TRACKING, MONITORING, & DISCLOSURE

TECHNOLOGICAL TOOLS FOR CRYPTOCURRENCY REGULATION

Prof. Aviv Zohar

A historical perspective

Encryption was initially all “military” uses.

Engima in WW2.

Perception is: Enemy encryption must be broken.

Get lots of computers and break it.

A historical perspective

Enter the private sector.

- DES Developed in the 70s by IBM
- Became a standard in 77. (solicited by Govt.)
- Encryption at IBM later driven by business needs (e.g. protect communication to ATMS)


WARNING
This shirt is classified as a munition and
may not be exported from the United
States, or shown to a foreign natio
RSA
encryption in pri

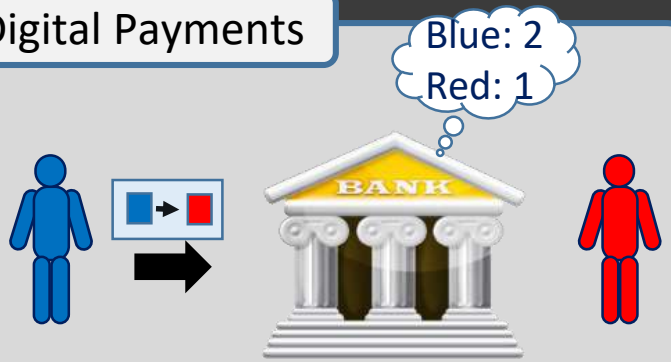
A historical perspective

- DES was Weakened by NSA (56bit keys)
- Exporting strong encryption was illegal in US.
  - Should we give strong encryption to terrorists and enemies?
- Restrictions eased by the year 2000.
- Now EVERYWHERE.
  - every phone and every bank’s website, every wifi router, and TV.

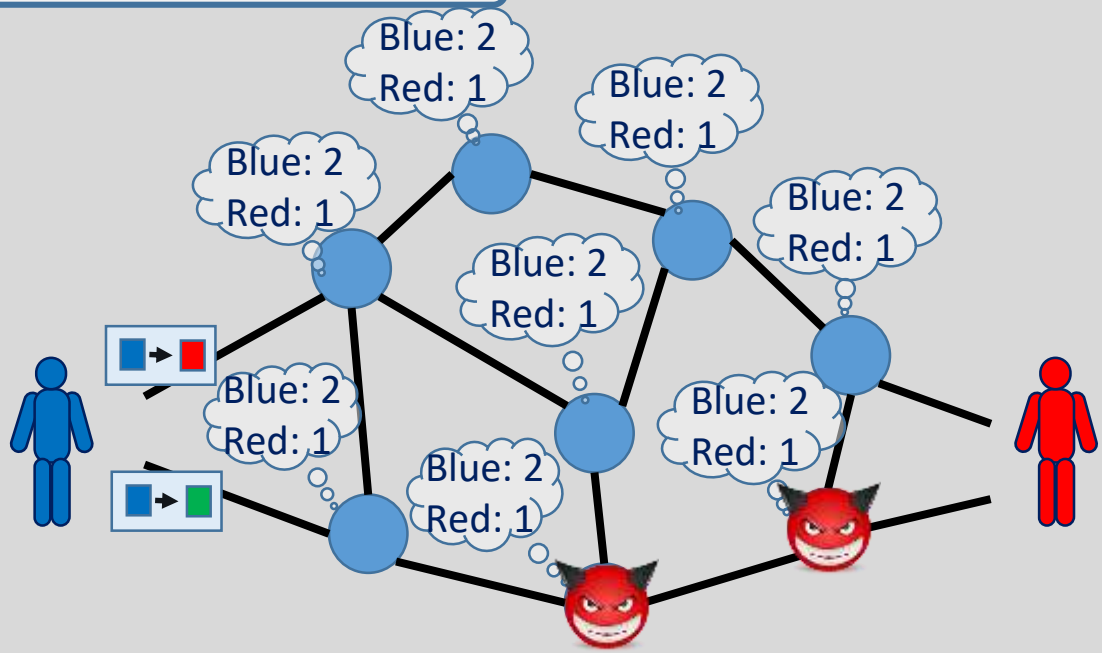
We are (possibly) undergoing a similar disruption with money transfer / assets / trade of digital goods.

- How do we behave in this new world?

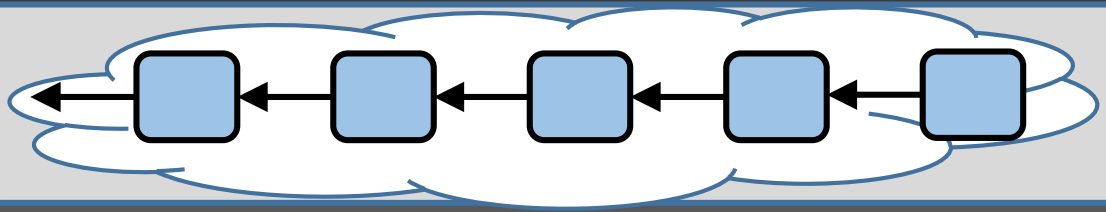
Digital Payments



Bitcoin & similar currencies



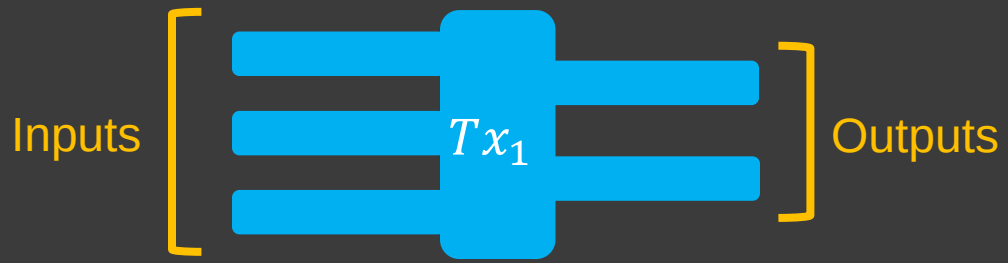
Secured by
“proof-of-work”



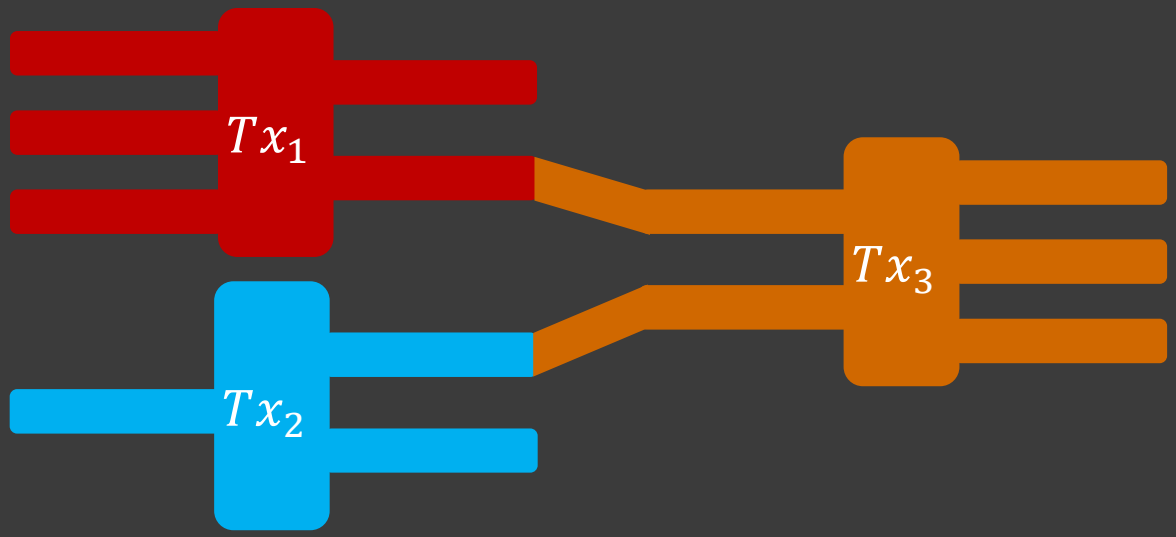
The Blockchain:

A record of transactions

Bitcoin’s transaction

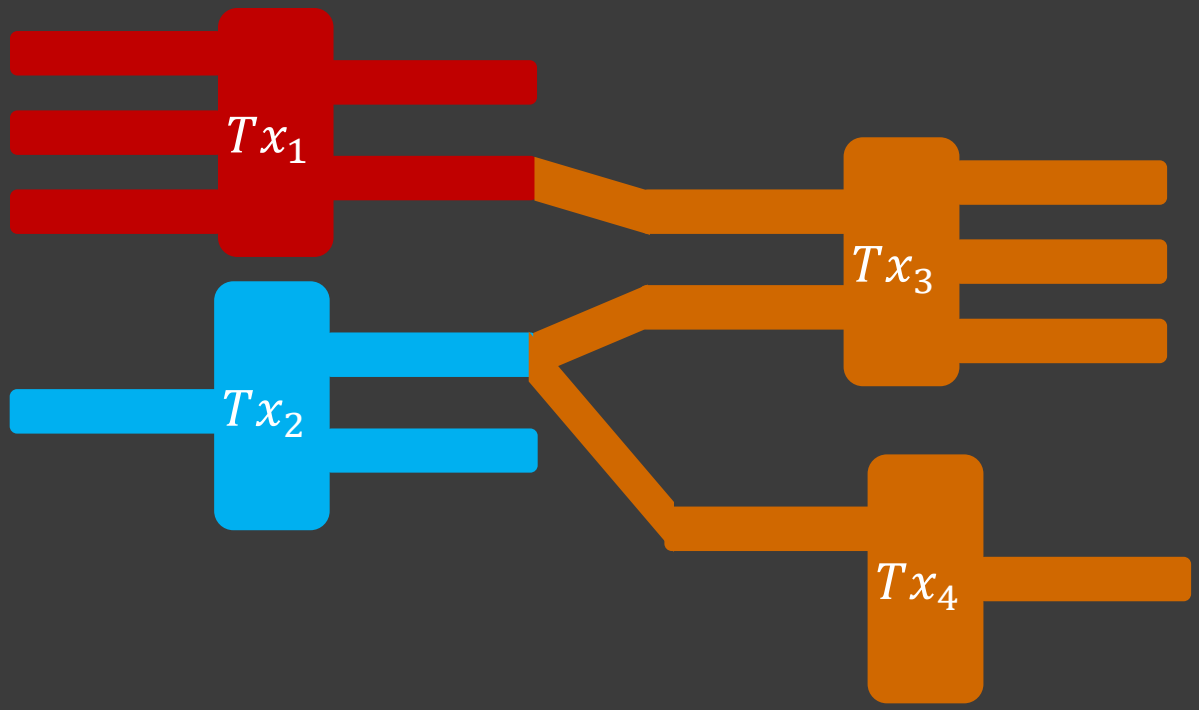


Bitcoin’s transactions

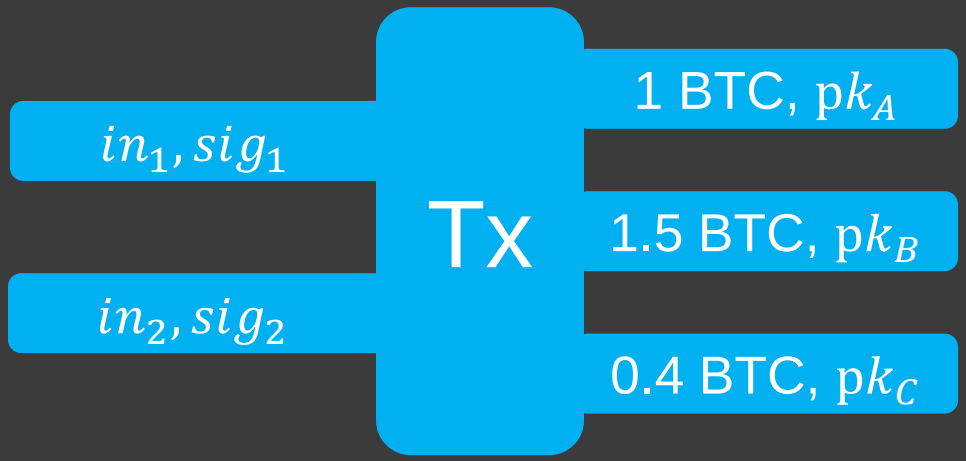


- UTxO vs account model.

Double Spend



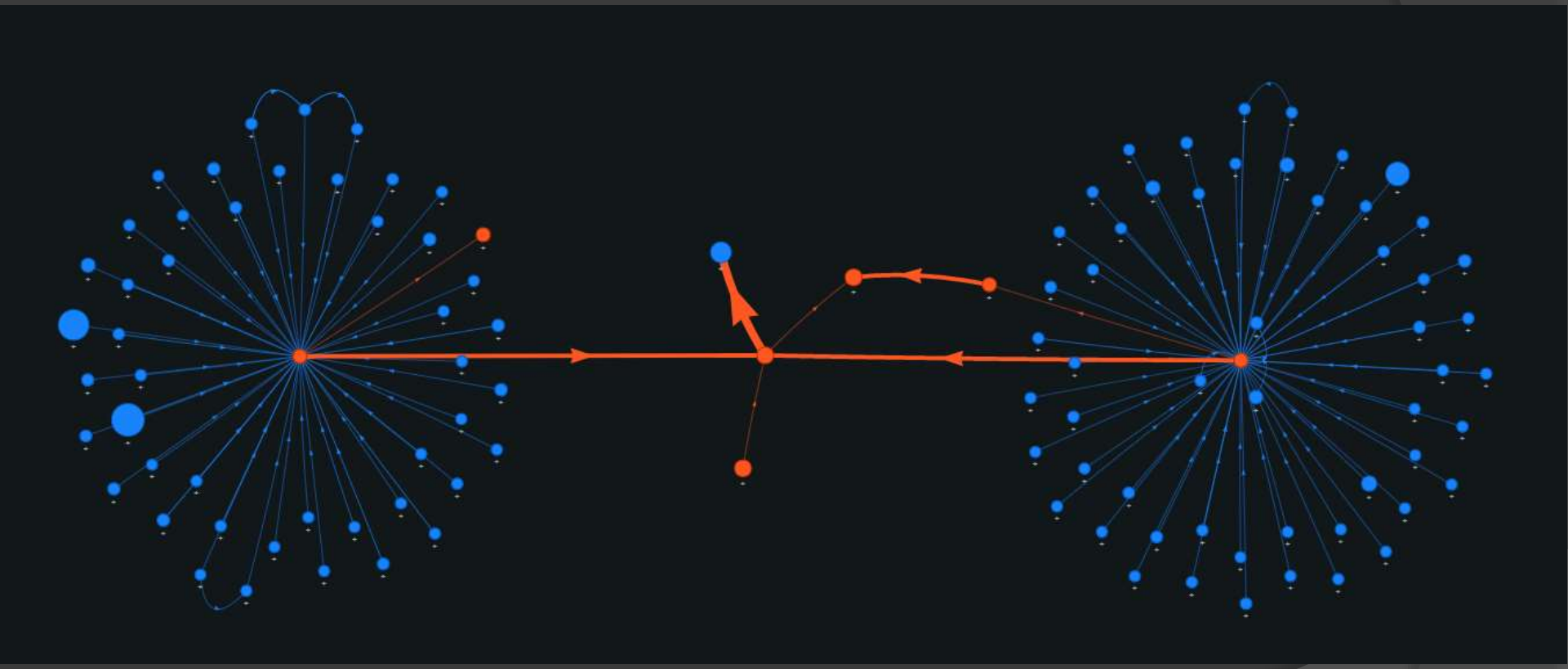
Bitcoin is pseudonymous



A new pubkey for every transfer (whenever possible)
Still,

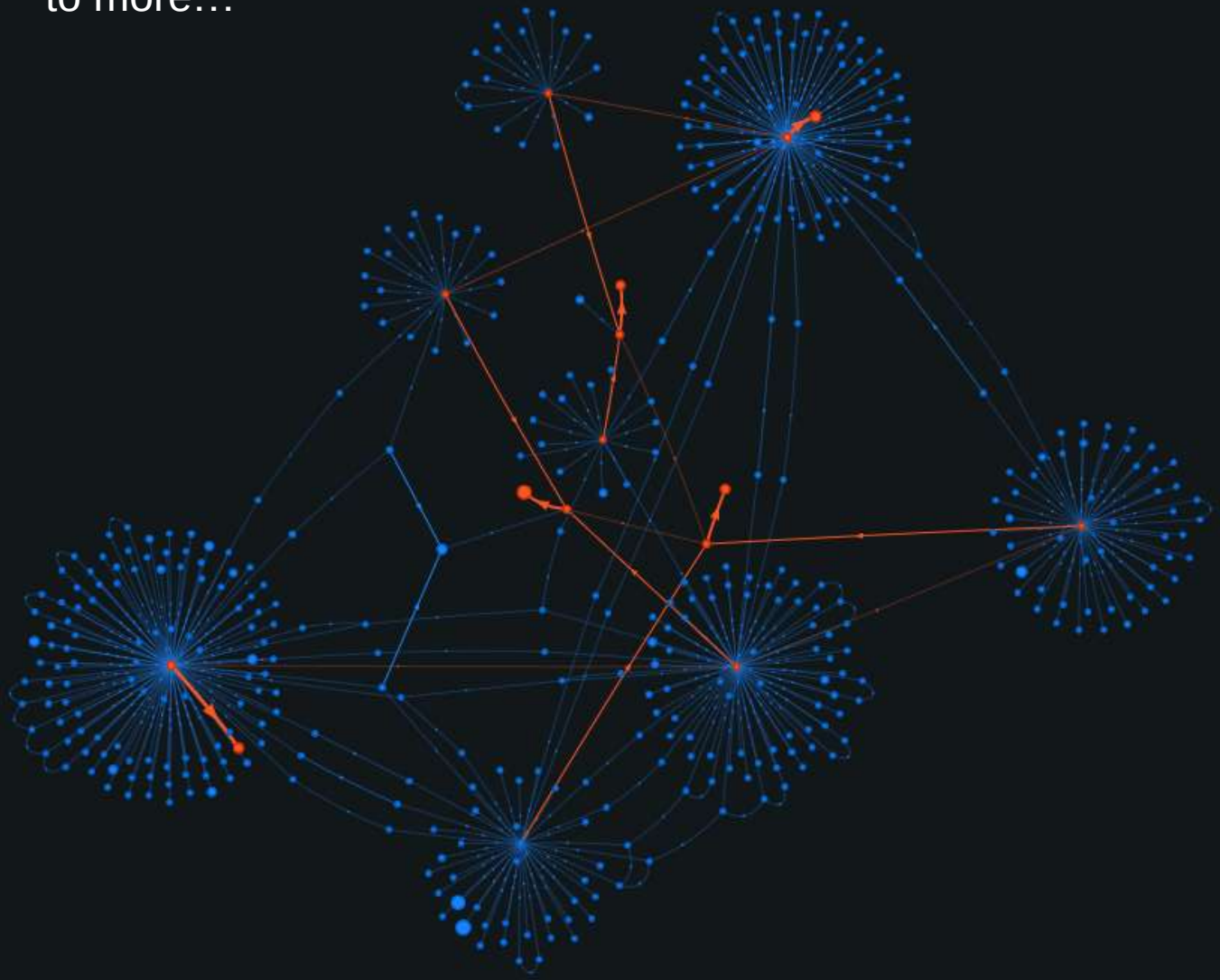
- Amounts revealed
- Some Linkability

100BTC of paymets to Locky aggregated into an exchange
(payments 0.5,1,2,3,7 BTC collected into two 50 BTC transactions)



Generated using oxt.me

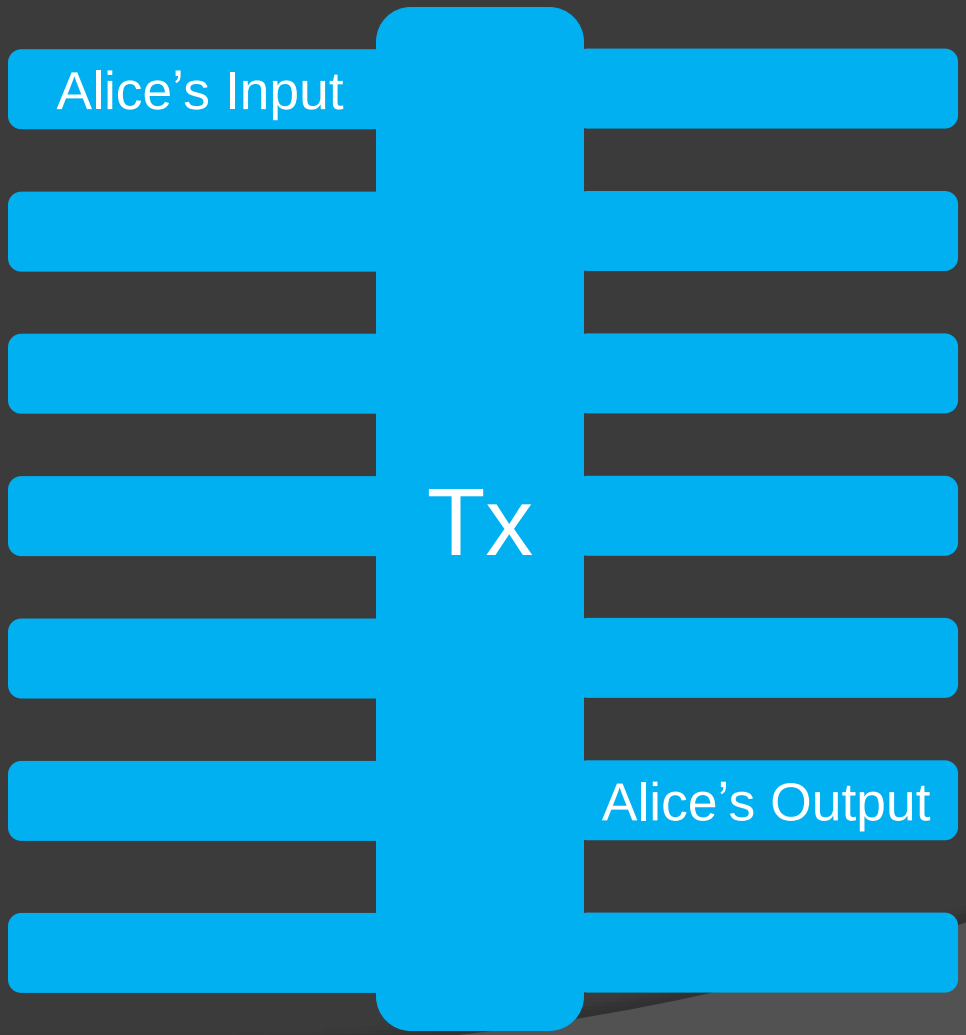
Following change addresses leads to more…



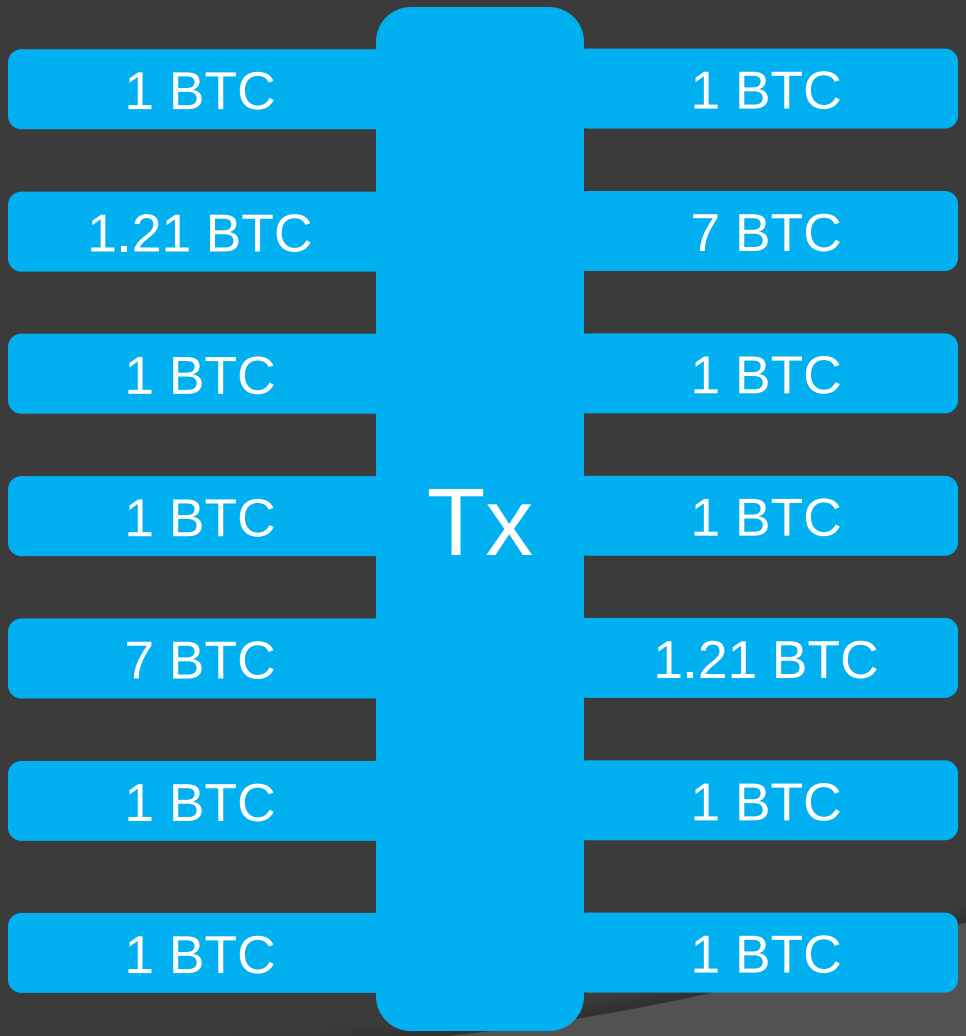
Generated using oxt.me

Generated using oxt.me

Coinjoin

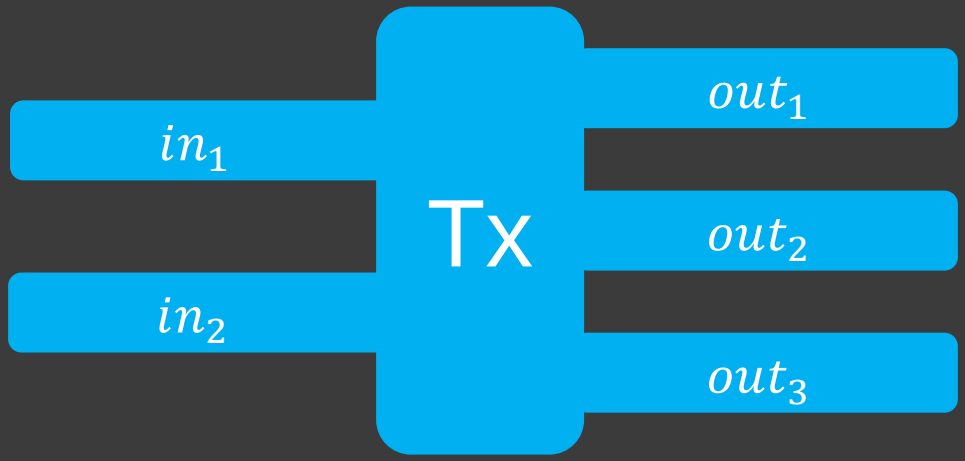


- Must be careful about amounts, partners




Transactions laundering
money in a mixer.
Generated using oxt.me

Hiding amounts



Must verify:

sum of inputs = sum of outputs

No output is negative

Use cryptography to do this.

Degrees of knowledge:

- We see everything (power to investigate without user knowing)
- The user can prove to us (voluntarily or after being compelled by court order) things about his holdings
- No one can see anything and no one can prove anything. (No such system exists!)

Advanced Privacy coins

- Everything on the blockchain is encrypted.
- No one can see sender, receiver, amount.
- (but sender and receiver know, and can prove they own and transfer money)

Problem: how do we validate

Solution: zero-knowledge proofs

Outline

Zero Knowledge Proofs

- 2012 Turing Award
  Goldwasser & Micali
  (Original paper in 1989)

- Prove a computational statement, without revealing some of the private input.

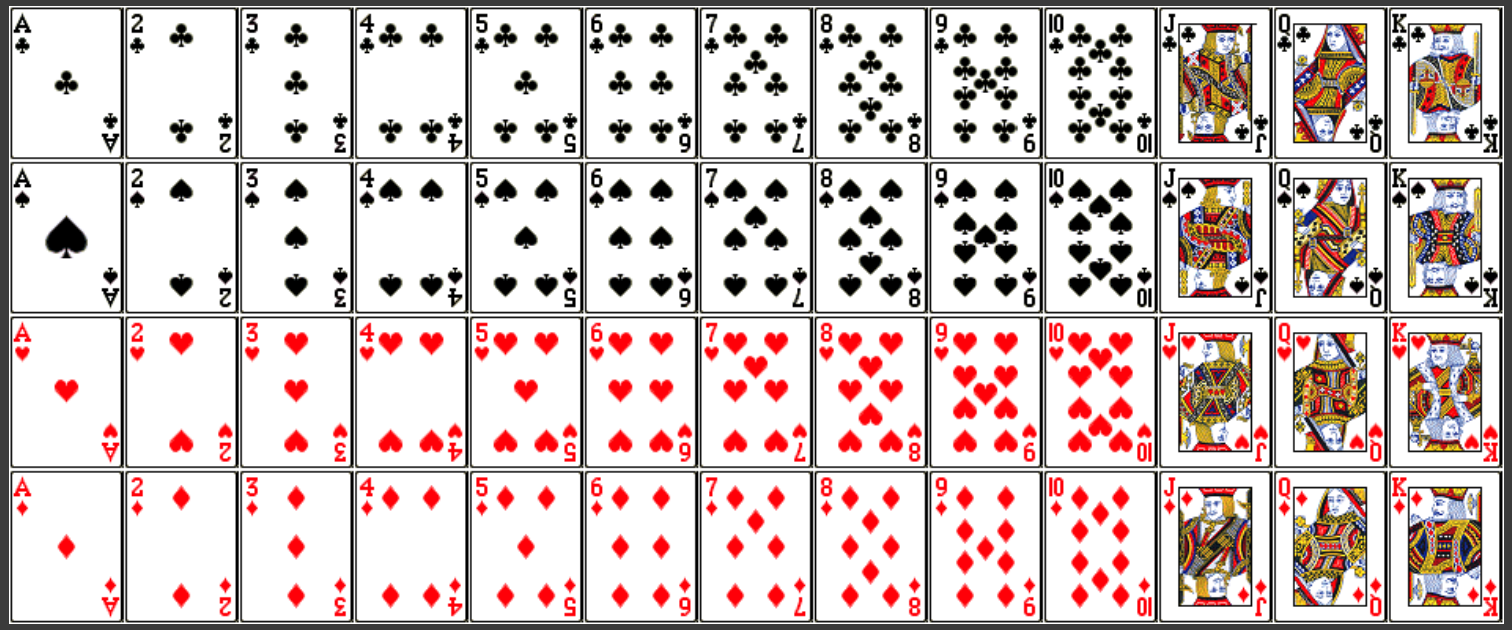
- Newer research has made ZKPs feasible (run in reasonable time)

What are these

"Zero Knowledge Proofs"?

An Example...

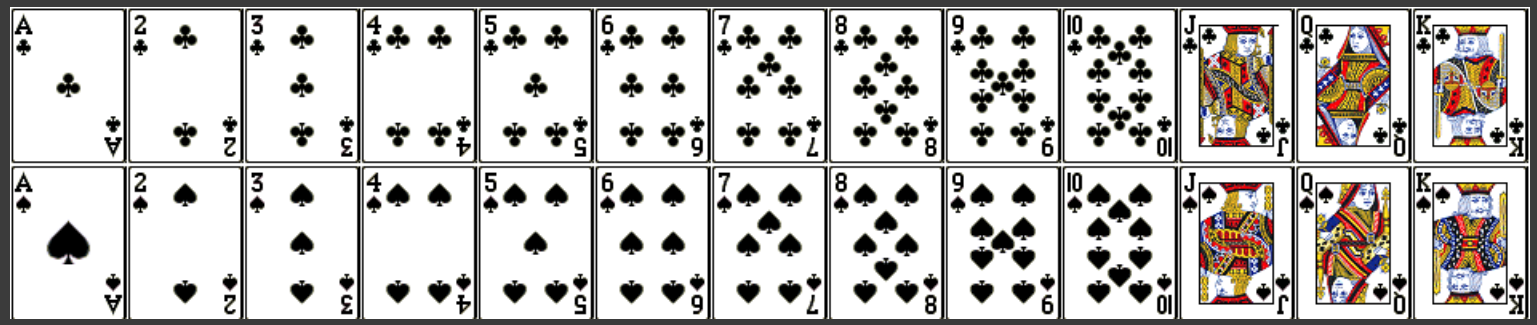
- Alice & Bob are playing cards
  - In the deck: 26 red cards + 26 black cards



- Alice removes a card and keeps it secret
- She states “My Card is Red!”

Bob Asks Alice to prove this, but Alice wants to keep the rank of her card secret.

- She hands Bob all black cards in the deck.

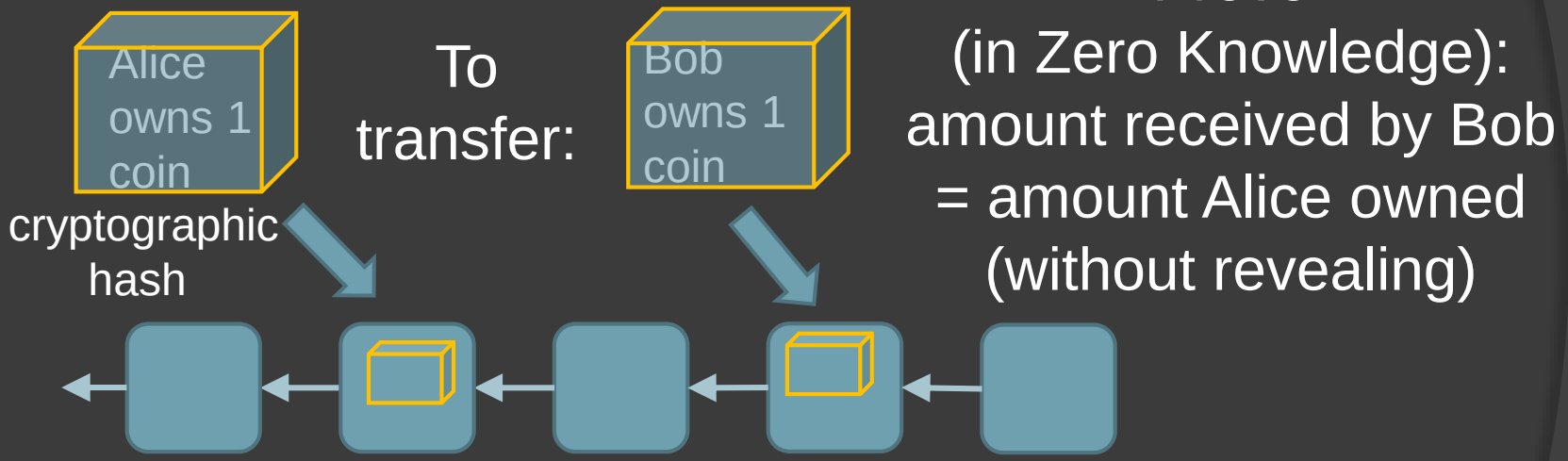


- He checks that none are missing, and is convinced, but gains no knowledge of the rank.

Advanced privacy layers

Zero knowledge proofs applied to blockchains:

(ZeroCash [Ben Sasson et. al])

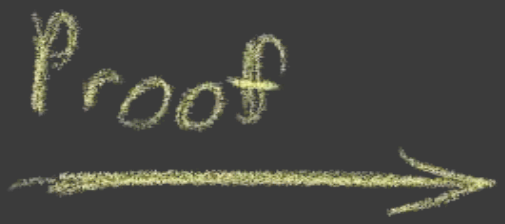


Outcomes:

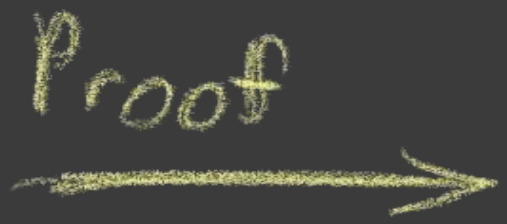
1. Cannot see amounts
2. Cannot link payments

But, transactions are still validated.

- The account I am sending to is private, but it’s not on a black list
- I paid taxes on this income



- This transaction is below 10K or it is above 10K and was approved (but I won't say which of these happened!)



- I’ve sent Regulator A encrypted details.
- I’ve sent the decryption key to Regulator B.

Many more uses

- Insurance
  - According to GPS, I don’t go over the speed limit (but don’t reveal which GPS trace is mine)
- Supply chain
  - I’ve ordered all raw materials needed to produce the items I promised to sell you.
- Loans
  - I have a high credit score (but don’t show credit history)
  - I did not borrow against this asset with another lender (but keep activity private)