Did I say anonymity?
I meant fungibility

axel simon, Office of the CTO

axel@redhat.com

OpenFintech Forum
2018-10-11

Presentation agenda

- Fungibility?
- Why is it desirable?
- What does it mean in a blockchain / DLT context?
- How can we achieve it?

  privacy/anonymity on the blockchain
- How is it relevant to permissioned environments?

What is fungibility

FUNGIBILITY

(it’s not about mushrooms)

Fungibility is a property of certain goods & commodities (and services) where individual units can be exchanged for another without it making any difference.

ie: you don’t care what exact grains of rice make up 1 kg of rice, the grains are essentially interchangeable.

Fungibility ≠ liquidity.

CC Thomas Wanhoff

FUNGIBILITY

(it’s not really about rice either, in our case)

ie: you don’t care what Euro notes make your 100 €, the bills are interchangeable

Money is fungible.

CC Ron Reiring

Why is fungibility desirable?

WHY IS FUNGIBILITY DESIRABLE?

OR WHAT HAPPENS WITHOUT IT

“Why?” before “how?”

CC Michael Coghlan

WHY IS FUNGIBILITY DESIRABLE?

OR WHAT HAPPENS WITHOUT IT

“Why?” before “how?”:

Money should be fungible.

CC Michael Coghlan

WHY IS FUNGIBILITY DESIRABLE?

OR WHAT HAPPENS WITHOUT IT

“Why?” before “how?”:

Money should be fungible.

If it isn’t, bad things™ happen:

- (Impractical) onus to check your money’s history.

CC Michael Coghlan

WHY IS FUNGIBILITY DESIRABLE?

OR WHAT HAPPENS WITHOUT IT

“Why?” before “how?”:

Money should be fungible.

If it isn’t, bad things™ happen:

- (Impractical) onus to check your money’s history.

- all coins are equal, but some are more equal than others.

CC Michael Coghlan

What does fungibility mean in a blockchain/DLT context?

FUNGIBILITY + BLOCKCHAIN

= ANONYMITY

If your money has history attached to it, you run into problems.

FUNGIBILITY + BLOCKCHAIN

= ANONYMITY

If your money has history attached to it, you run into problems.

To be economically functional, a cryptocurrency needs to be fungible.

FUNGIBILITY + BLOCKCHAIN

= ANONYMITY

If your money has history attached to it, you run into problems.

To be economically functional, a cryptocurrency needs to be fungible.

Use: anonymity and privacy techniques.

FUNGIBILITY + BLOCKCHAIN

= ANONYMITY

This is interesting: we essentially need the properties that prompted people to label Bitcoin “the money of criminals”

Attempts at fungible cryptocurrencies: Zcash, Monero, Dash, etc.

How can we achieve fungibility: privacy and anonymity techniques

WHAT TECHNIQUES CAN WE USE

A NON-EXHAUSTIVE TOUR

What aspects of transactions can we hide?

- sender
- receiver
- amount
- more? (time, location)

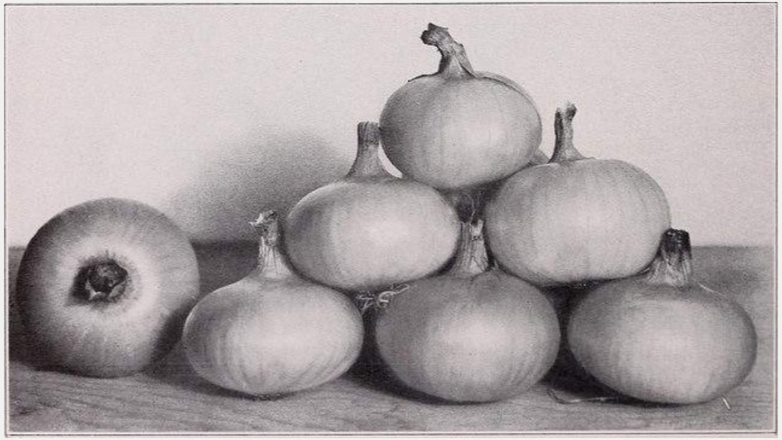
CC Ognjen Odobasic

WHAT TECHNIQUES CAN WE USE

THE BASICS

Before anything else consider:

- reuse of wallet addresses
- IP privacy
    - anonymisation networks like Tor
- shoulder surfing
- a hard one: cookies and trackers
- hiding in a crowd
    - ie: is everyone doing it?
    - how big is “everyone”?



Public Domain, via Internet Archive Book Images

WHAT TECHNIQUES CAN WE USE

THE LESS BASIC

Another “obvious” solution:

- Don’t do things on-chain

- The advanced version:

  - layer 2 solutions (Lightning, Plasma, Raiden, BOLT)
  - Quorum v1’s private transactions

CC John Fowler

WHAT TECHNIQUES CAN WE USE

MIXING COINS

- Tumblers, Mixers

- Coins go in, coins go out
- Need I say, risky?

- CoinJoin

- Join transactions between A & B and C & D into a big ABCD transaction
- Hides: whom
- Requires a third party

- Enhancements: CoinShuffle, ValueShuffle, PathShuffle

- Hides: whom, how much
- No third party

CC Mike Cohen

WHAT TECHNIQUES CAN WE USE

CONFIDENTIAL...

- Confidential Transactions
  - Uses: cryptographic commitments
  - Hides: amount
- Confidential Assets
  - Uses: cryptographic commitments
  - Hides: amount, asset type

WHAT TECHNIQUES CAN WE USE

CONFIDENTIAL...

- Ring Signatures

- Uses: ring signatures :)
- Hides the sender among a group of potential senders

- Stealth Addresses

- Uses: ECC cryptography + dual-key (view, spend)
- Hides: recipient (sender can create one-time destination address for recipient)

WHAT TECHNIQUES CAN WE USE

SOME MAGIC

- Mimblewimble:
  - prevent the blockchain from "talking"
  - effectively modify what gets recorded on the chain
  - removing historical data improves privacy

WHAT TECHNIQUES CAN WE USE

SOME CRYPTOGRAPHIC MAGIC: ZERO-KNOWLEDGE PROOFS

- ZK-SNARKs

- Hides: amount, sender, recipient
- Needs: trusted setup
- Uses: a lot of computing power, 10 kB per proof

- ZK-STARKs

- Hides: amount, sender, recipient
- Needs: no trusted setup,
- Pros: Quasi-linear proving time, poly-logarithmic verification time

- Bulletproofs

- Hides: amount, sender, recipient
- Pros: no trusted setup, smaller proof size (1 kB), proofs can be aggregated
- Cons: more time consuming than SNARKs

You can trust me, this transaction is valid, but I won't tell you why!
12qwdiunb23y 87rtx294btrilwabgfli7wfw rq3ru3brgwavrf1 2HQ38RGW3RZW43T 3WR2fuqi3bgfxv3w g73wuf214124indsfa wgfiubwggw1y24892412841241uabsfwq

Via vitalik.ca

What about permissioned blockchains?

WHAT ABOUT PERMISSIONED DLTs?

AKA “I’M NOT DOING A CRYPTOCURRENCY”

Money needs fungibility, but so do:

- company shares,
- bonds,
- other precious metals

You probably want fungibility here too.

Transaction confidentiality cited as a major security concern.

Another type of fungibility

MORE FUNGIBILITY QUESTIONS

Fungibility of tasks:
- one person can do the job in 10 days, or
- ten persons can do the job in 1 day

Not going into this here, but worth considering:
Execution of fungible “smart contracts” tasks?

Can “smart contracts” be encrypted?
→ essentially, entering the realm of Secure Multi-Party Computation

FIN

redhat.

THANK YOU

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos