Bitcoin,
a look under the bonnet

Boris Škorić
TU/e

ANP colloquium
May 26, 2015

Outline

- Bitcoin 101
- Crypto
  - one-way functions
  - digital signatures
- Transactions
- Mining
- Binding it all together
- Anti-censorship
- Cautionary notes

What this talk is NOT about

NOT:

- History of cryptocurrencies
- Economics / politics
- How to become rich
- How to attack Bitcoin

Bitcoin 101

- Cryptocurrency
  - assets are purely digital
  - secret key gives access to "account"
  - crypto for proving ownership
  - crypto for signing transactions
  - crypto for creating new money
- Decentralized
  - peer to peer communication
- "Block chain"
  - all transaction history is public

Quick facts about Bitcoin

- Created in 2008 by "Satoshi Nakamoto"
  - open source
  - based on lots of prior work
  - but with unique combination of ingredients
- Accepted by > 10^5 merchants
  - easy (international) transfer of money
  - PR value
- Current exchange rate:

  1 bitcoin = 209 euro

Who is Satoshi Nakamoto?

1 bitcoin = 10^8 Satoshi

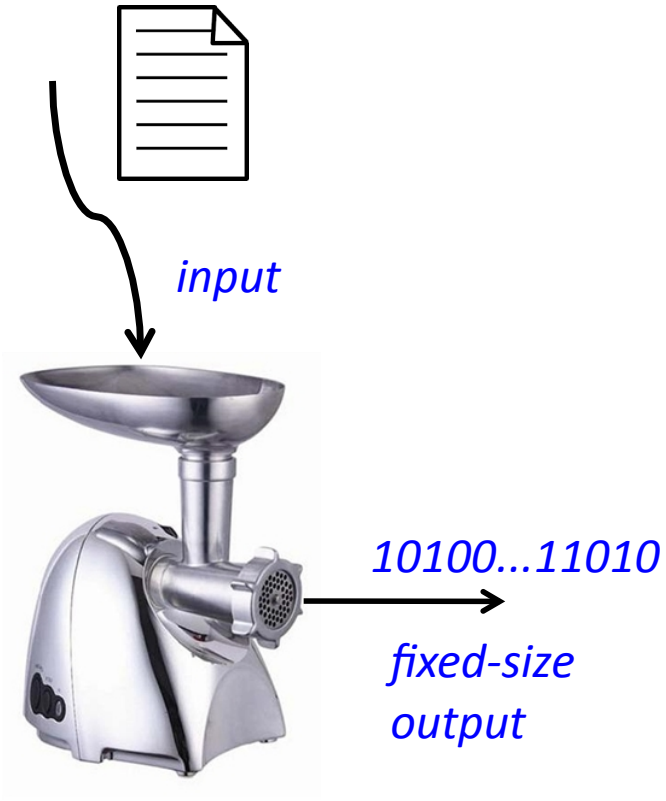
Dorian S. Nakamoto?
(Los Angeles, March 2014)

There are many allegations

Concept #1: One-way hash function

"Cryptographic hash function"

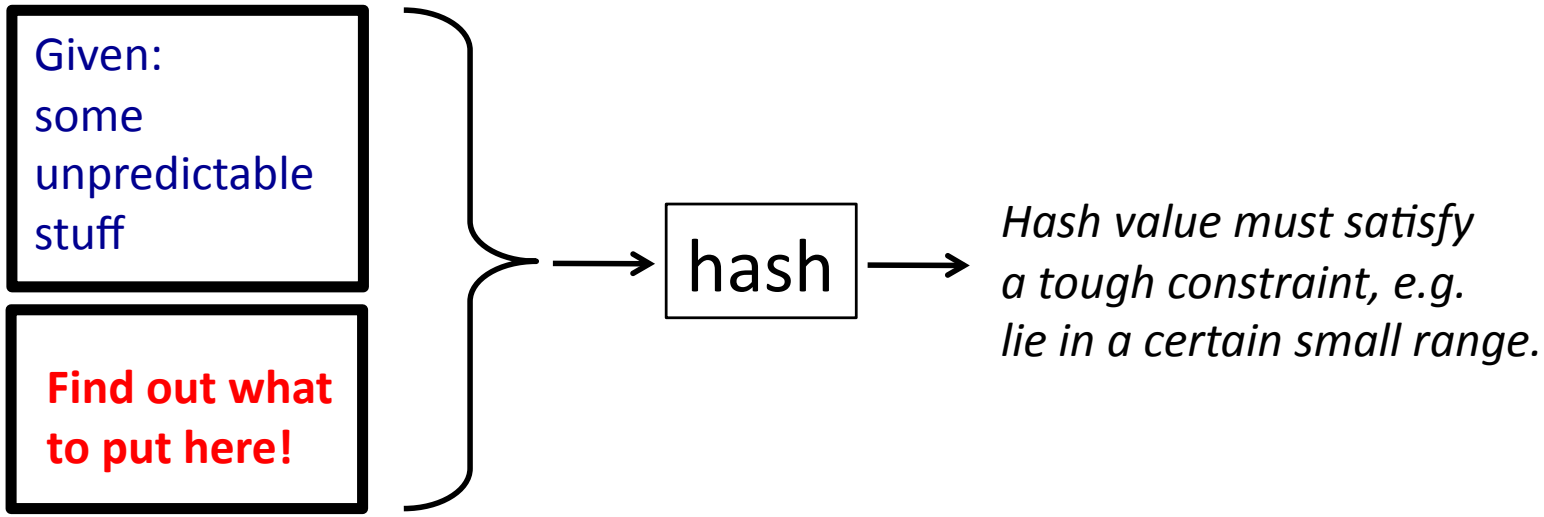
- easy to compute
- very difficult to invert
- low prob. of collisions
- compressed & unique digest



Example: SHA256

- arbitrary input size
- output size 256 bits

Proof of work



- Solving this problem costs a lot of trial & error => CPU time.
- Solutions are easily verified!

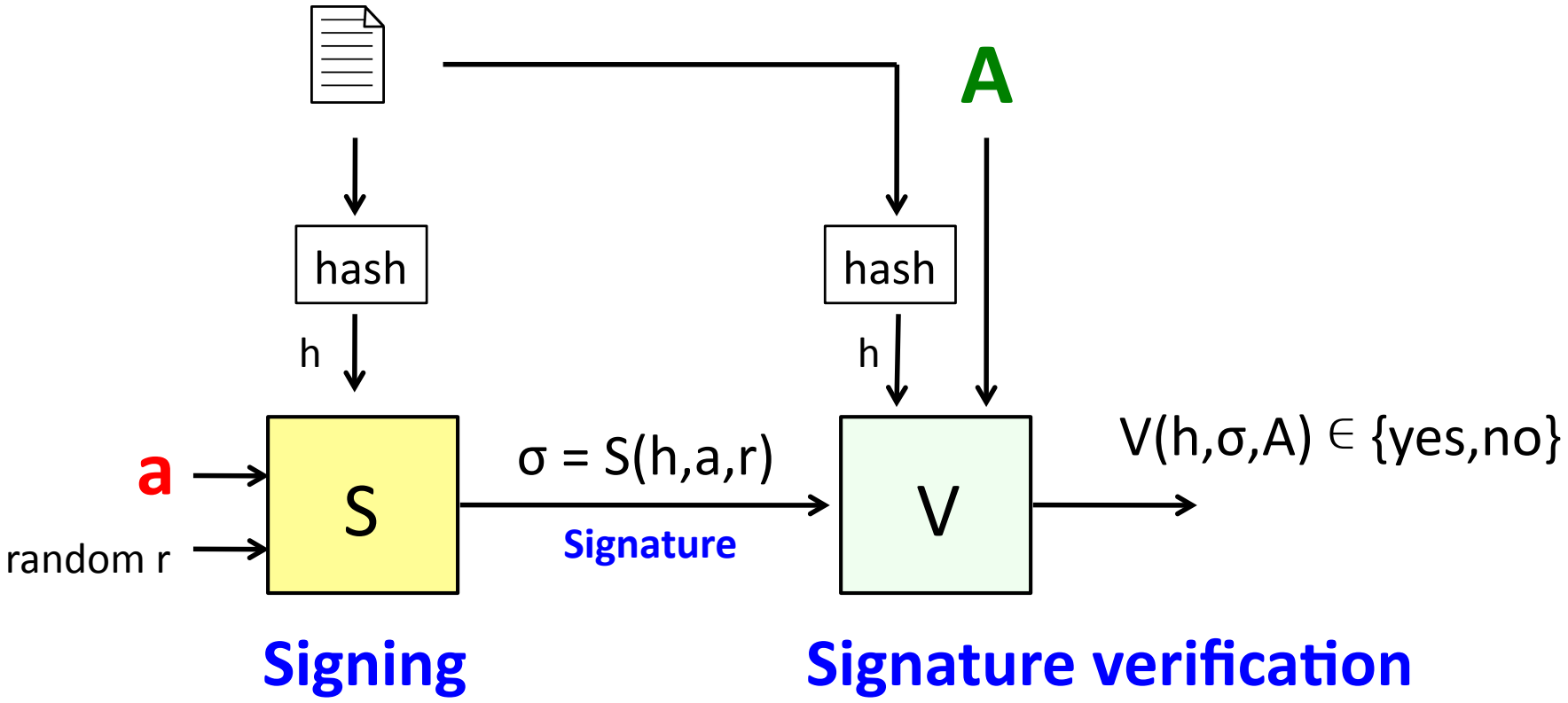
Concept #2: Digital signature

Main concept: key pair (**a**, **A**)

A *can be computed from* ***a****; the reverse is difficult*

private key (secret)

public key



Digital signatures

Anyone can *verify* a signature

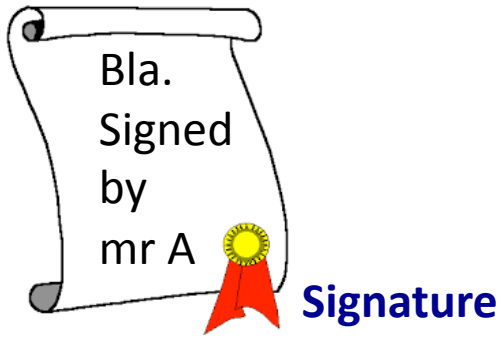
- only the public key is needed

Only one person can *generate* signatures consistent with *A*

- private key **a** is needed

Successful verification of signature proves two things

1. message integrity
2. authenticity



"The holder of the private key confirms this message"

Bitcoin accounts

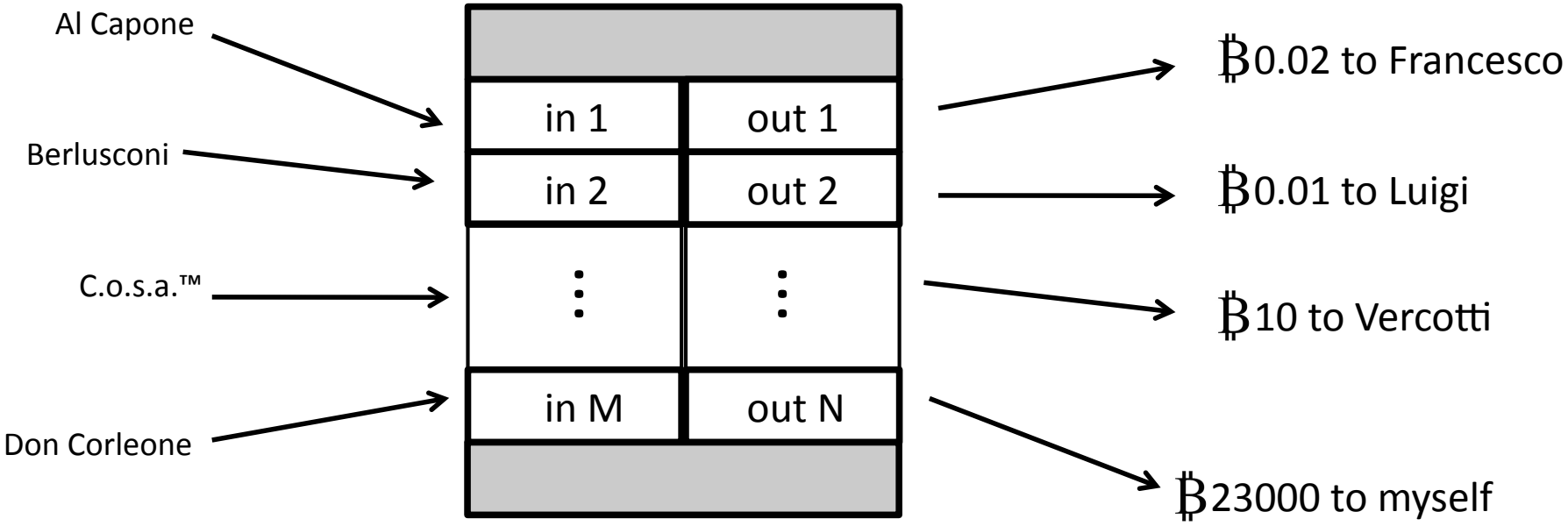
Choose your own key pair

- public key is your "account number"
- private key gives access to account
  - prove that the account is yours: signature
  - confirming a payment: sign it

You can make as many accounts as you want, completely for free !

Bitcoin transactions

`Transaction` data structure

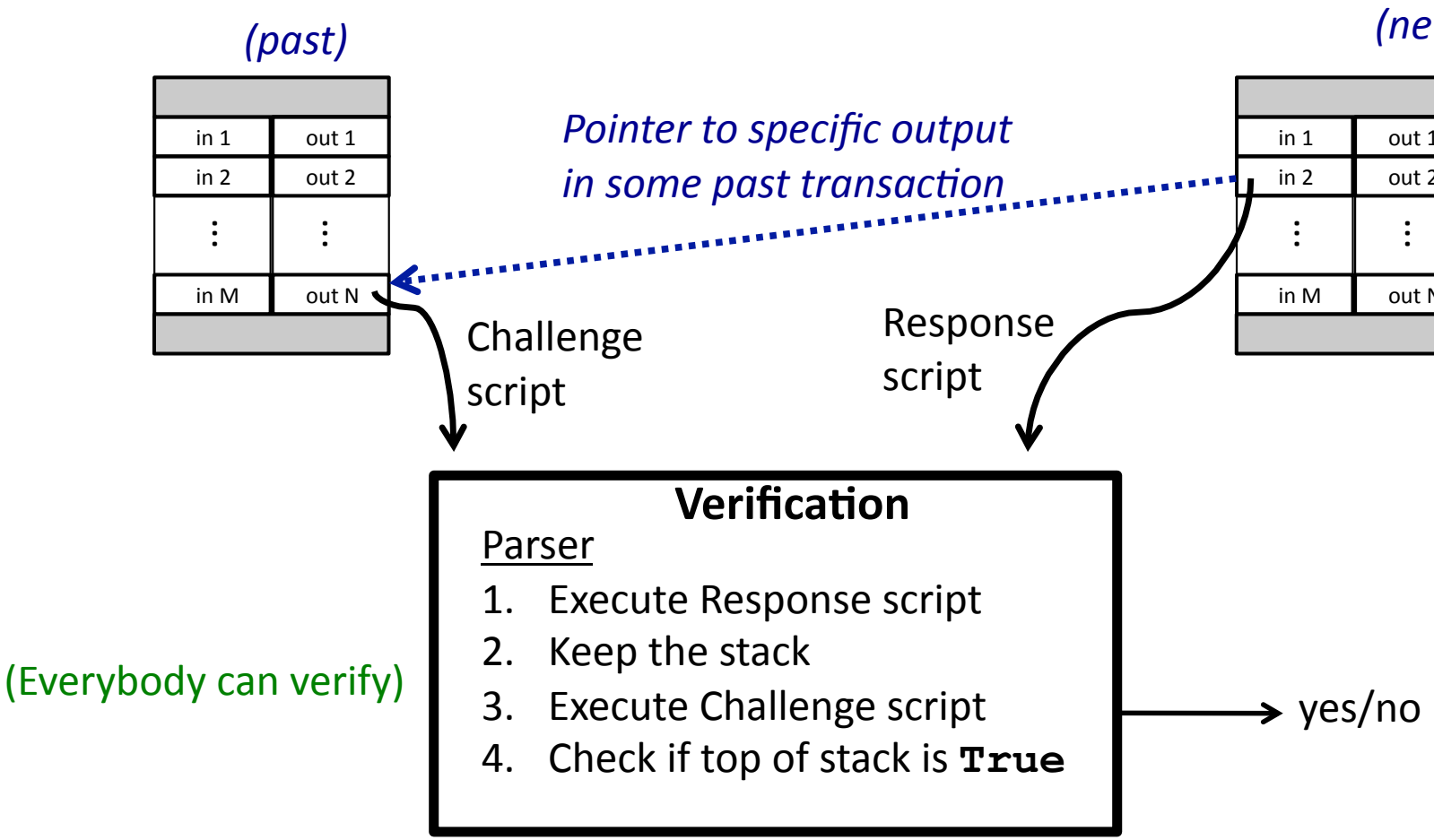


"in" data:

- payments to your account
- each "in" data proves ownership
  - digital signature
  - possibly different accounts
- each signature also covers all the "out" data

Small transaction fee: out < in

Transaction: `Script` language



The `Script` language is too expressive

- leads to implementation bugs
- many options are now forbidden

Allowed challenge script types

Type	***Prove knowledge of:***	
Pay to Pub.key	private key	
Pay to Pub.key hash	pub.key & priv.key	
Multisig	n out of k private keys	n,k heavily restricted
Nulldata	---	40 bytes arbitrary data; Max one Nulldata per transaction
Pay to script hash	challenge script + whatever it demands	Must be one of the above script types

Mining

Users

We want to do these transactions:

peer-to-peer

Miners

- Collect transactions
- Signatures OK?
- Fees OK?
- Scripts OK?
- Double spending?
- Proof of work

(simplified view)

BLOCK

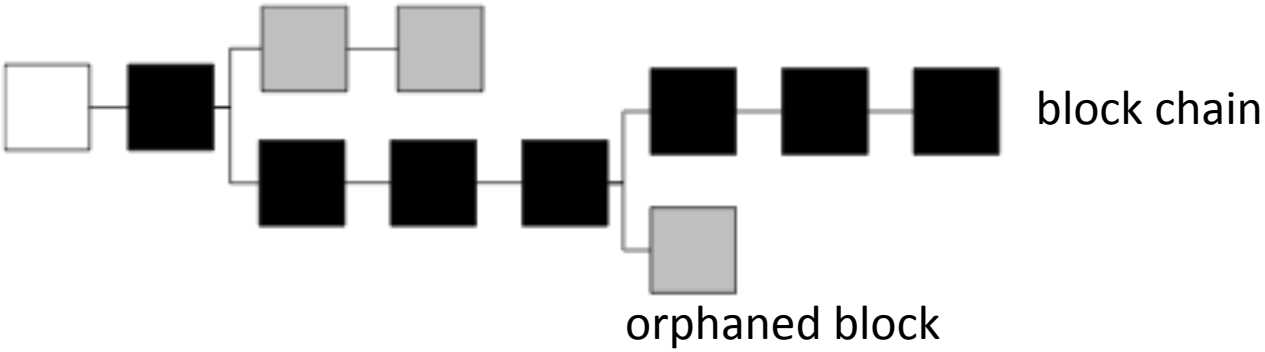
pointer to previous block
list of collected transactions
coinbase transaction
Find out what to put here

hash → ***should be smaller than target T***

$T \approx 2^{188}$

Lowered every 2016 blocks

Block chain



Incentives for the miner:

- reward for proof of work, currently 25 BC
- transaction fees

The incentives stabilize the system

- transaction confirmation mechanism brings reward

Anti-censorship

Whole block chain must be visible

- otherwise you cannot trust bitcoin
- Difficult to censor!

THE WORST THING ABOUT CENSORSHIP IS [redacted].

How to write data into blockchain?

- Control over data within transaction
- Plenty of options!

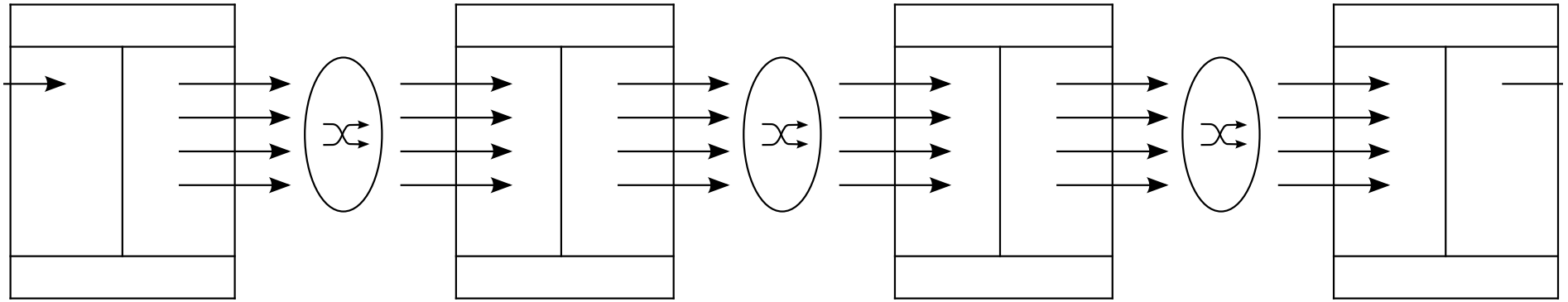
Krzysztof Okupski
MSc thesis, Dec. 2014:

"(Ab)using Bitcoin for an anti-censorship tool"

- Bitcoin specification document
- open-source tool

Embedding data in transactions

- Create 2^N accounts $\Longrightarrow$ N bits of info in account identifier
- Keep pumping ALL money through your accounts
- Pay to scripthash, with 1-out-of-14 multisig



Put information in:

- nulldata output
- choice of 14 public keys in challenge scripts
- permutation of "in" w.r.t. "out"
- splitup of the budget (combinatorics: "composition")
- signatures

Additional tricks:

- text only
- reduced character set
- compression

Fees: 16 Satoshi per embedded byte

Reading data from transactions

Reading is not dangerous

- Anybody can read the blockchain
- You don't even have to be part of the P2P network
- What you need to know:
  - where to look
  - how to parse

Remarks (1/2)

Black market, crime, etc.

- Public keys are pseudonyms
- But: full history is visible; exchange knows your identity
- Special effort needed for laundering/mixing/anonymizing

Theft

- ∃ specialized bitcoin-stealing malware
- Store private keys offline
- ***Use*** private keys offline (air gap)

Supposedly decentralized, but ...

- Small number of entities dominates mining
- Chinese mining farms

Remarks (2/2)

Bitcoin crypto seems flawless

- That's a first.

Bitcoin is cluttered

- scripts instead of fixed flowchart
- too many transaction types
- ....

Mining is a tremendous waste of energy

- Nothing useful is created, only "art"
- Find better confirmation mechanism

Summary

A look under Bitcoin's bonnet

- one-way hashes
- signed transactions
- proofs of work
- meshed together in the block chain

Well designed system basics

- stabilizing incentives
- solid crypto

Anti-censorship

- embed data in transactions
- cost = fees: ≈16 Satoshi/byte