WHAT IS BLOCKCHAIN?

A brief prelude to cryptocurrencies

Domagoj Vrgoč

WHAT DO KIDS TALK ABOUT THESE DAYS?

- Bitcoin/blockchain is all the rage on the net:
  - Already mainstream (your parents are asking should they buy bitcoin)
  - Blockchain proposed for everything these days
  - For insta gains of market value sell yourself as a "blockchain company"

- Main reason: money

COIN	PRICE	24H	MKT CAP
Bitcoin BTC	$9,578	2.13%	$162,973,122,834

WHERE DOES THIS COME FROM?

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

WHAT MAKES BITCOIN WORK?

Blockchain

Decentralized concensus

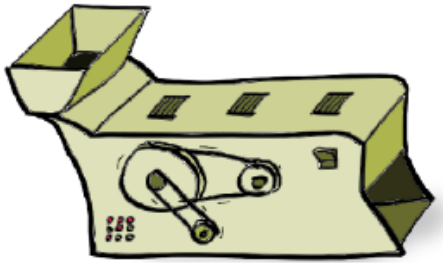
BLOCKCHAIN

- Publishing data in a transparent way:
  - Append only ledger
  - No modifications of published data are possible
  - To assure this I only need to store a few bits of information
  - Even for terabytes of data

- Not the same as Bitcoin; can be centralized

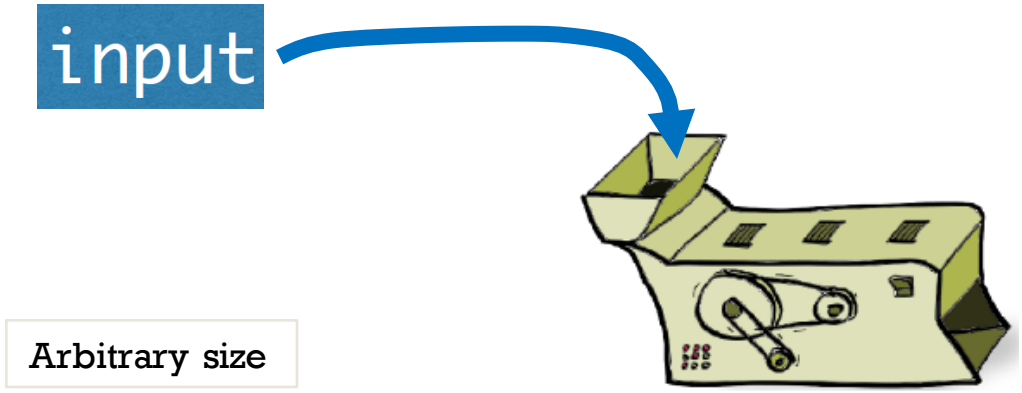
BLOCKCHAIN

- One technical ingredient: *cryptographic hash functions*



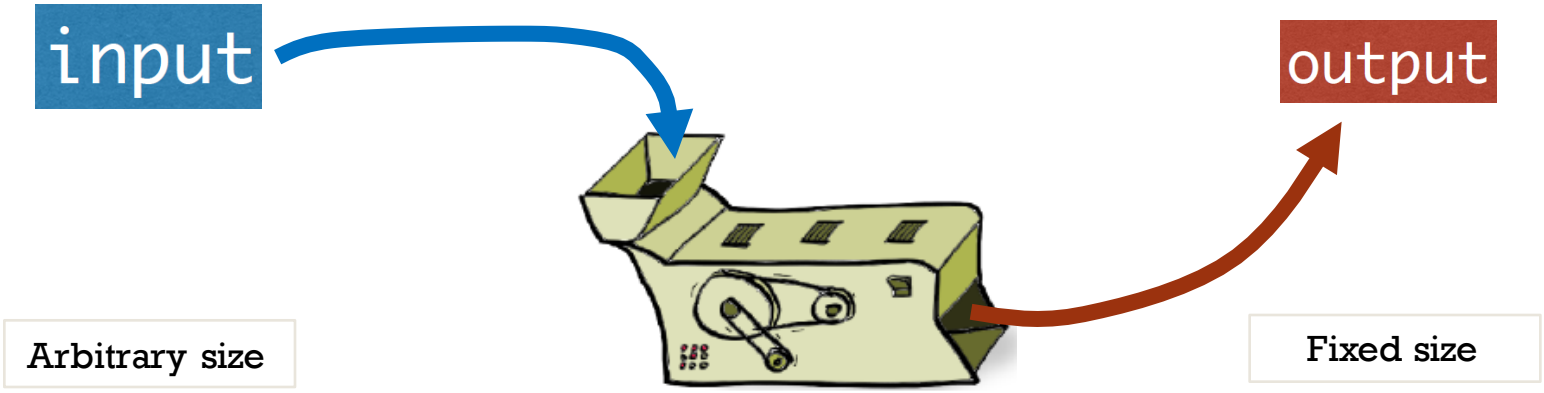
BLOCKCHAIN

- One technical ingredient: *cryptographic hash functions*



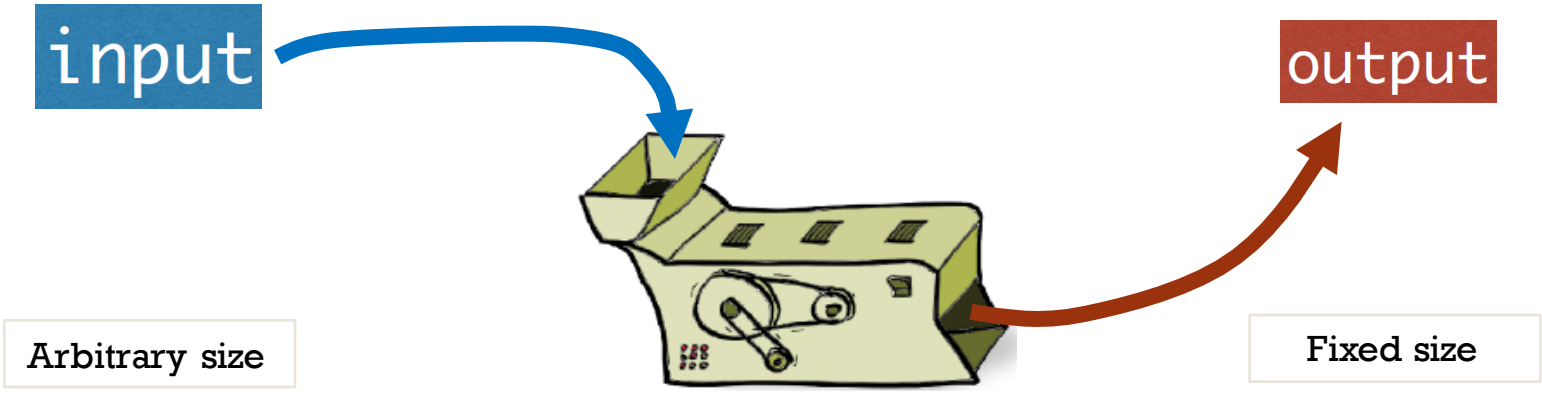
BLOCKCHAIN

- One technical ingredient: *cryptographic hash functions*



BLOCKCHAIN

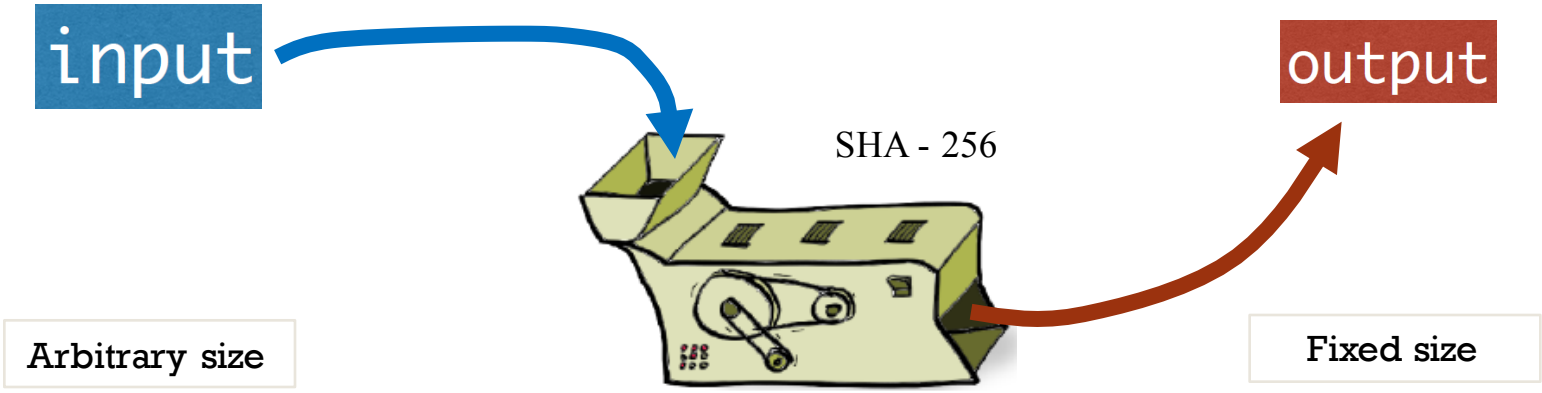
- One technical ingredient: *cryptographic hash functions*



Output gives no information about the input

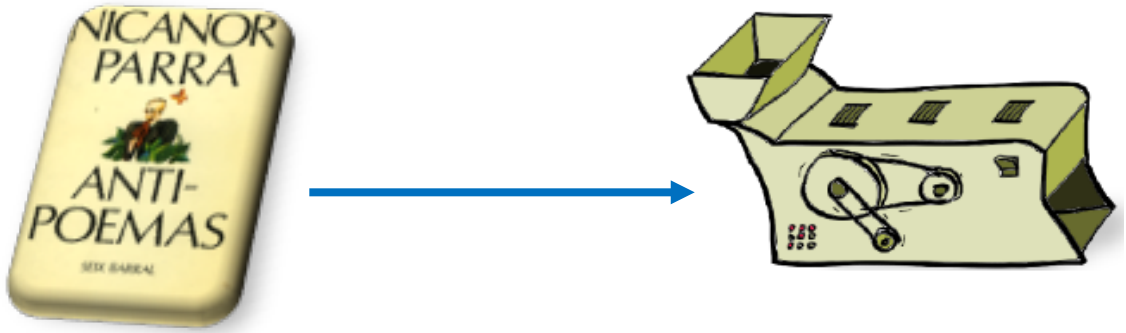
BLOCKCHAIN

- One technical ingredient: *cryptographic hash functions*

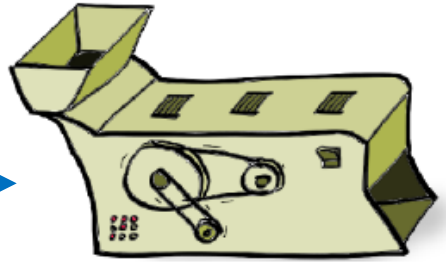


Output gives no information about the input

HOW DO HASH FUNCTIONS WORK?

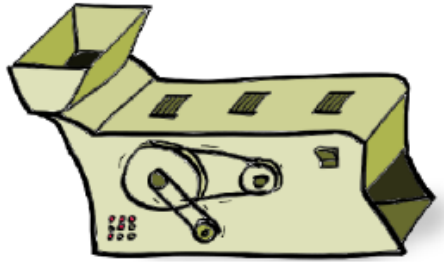


HOW DO HASH FUNCTIONS WORK?



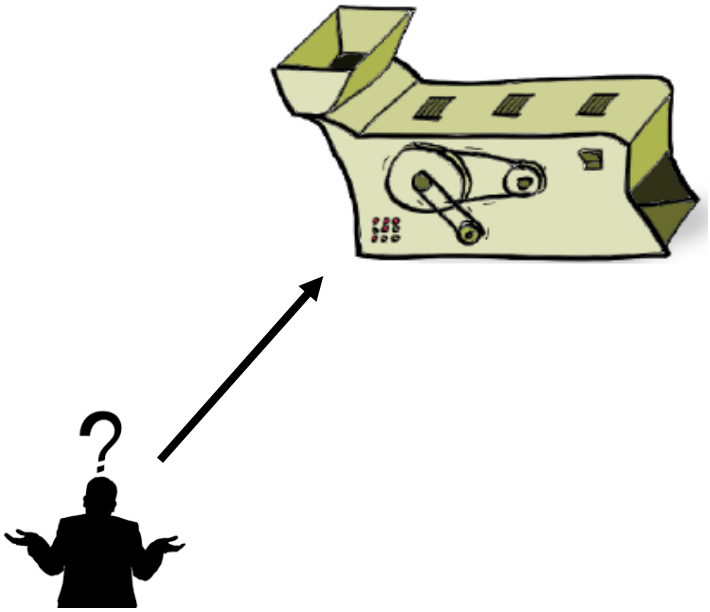
43115F48F39C0120C5D4D
3435DFD5CD933734963D4
75364A9C232B71DB601EE4

HOW DO HASH FUNCTIONS WORK?



43115F48F39C0120C5D4D
3435DFD5CD933734963D4
75364A9C232B71DB601EE4

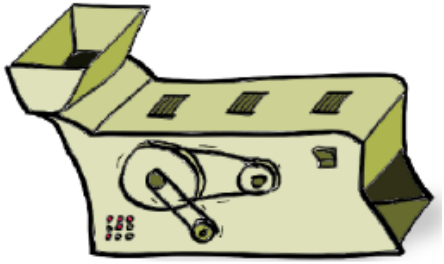
HOW DO HASH FUNCTIONS WORK?



43115F48F39C0120C5D4D
3435DFD5CD933734963D4
75364A9C232B71DB601EE4

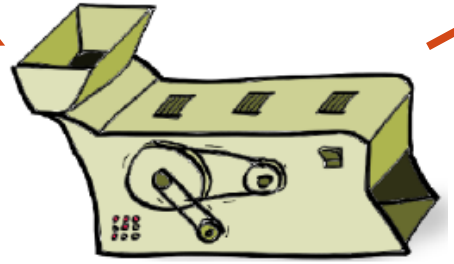
HOW DO HASH FUNCTIONS WORK?

Bitcoin



HOW DO HASH FUNCTIONS WORK?

Bitcoin

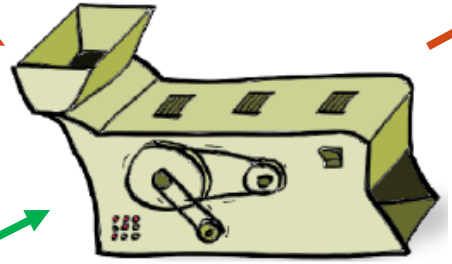


B4056DF6691F8DC72E5630
2DDAD345D65FEAD3EAD9
299609A826E2344EB63AA4

HOW DO HASH FUNCTIONS WORK?

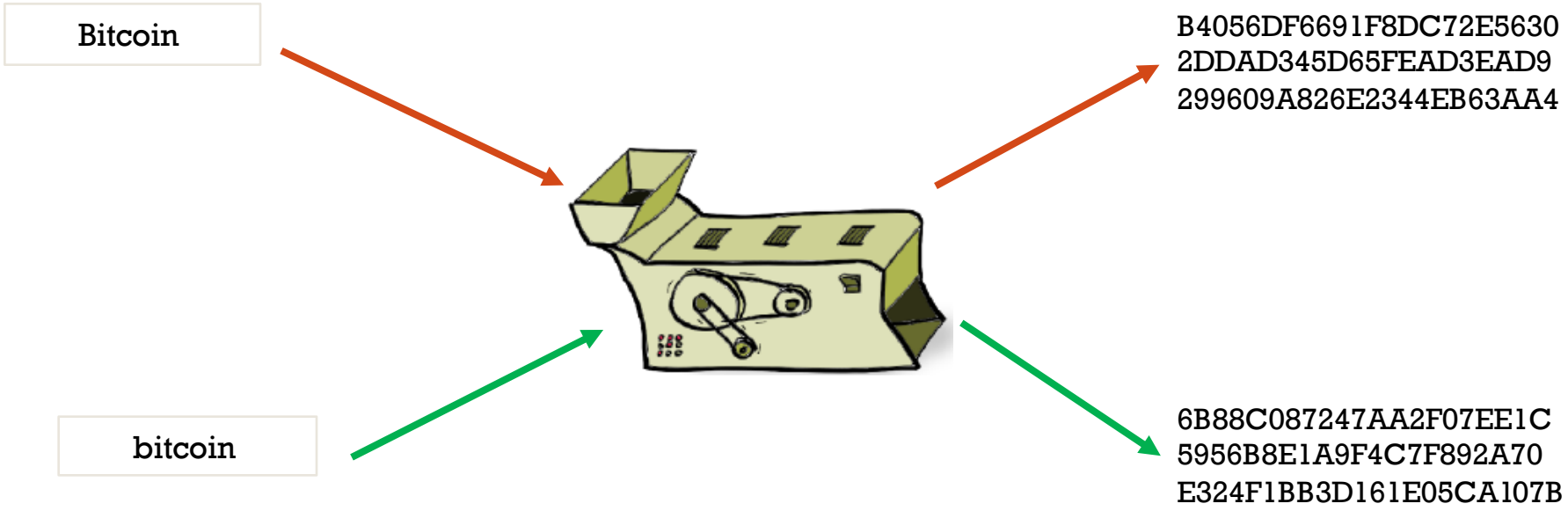
Bitcoin

bitcoin

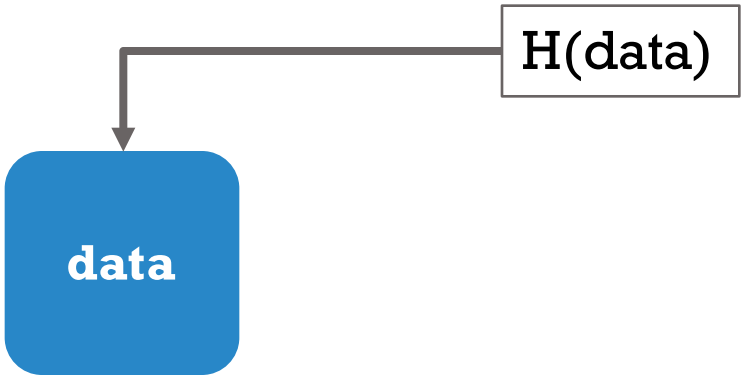


B4056DF6691F8DC72E5630
2DDAD345D65FEAD3EAD9
299609A826E2344EB63AA4

HOW DO HASH FUNCTIONS WORK?

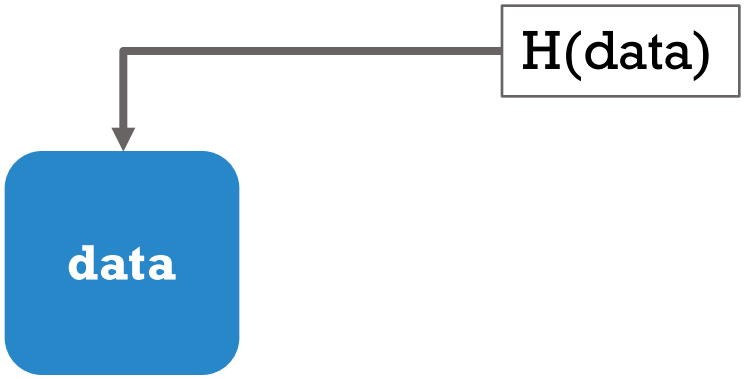


WHAT'S THE POINT?



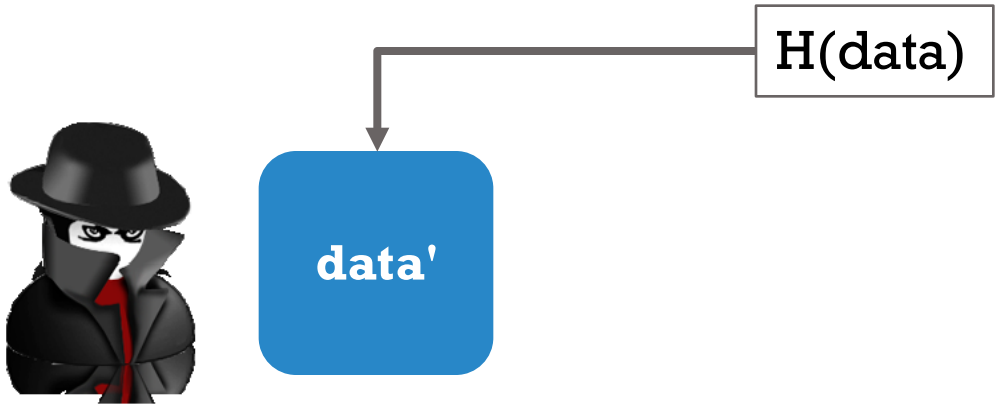
To verify that the data did not change, only the hash is needed

WHAT'S THE POINT?

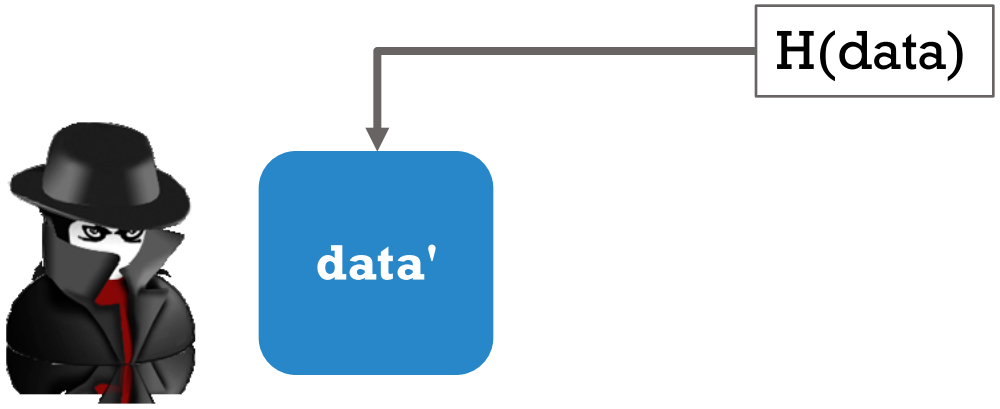


H(data)

WHAT'S THE POINT?

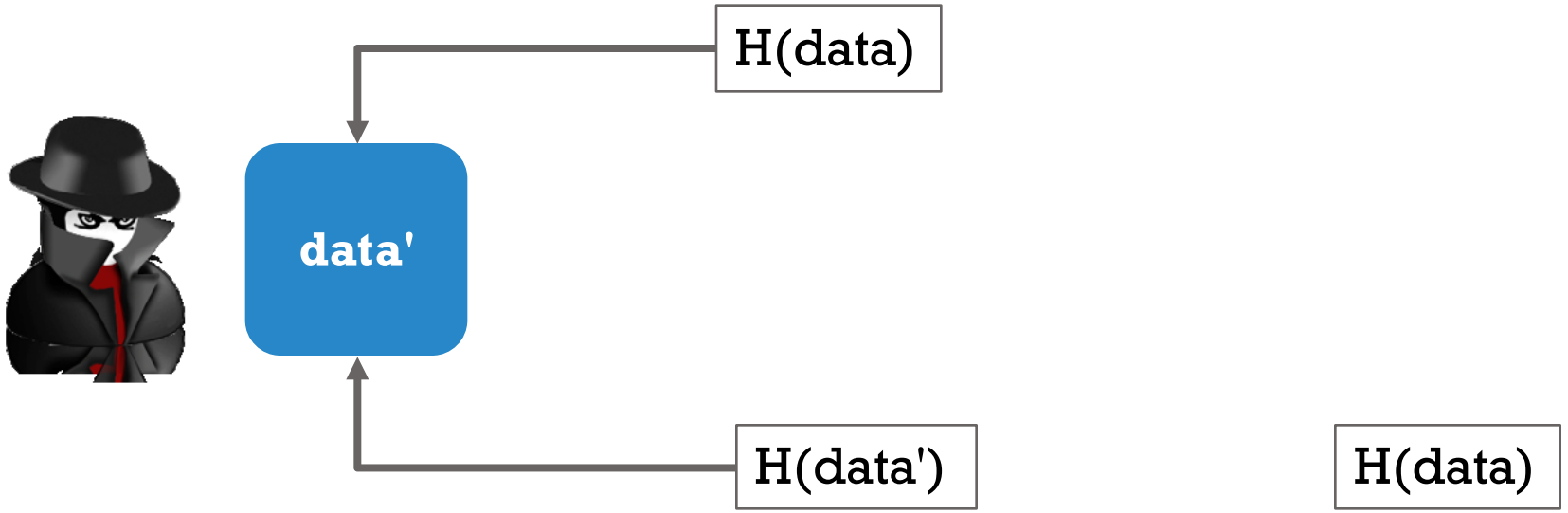


WHAT'S THE POINT?

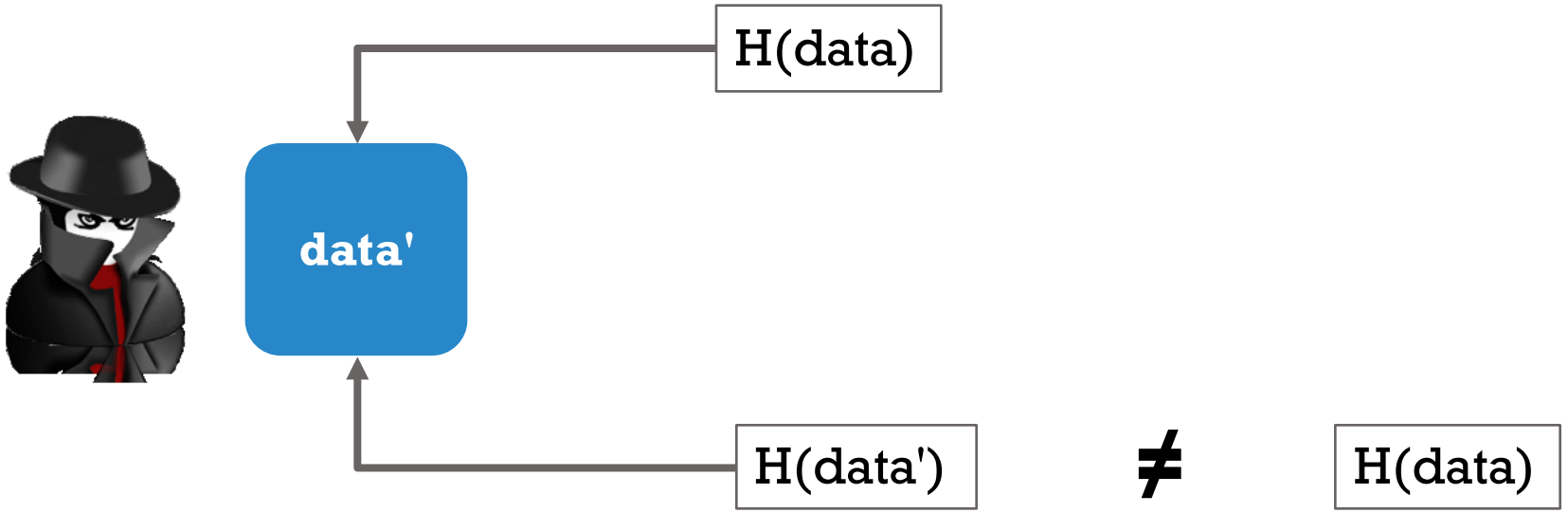


H(data)

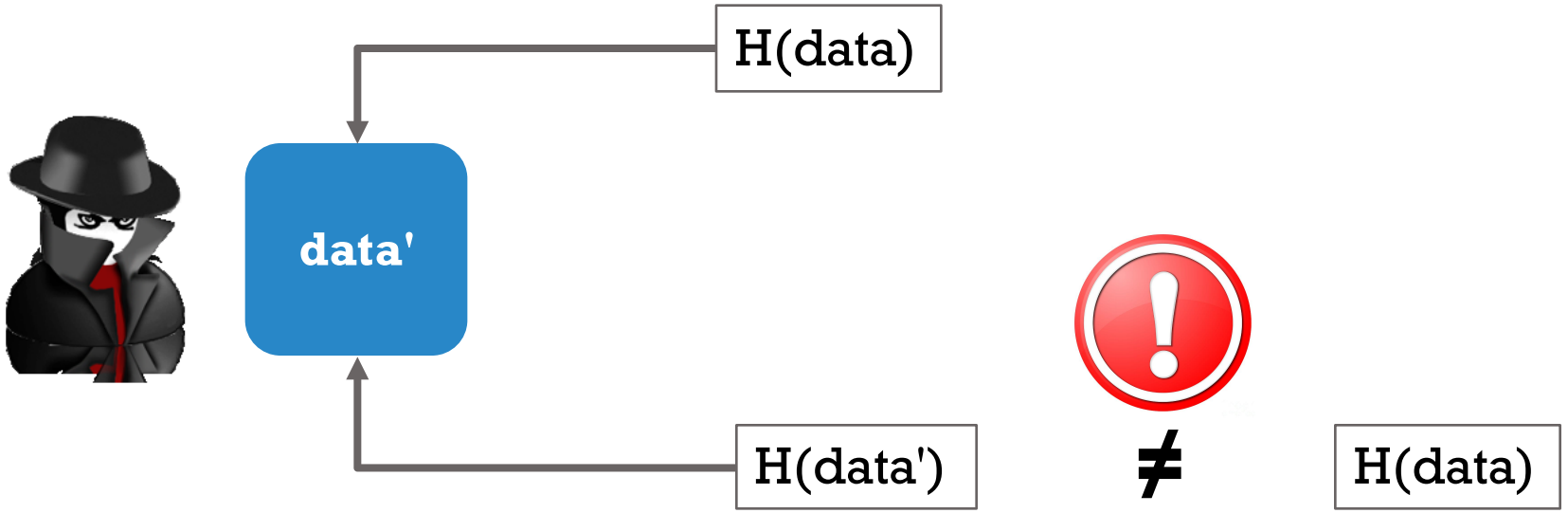
WHAT'S THE POINT?



WHAT'S THE POINT?

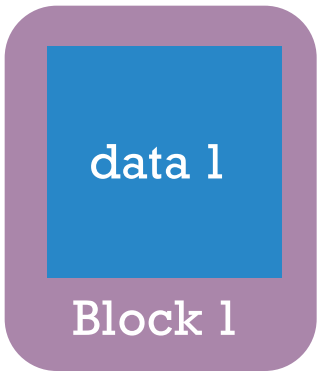


WHAT'S THE POINT?

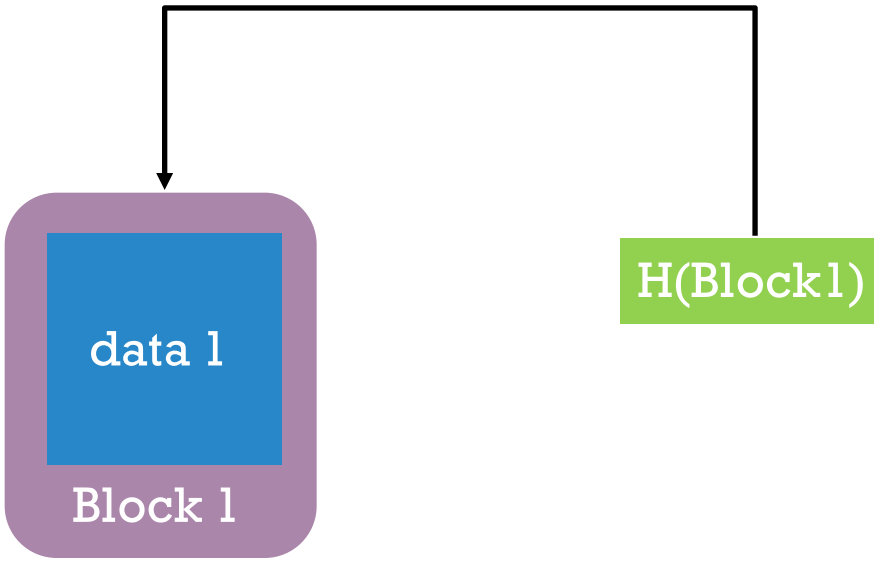


BLOCKCHAIN

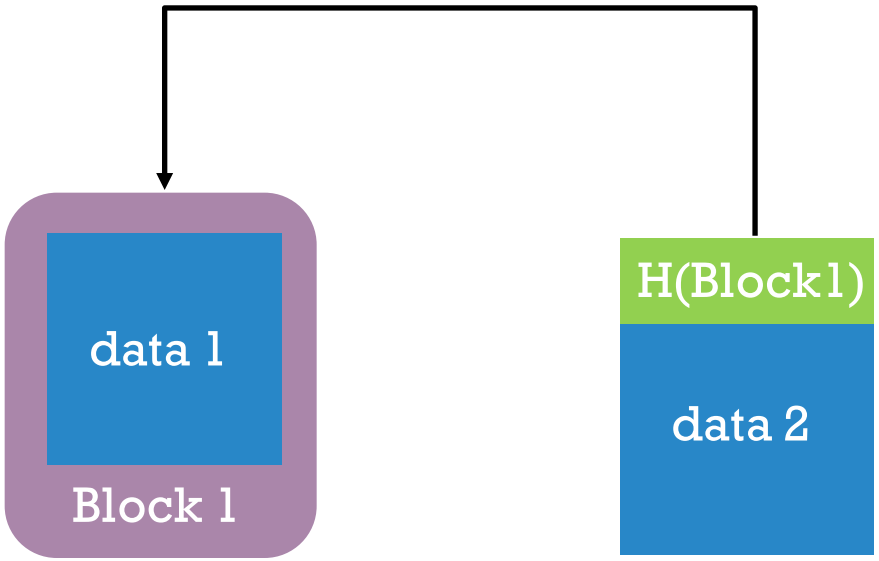
BLOCKCHAIN



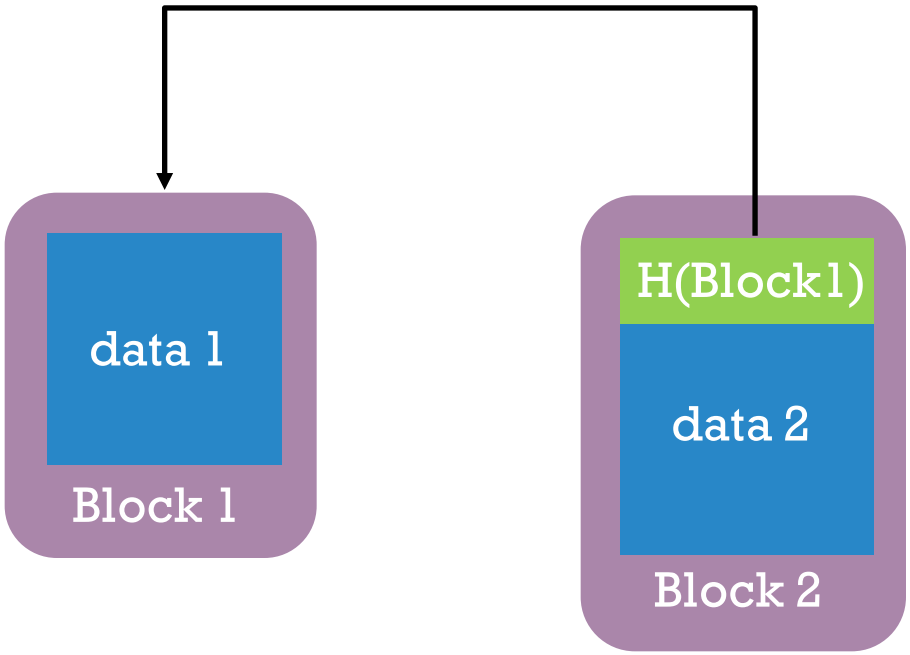
BLOCKCHAIN



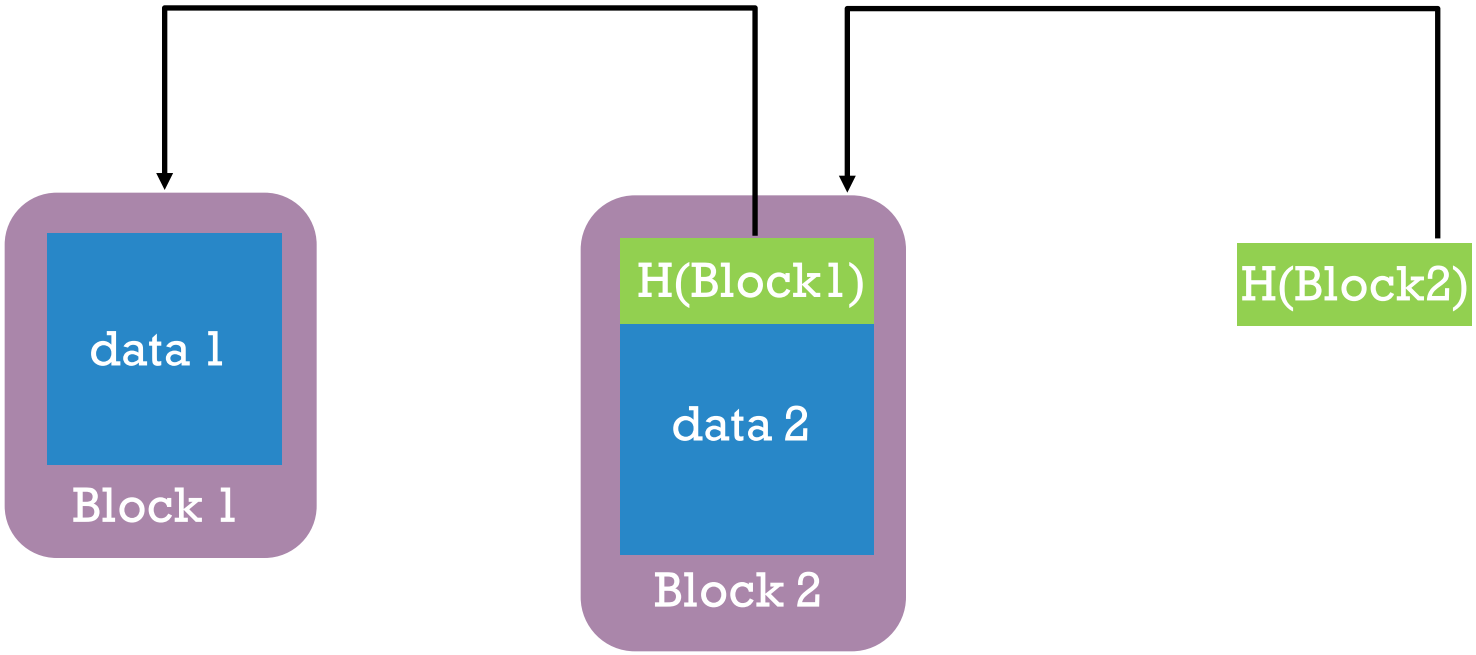
BLOCKCHAIN



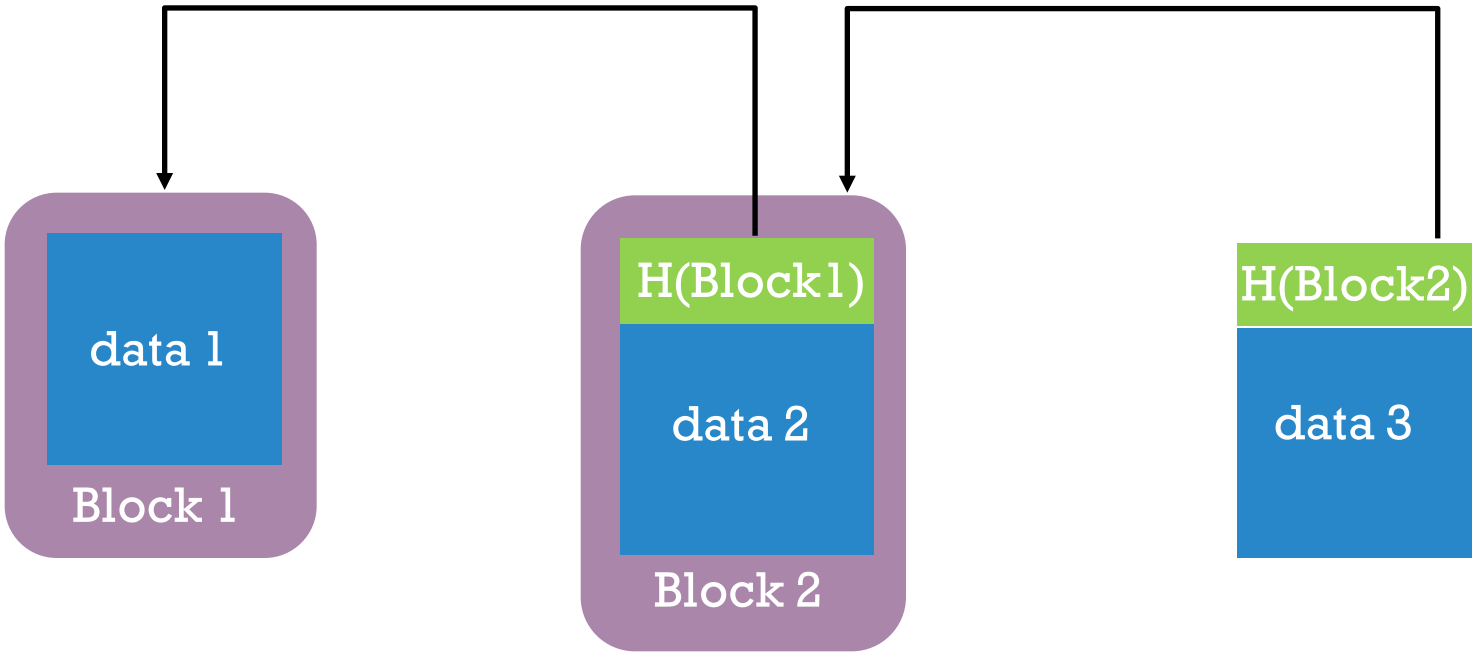
BLOCKCHAIN



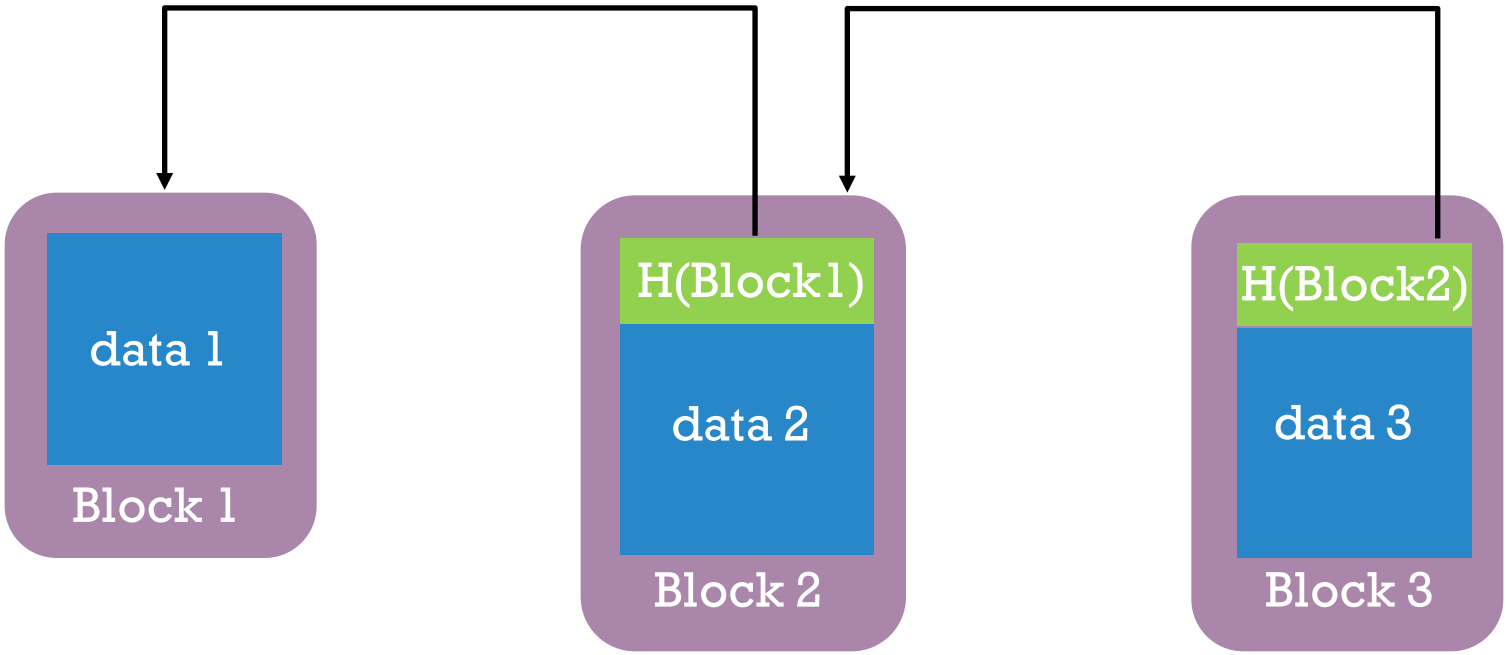
BLOCKCHAIN



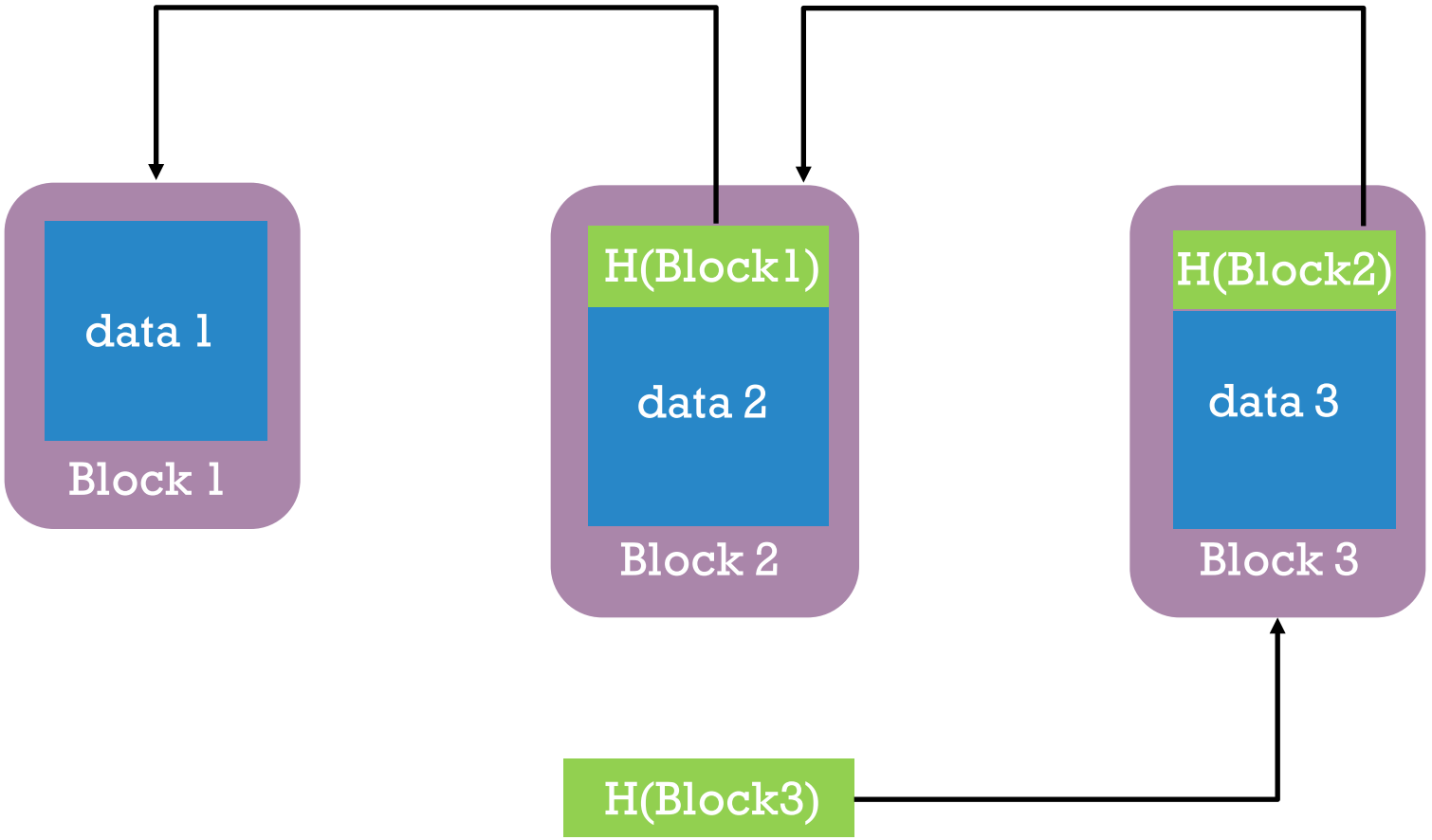
BLOCKCHAIN



BLOCKCHAIN

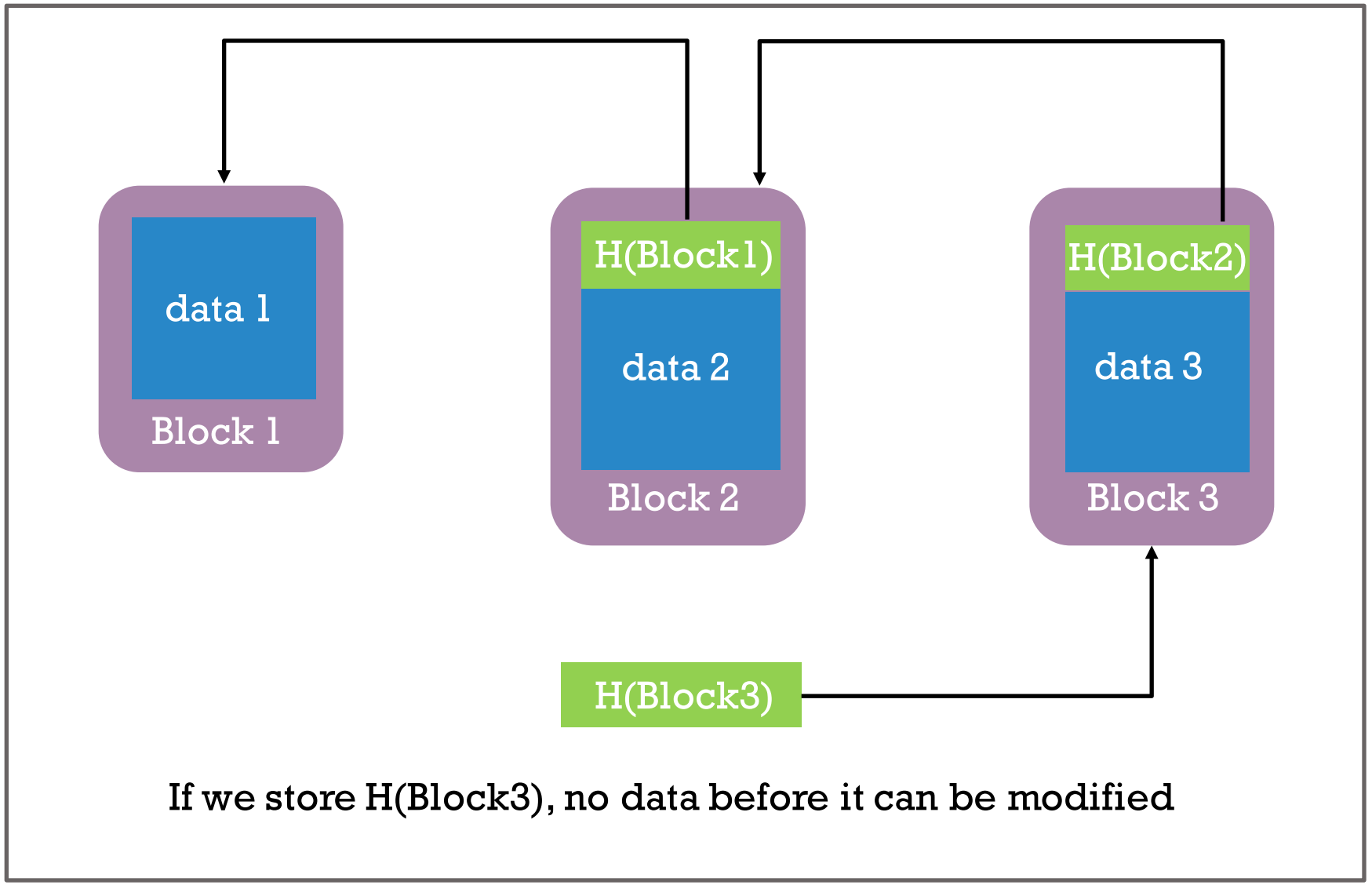


BLOCKCHAIN



If we store H(Block3), no data before it can be modified

BLOCKCHAIN



If we store H(Block3), no data before it can be modified

BLOCKCHAIN USE CASE: OPEN DATA

"Data to the people"

BLOCKCHAIN USE CASE: OPEN DATA

"Data to the people"

BLOCKCHAIN USE CASE: OPEN DATA

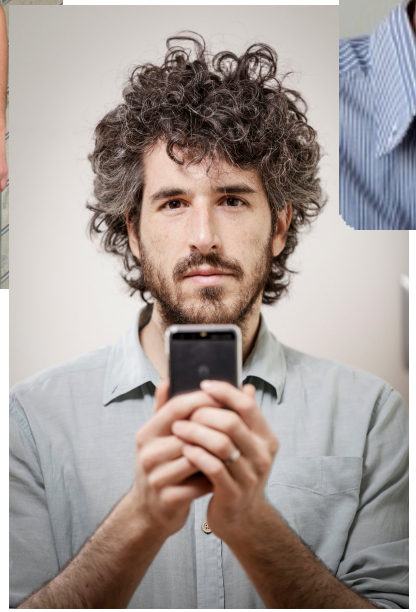
- Government data can be transparent and **immutable**
  - Just publish it in a blockchain
  - Anyone with a hash can check that the data did not change
  - Also works for completely secret data (hash of the hash)

- Good way to go about it:
  - A consortium of non profit agencies monitoring government data
  - Government publishes the data in a blockchain manner
  - Periodically (weekly/monthly) the final header is saved

- Ongoing work at the Institute for Foundational Research on Data

WORK DONE AT UC

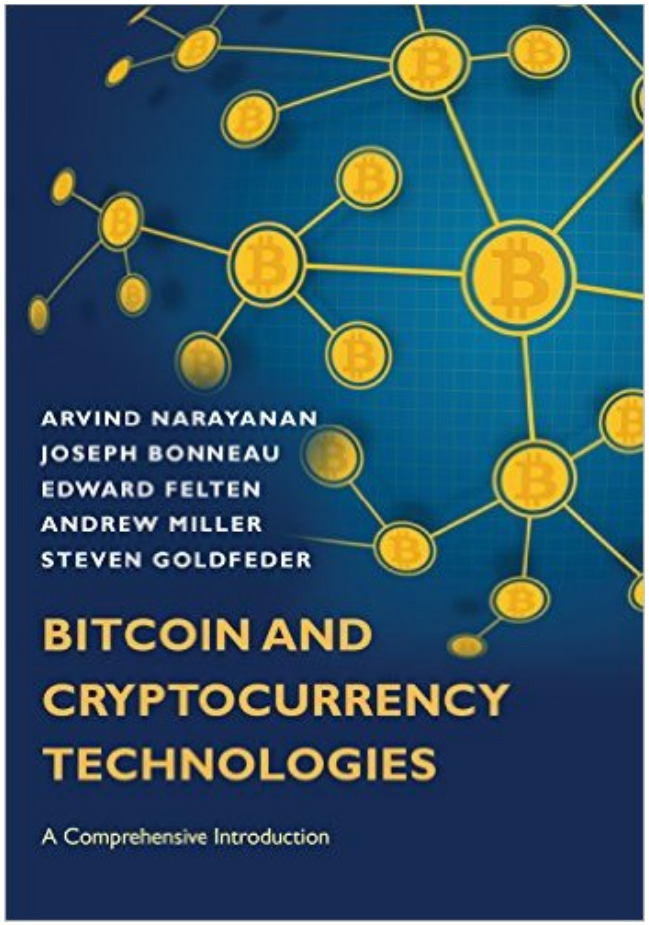
- DataLab DCC/Institute for Foundational Research on Data



WHAT ARE WE DOING AT DATALAB?

- When should I cheat in Bitcoin mining?
- Should the protocol be changed?
- Is the Bitcoin's network as Satoshi intended?
- Blockchain based tools for public/government data

WHERE TO LEARN MORE?



Thank you!

BACK TO CRYPTOCURRENCIES

SIMPLE CRYPTOCURRENCIES

- Blockchain can be used to record financial transactions
  - We can check where the money comes from
  - We can check it was not spent twice
  - No forgery is possible

- But someone has to check this and publish the blocks:
  - Government/bank does this, but does not publish your data

- This scheme is known as Scrooge-coin:
  - Actually used in practice (Ripple ~ 34 Billion USD)
  - Precursor to this (without the blockchain): paypal

DECENTRALIZATION

- Issues with having a central party maintaining the blockchain:
  - Allows manipulating access, value, validity
  - Can blacklist people (free market does not allow this)
  - Single point of failure

- Do we really need this?

BITCOIN'S DECENTRALIZATION MODEL

- Main ideas:
  - A peer-to-peer network maintains the blockchain
  - One node puts the next block in the chain

- Who puts the block:
  - Nodes compete to solve a computational puzzle (mining)
  - The winner gets newly created bitcoins (how bitcoins are created)

BITCOIN'S DECENTRALIZATION MODEL

- Why does this work?
  - There is money involved
  - Solving the puzzle requires a lot of electricity (costs money)
  - If the miner includes "wrong" transactions in the block:
    - She loses her money (block reward)
    - Because the rest of the network will catch on this and reject the block

BITCOIN

- Pros:
  - Decentralized
  - Secure (no forgery possible)
  - Fast

- Cons:
  - Slow: VISA has an order of magnitude more throughput
  - An ecological catastrophe? (mining wastes electricity)
  - Irreversible transaction

CRYPTOCURRENCIES WITH OTHER USES

- Ripple: a service for sending money (cheaper than SWIFT)
- Monero: complete anonymity (financial democracy tool)
- Ethereum/EOS:
  - Computation is done by the network
  - This is the future