (failure to publish keys)

fungibility, privacy & identity

- idealised fungibility is a building block
- we can retain privacy norms without losing investigation ability
- business record subpoenas for investigation (obligation to keep records)
- avoid pre-emptive mass surveillance default

2014 talk on “fungibility, privacy & identity”

https://www.youtube.com/watch?v=3dAdI3Gzodo

fungibility and scale summary

- need to consider delivered fungibility as well as size & number of transactions
- need data from anonymized analysis of usage patterns and overhead
- make available an improved range of tradeoffs for users:
- some users may be willing to pay more for fungibility/privacy than scale
- users of high scale / low value transactions not as sensitive on fungibility
- giving users flexibility to make economic choices is good
- fungibility and permissionless use is an important part of Bitcoin
- Bitcoin fungibility could do with some more improvements
- fungibility solutions are more practical than otherwise thought
    - their use reclaims some overhead vs simpler methods