Bitcannery:

Decentralised secret keeping network

April 2019

Problem

Distributed ledger is transparent and immutable, but it is hard to keep secret information on it

We have reliable tools for instant encrypted communication, but not for delayed one

Adjustable decryptability over time is not easy to achieve (see a time-lock encryption)

Possible solutions

Attorneys and notaries

Centralised web service

Time-locked encryption

'Heritable' Ethereum Smart contract

Blockchain-based: Enigma, Keep.network, Mywish, Safe Haven

Our solution

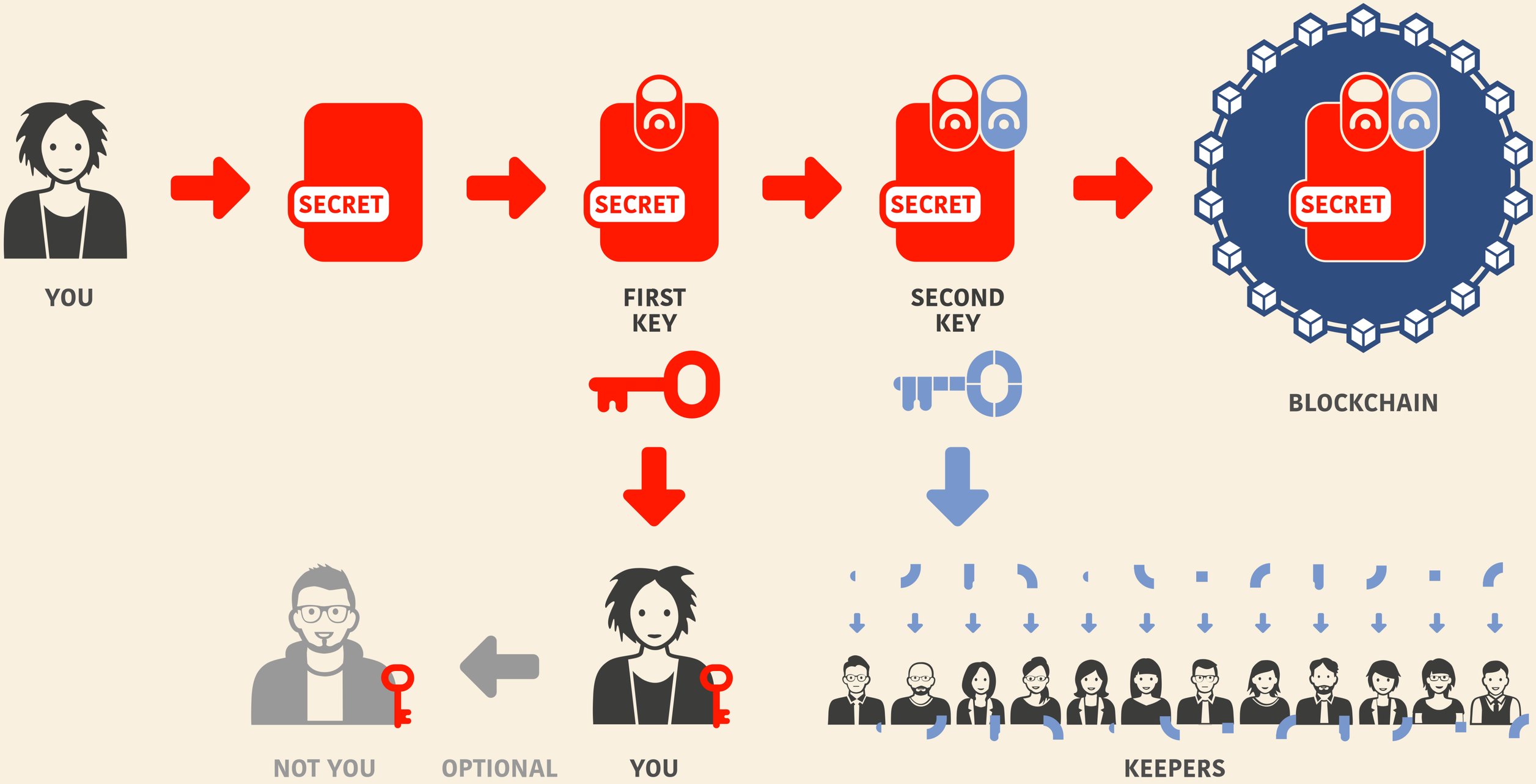
Keeping encrypted message on the blockchain

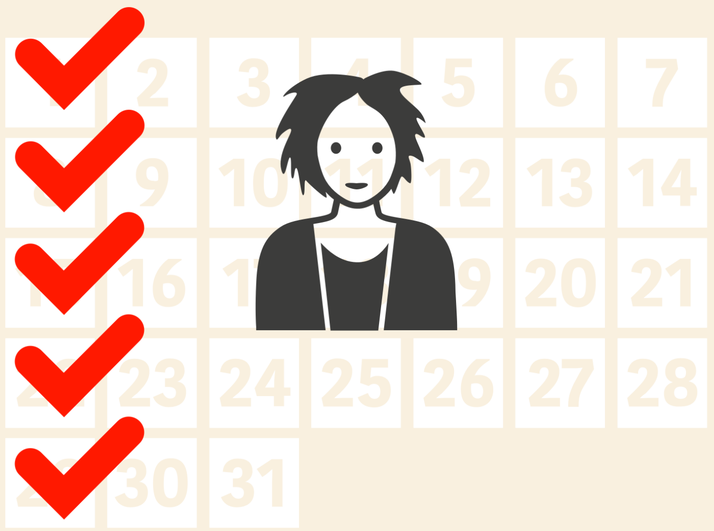
Network of incentivised agents aka Keepers

Two keys: one for addressee, another is split between Keepers

Shamir secret sharing method is used

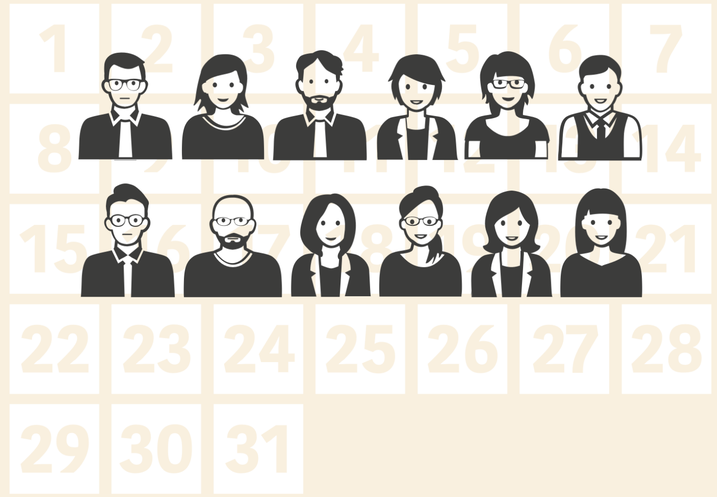
Sender uses periodical check-ins as a reverse trigger


SECRET
SECRET
SECRET
SECRET
YOU
FIRST KEY
SECOND KEY
BLOCKCHAIN
NOT YOU
OPTIONAL
YOU
KEEPERS



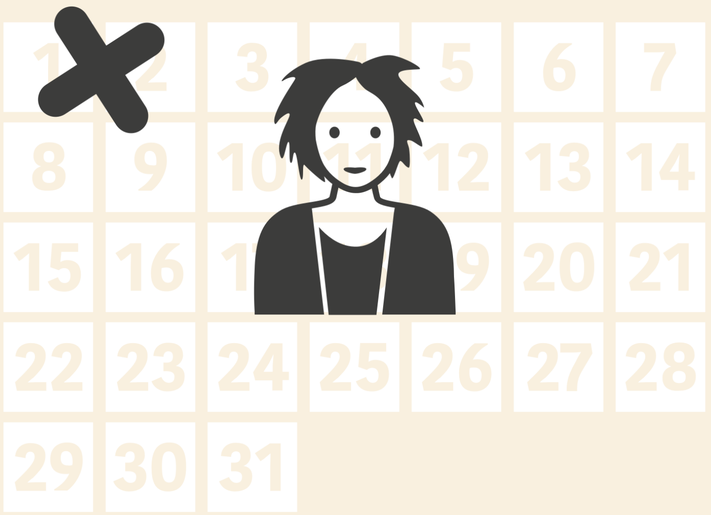
PERIODIC
CHECK-IN

PERIODIC
CHECK-IN

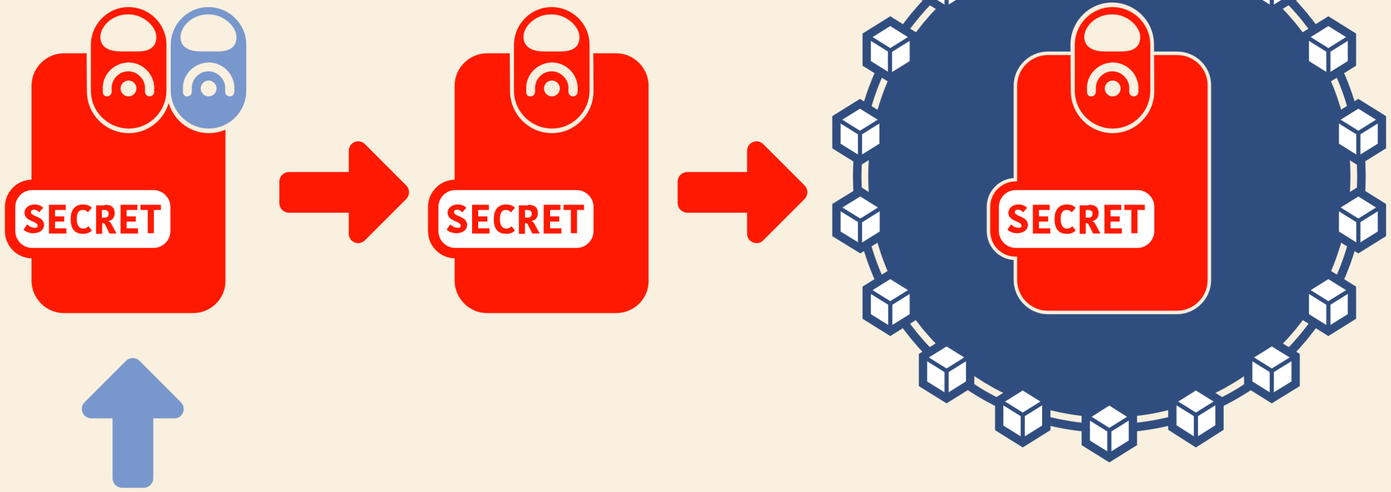


YOU

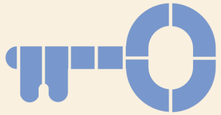
KEEPERS

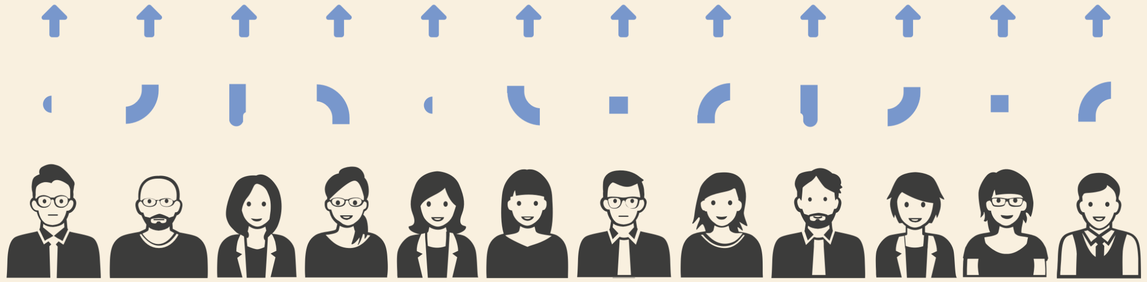


YOU MISSED CHECK-IN



SECOND KEY





KEEPERS

Possible applications

Data escrow

Data leaking

Insurance

Inheritance and wallet backups

References

- Speaker: Pavel Filippov, https://emdin.info
- https://bitcannery.net
- https://github.com/bitcannery
- https://github.com/bitcannery/bitcannery-cli/blob/master/HOWTO.md
- https://en.wikipedia.org/wiki/Secret_sharing
- https://www.gwern.net/Self-decrypting-files