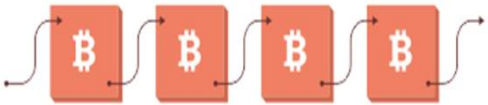
CS578:
Blockchain Technology: A Software Engineering Perspective

Dr. Raju Halder

Quick Review of Blockchain Technology

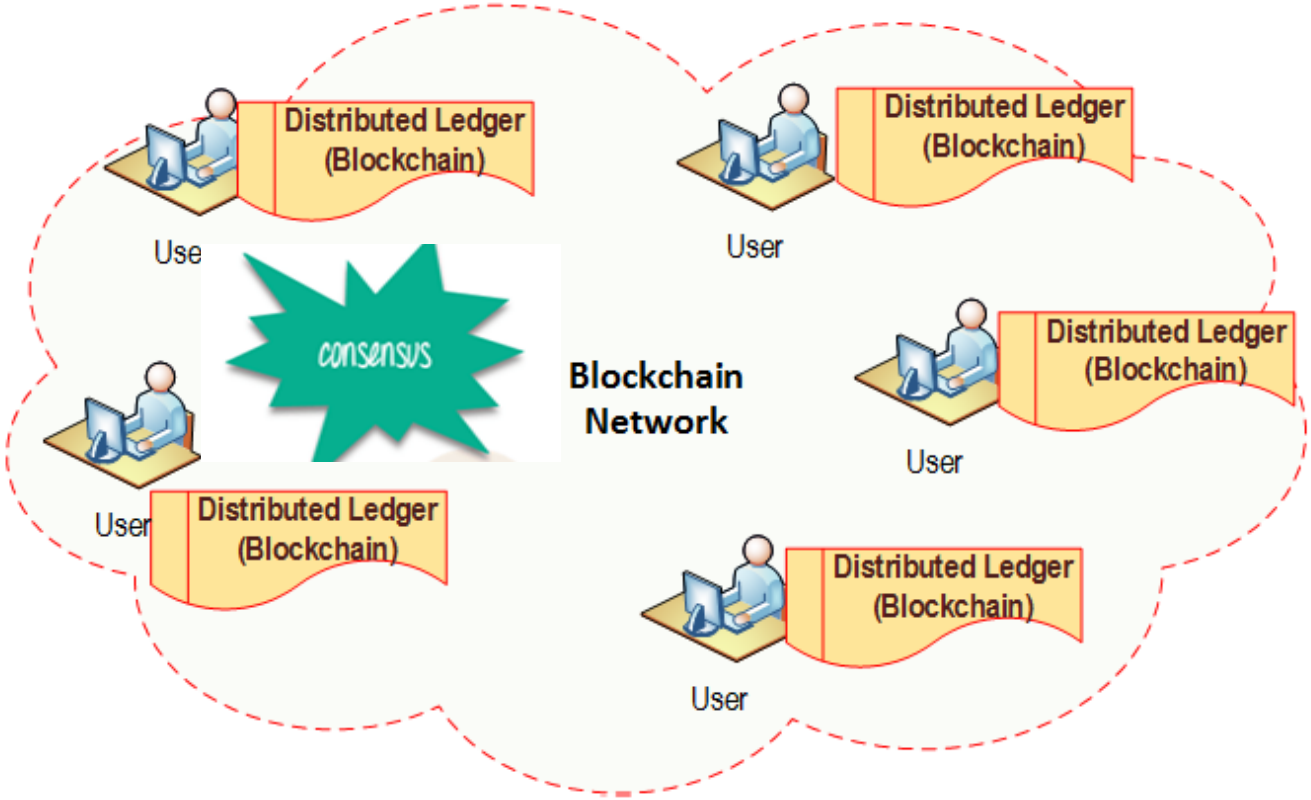
What is blockchain, and why does it matter?

- A blockchain is a historical record of transactions, much like a database
- Blocks in a chain = pages in a book.
- Each page in a book contains:
  - The text: the story
    - Equivalent to transactions in case of blockchain
  - Each page has information about itself (metadata): title of the book, chapter title, page number, etc.
    - Equivalent to transactions in case of blockchain



"Bits on Blocks", Blog by Antony Lewis, https://bitsonblocks.net/

Blockchain Network



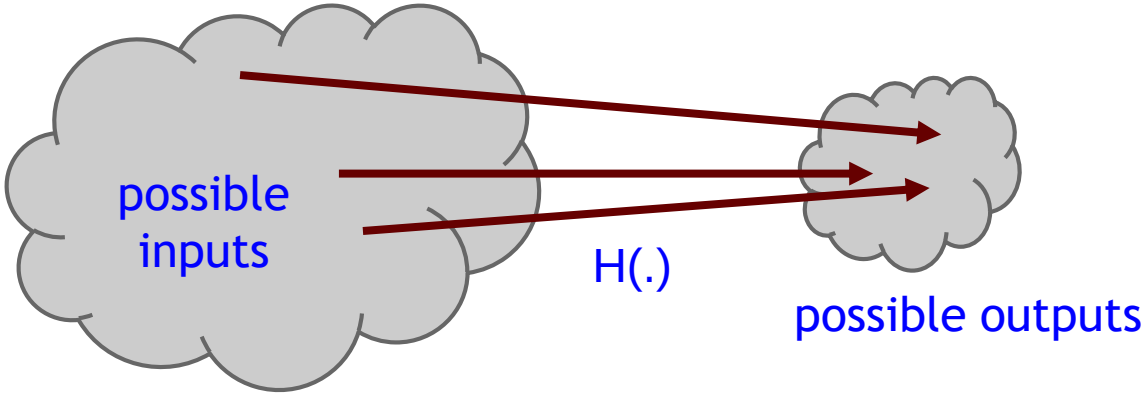
Hash function:

mathematical function

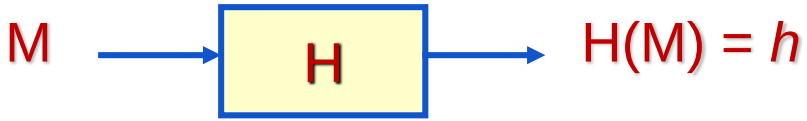
takes any string as input

fixed-size output (we'll use 256 bits)

efficiently computable (say, O(n))



One-Way Hash Functions



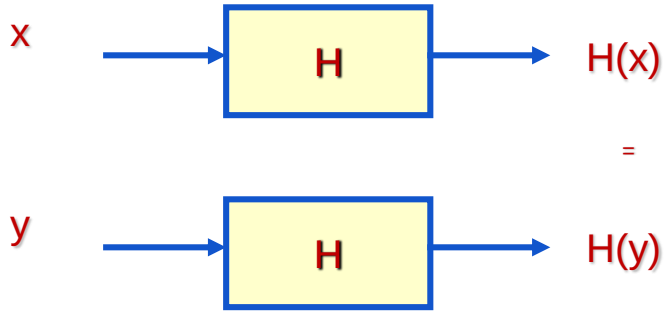
Example

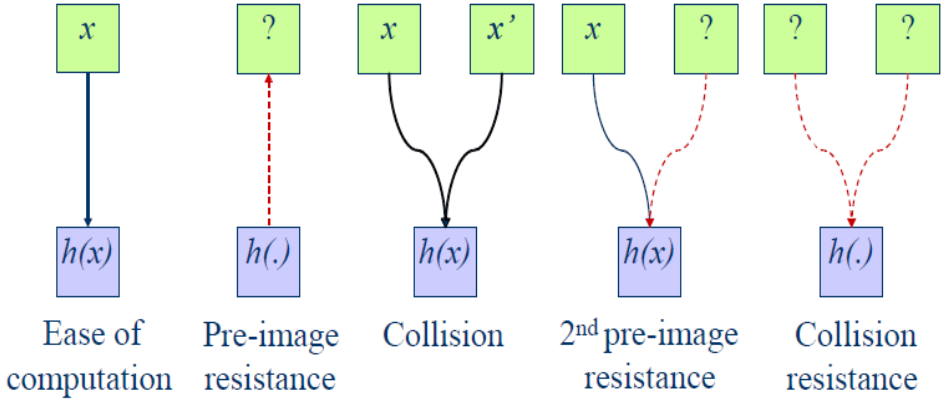
- M = “Elvis”
- H(M) = (“E” + “L” + “V” + “I” + “S”) mod 26
- H(M) = (5 + 12 + 22 + 9 + 19) mod 26
- H(M) = 67 mod 26
- H(M) = 15

Collision by Hash Function

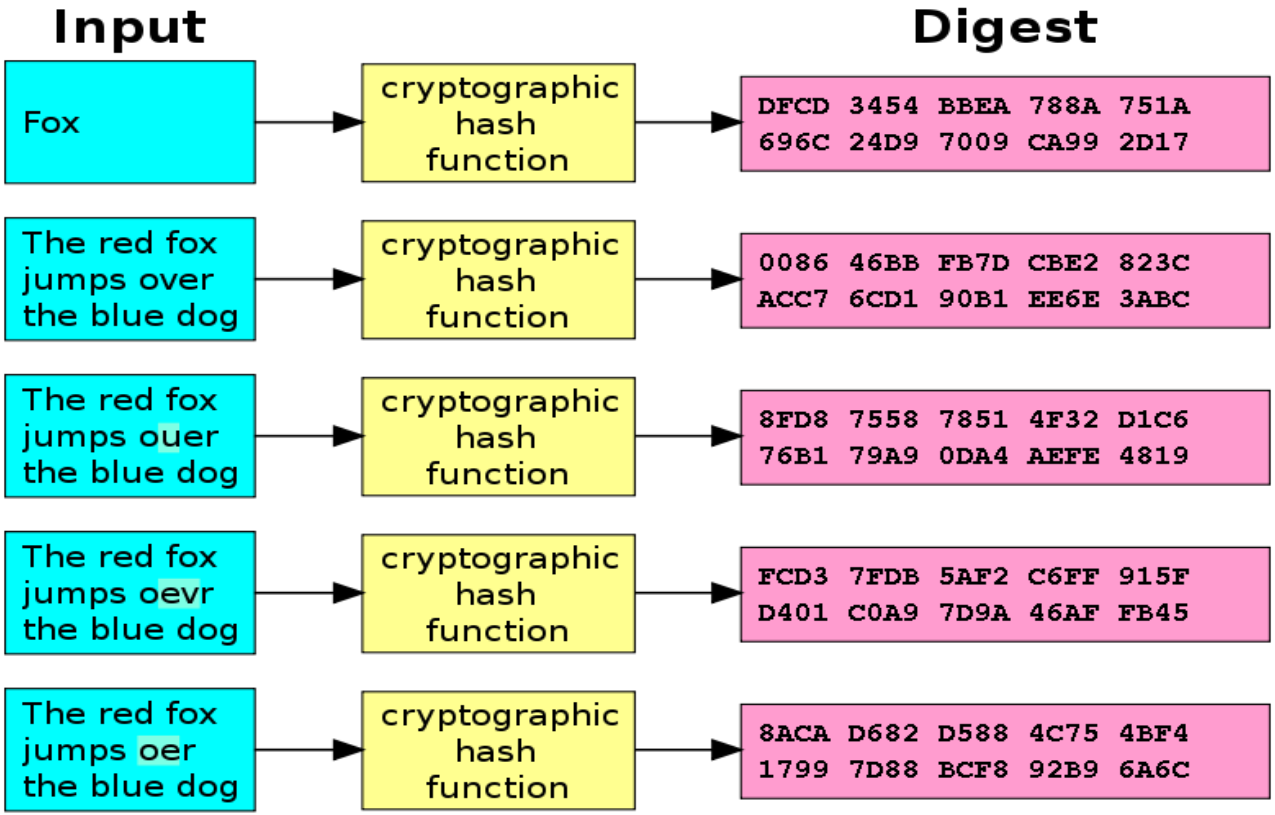
Example:

- **x = “Viva”**
- **Y = “Vegas”**
- **H(x) = H(y) = 2**





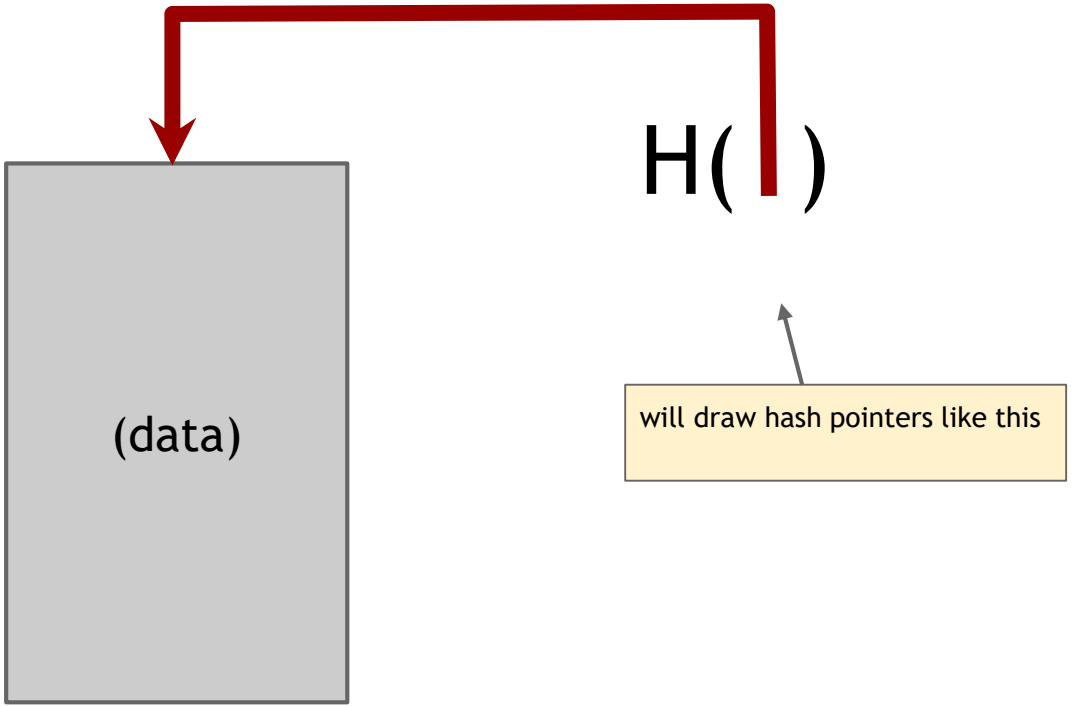
Avalanche effect on Hash



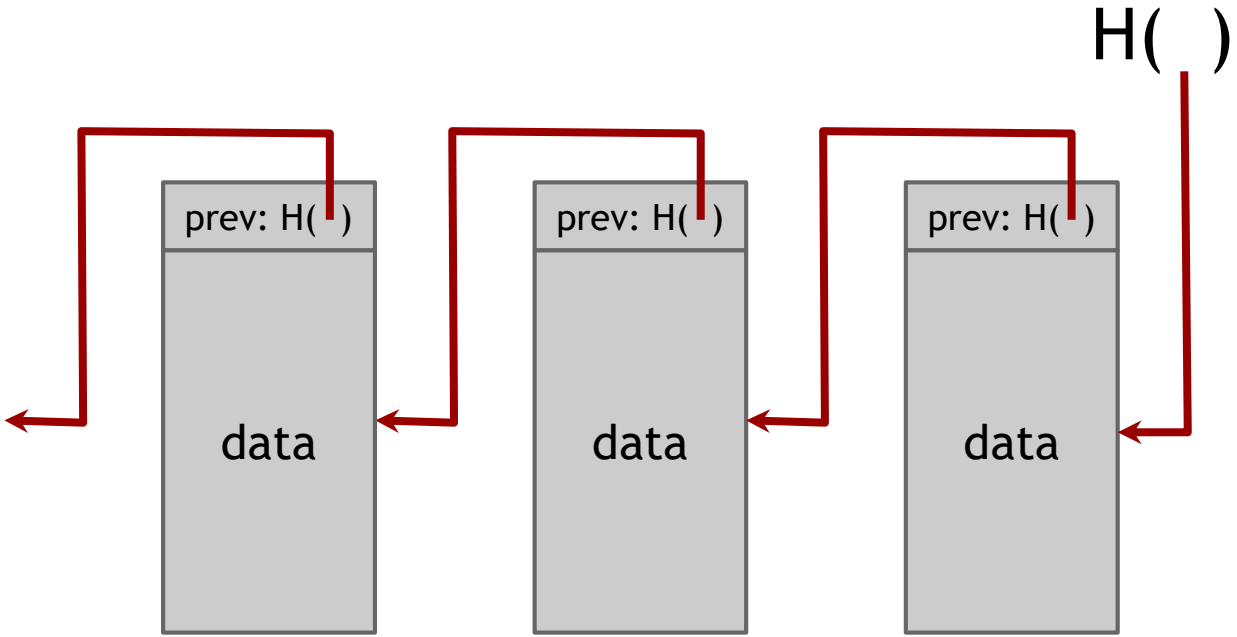
Hash Pointers and Data Structures

key idea:

Building Blockchain data structures with hash pointers

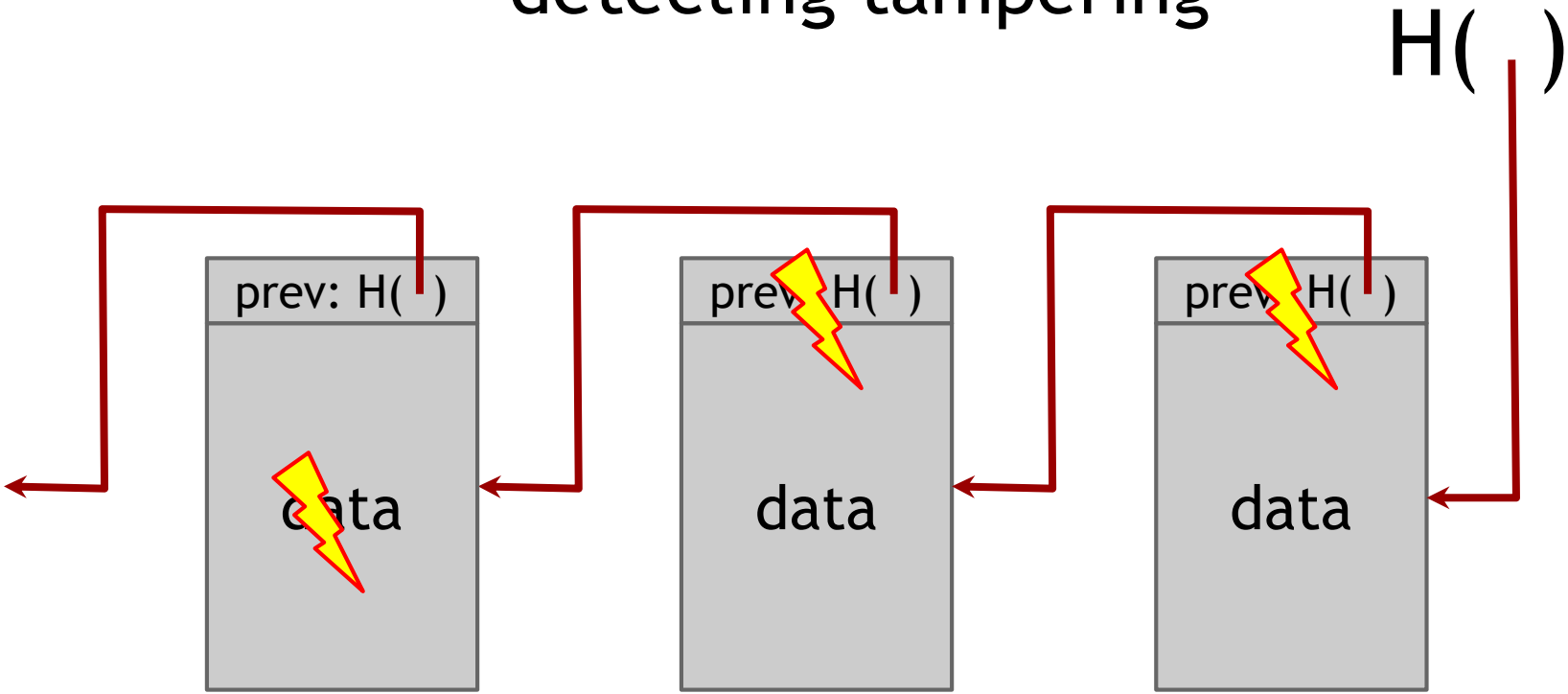

H( )
(data)
will draw hash pointers like this

linked list with hash pointers = “block chain”



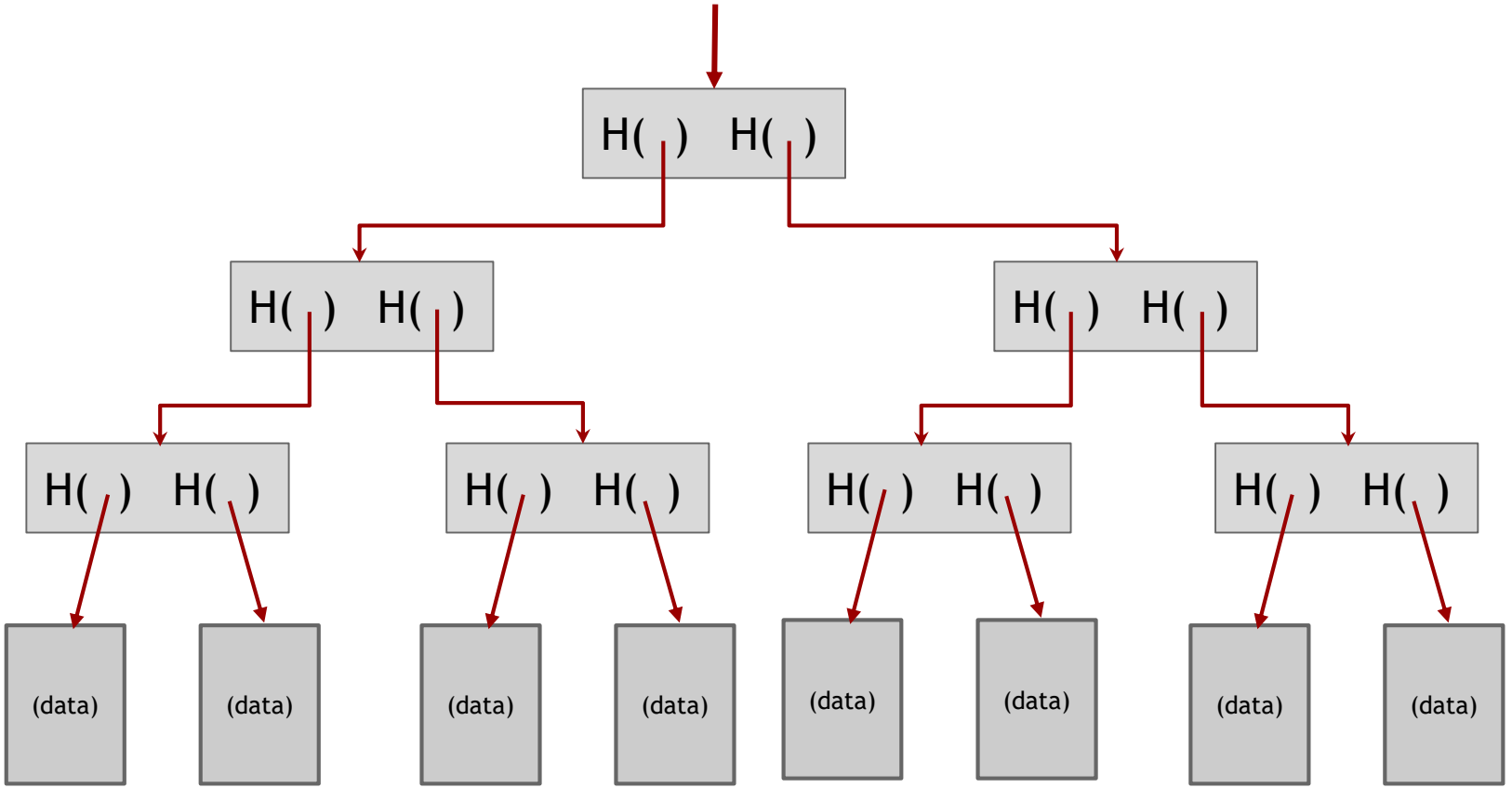
use case: tamper-evident log

detecting tampering

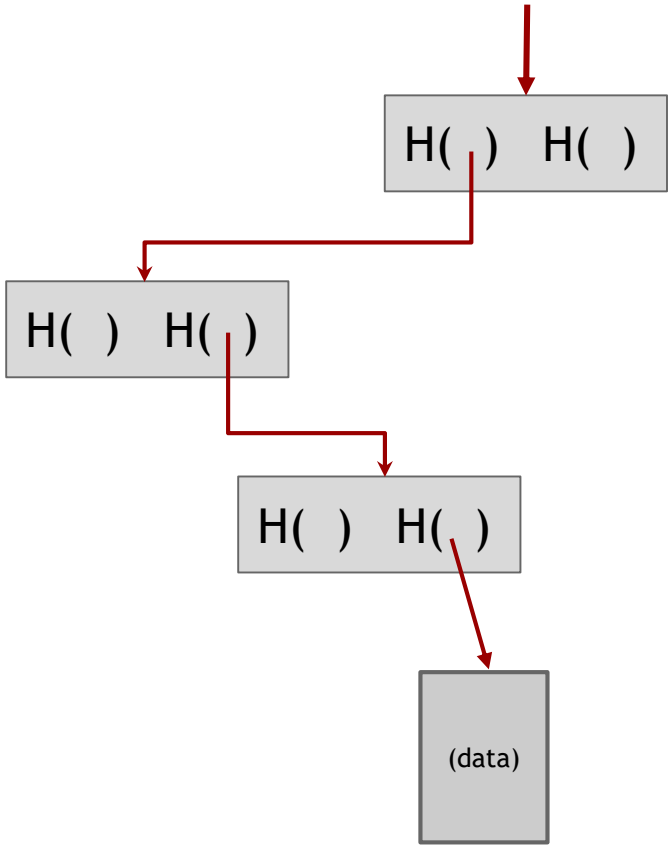


use case: tamper-evident log

binary tree with hash pointers = “Merkle tree”



proving membership in a Merkle tree

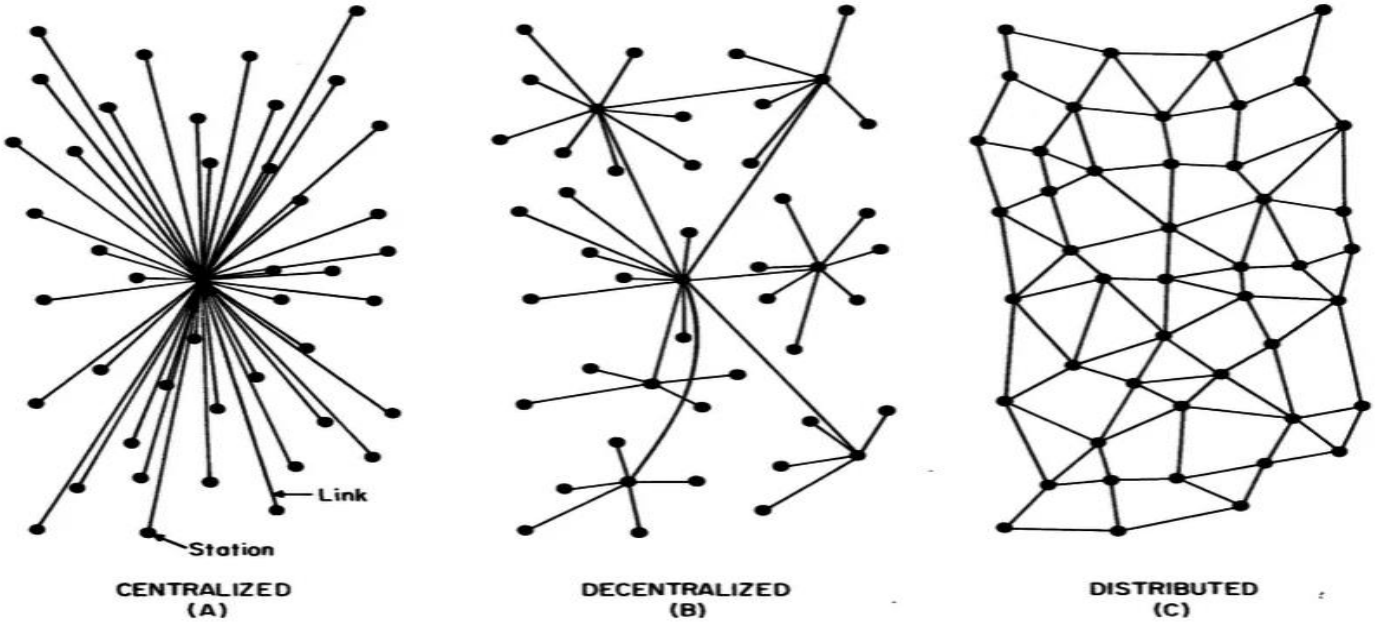


show O(log n) items

The Bitcoin network & Distributed consensus

Centralization vs. decentralization

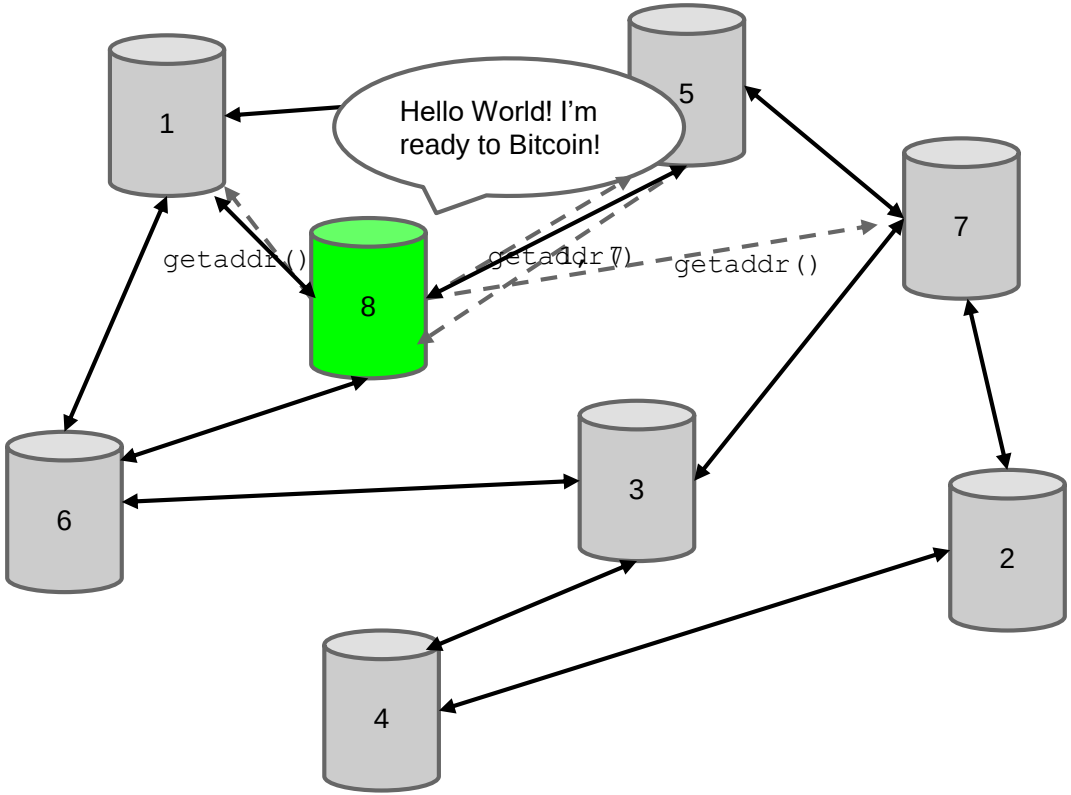
Competing paradigms that underlie many digital technologies



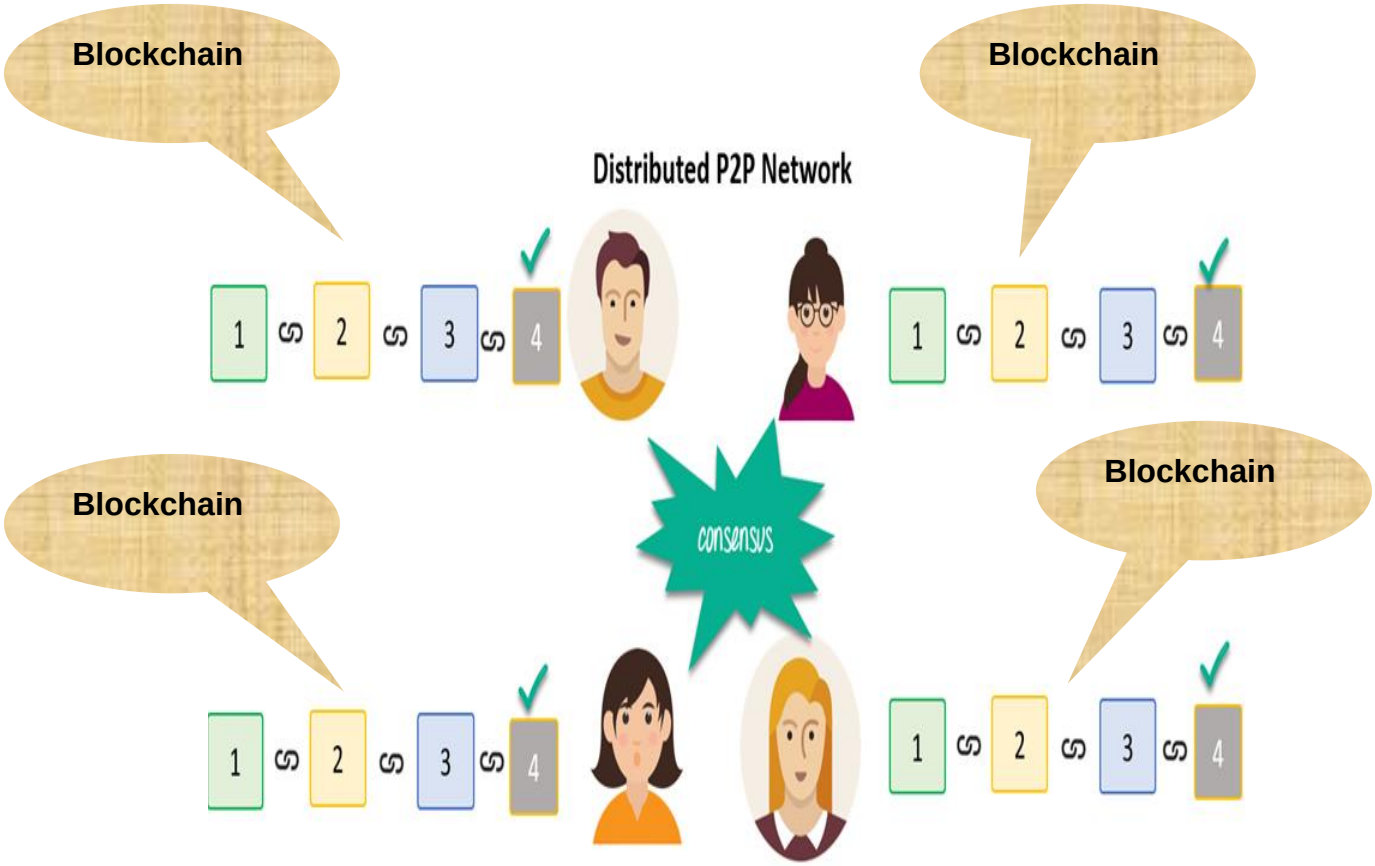
Bitcoin P2P network

- Ad-hoc protocol (runs on TCP port 8333)
- Ad-hoc network with random topology
- All nodes are equal
- New nodes can join at any time
  - Network Changes over time - dynamic
- No explict way to leave network
  - Forget non-responding nodes after 3 hr

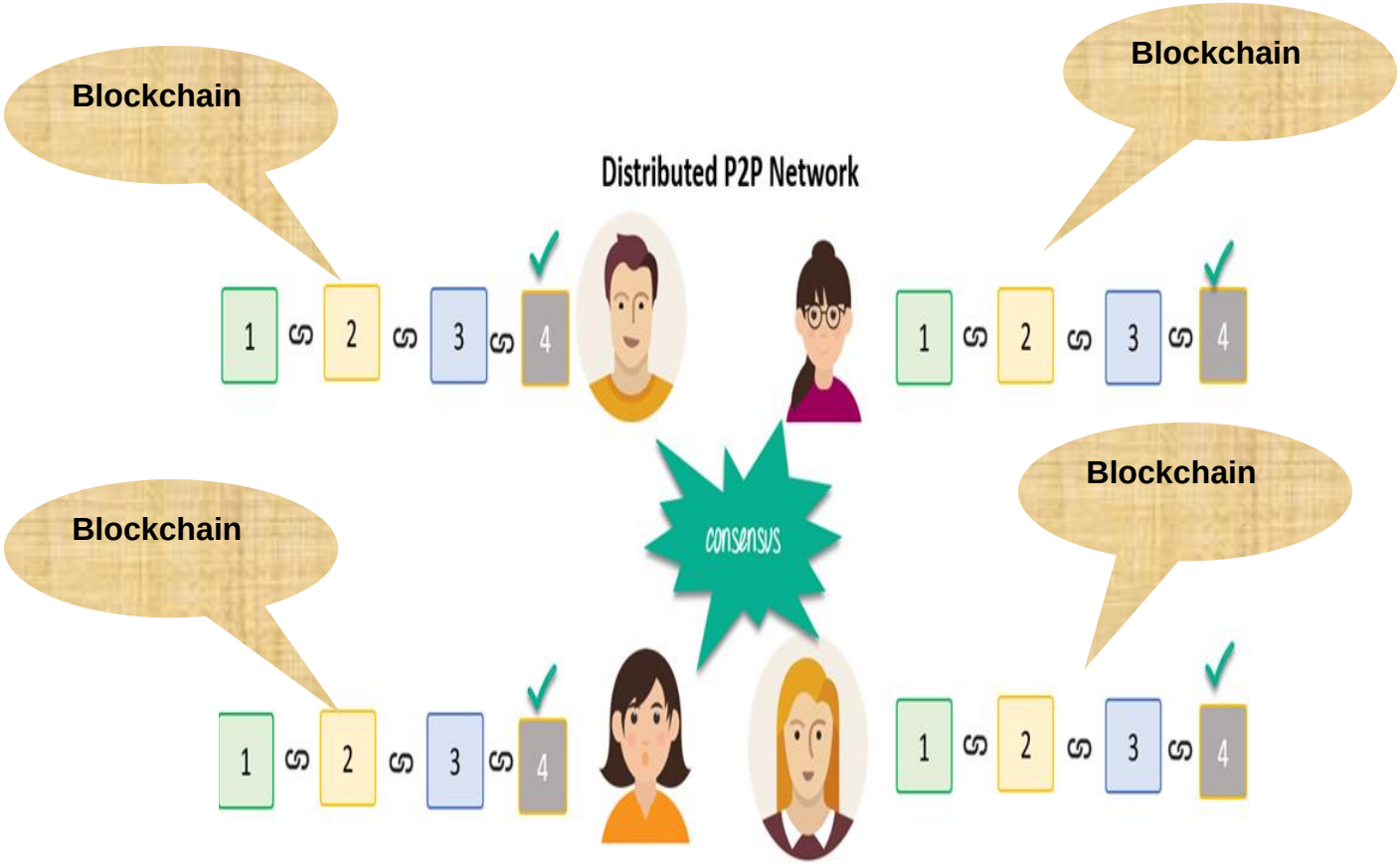
Joining the Bitcoin P2P network



Blockchain Network



How to achieve consistency?



The path to decentralization

- technology & incentive design

All Participants

Who maintains the ledger of transactions? (and how?)

Consensus

Who determines the validity of transactions to be included in the ledger?

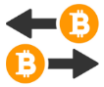
All Participants

Bitcoin Script

Who creates new Bitcoins?

Reward for Mining

BLOCKCHAIN WORKING PRINCIPLE

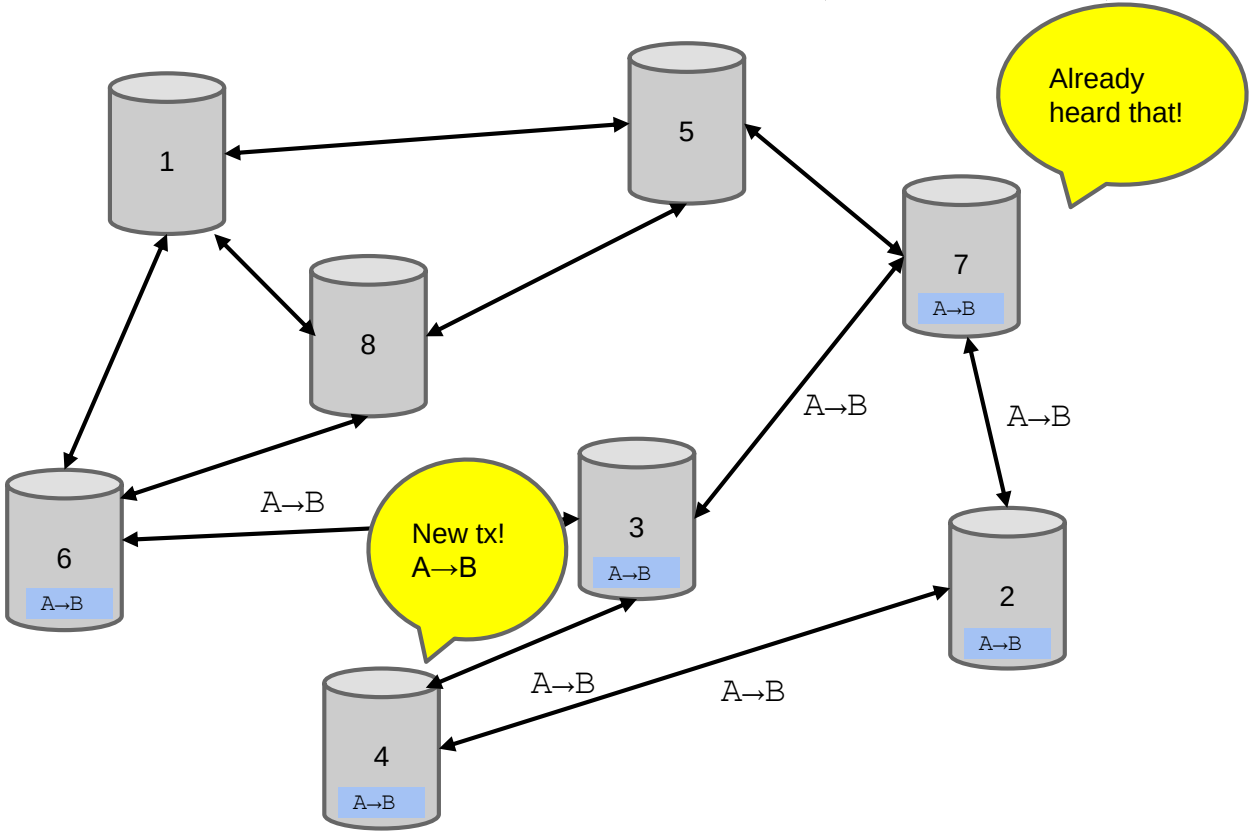


Transactions

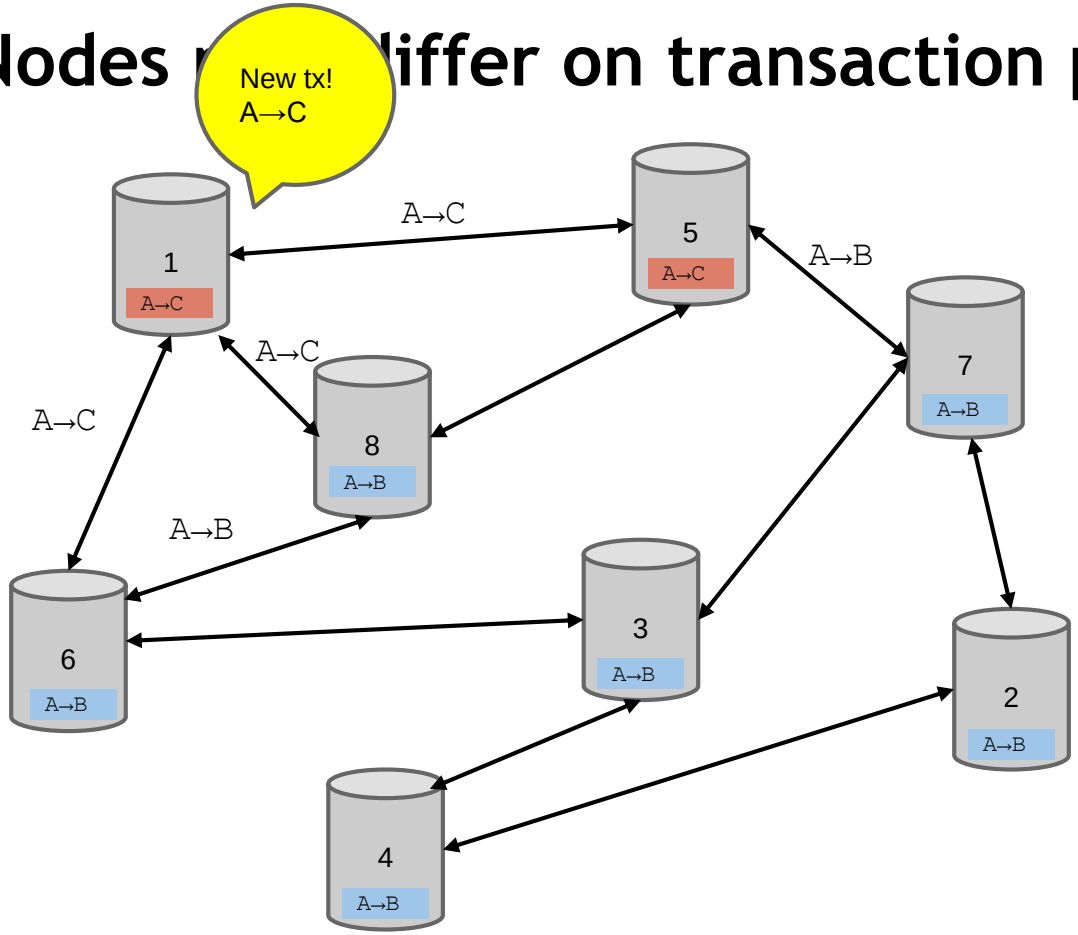
Process starts over

HOW THE BLOCKCHAIN WORKS?

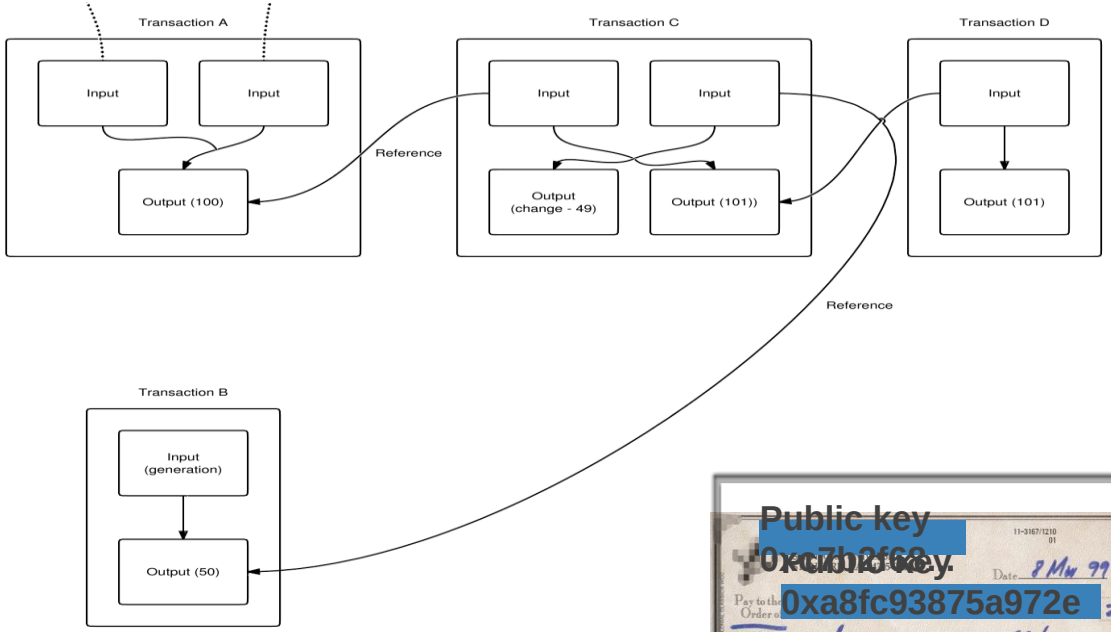
Transaction propagation (flooding)



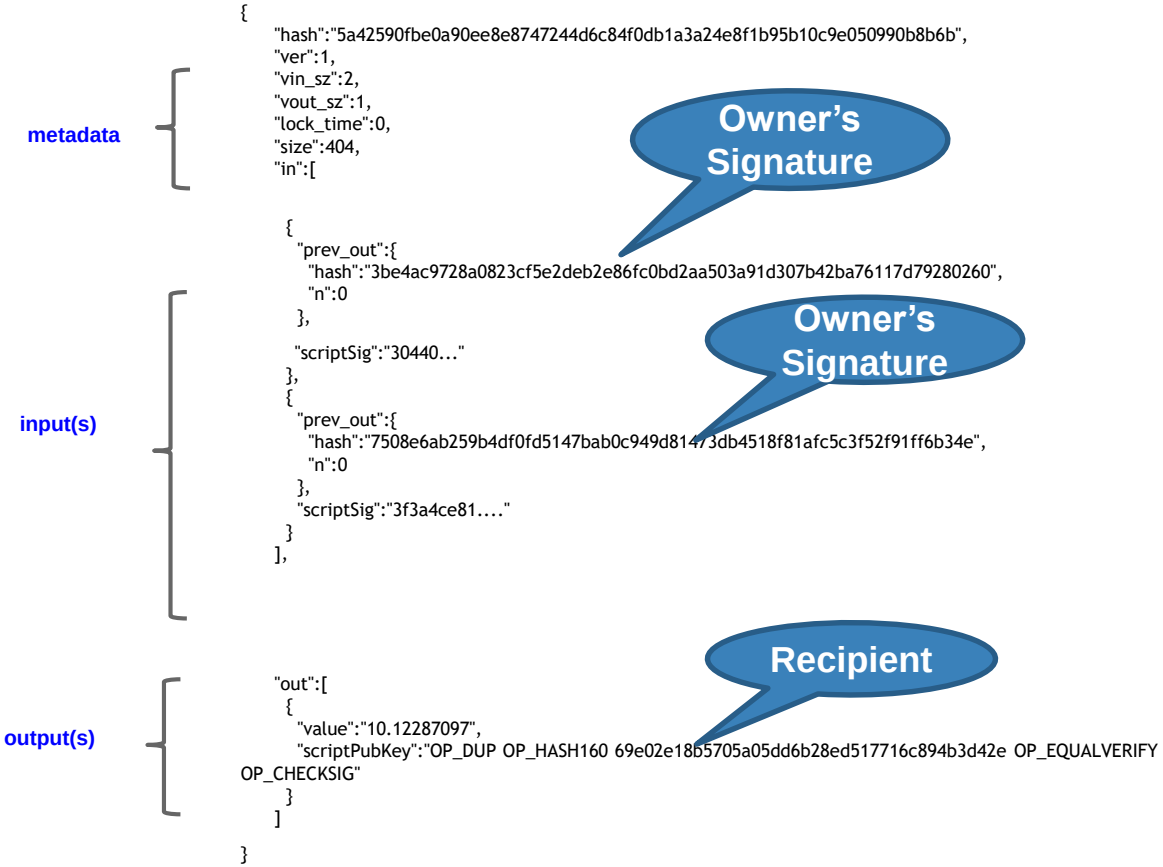
Nodes may differ on transaction pool

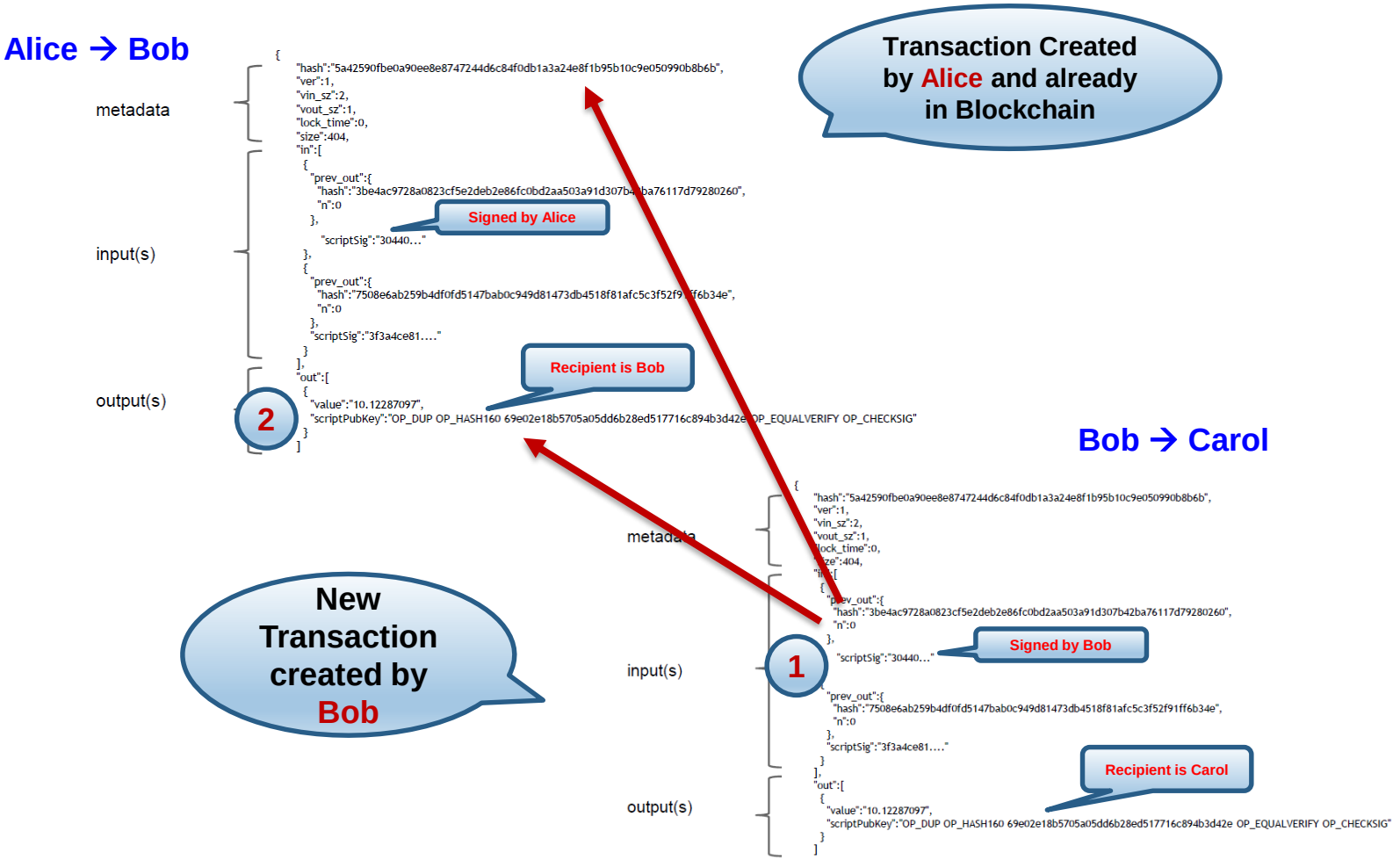


Bitcoin Transaction Structure

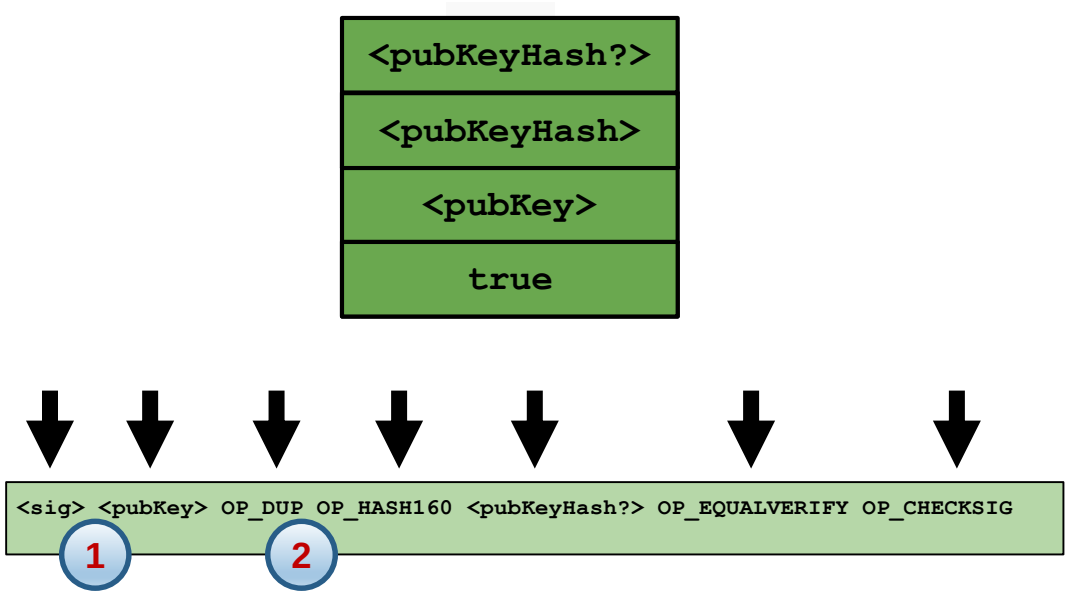


The real deal: a Bitcoin transaction

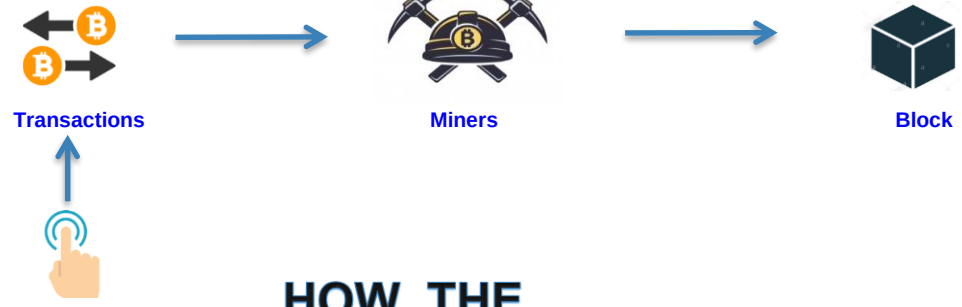



Alice → Bob
metadata
input(s)
output(s)
{
"hash":"5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",
"ver":1,
"vin_sz":2,
"vout_sz":1,
"lock_time":0,
"size":404,
"in":[
{
"prev_out":{
"hash":"3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",
"n":0
},
"scriptSig":"30440…"
},
{
"prev_out":{
"hash":"7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",
"n":0
},
"scriptSig":"3f3a4ce81…."
}
],
"out":[
{
"value":"10.12287097",
"scriptPubKey":"OP_DUP OP_HASH160 69e02e18b5705a05dd6b28ed517716c894b3d42e OP_EQUALVERIFY OP_CHECKSIG"
}
]
2
Signed by Alice
Recipient is Bob
Transaction Created by Alice and already in Blockchain
New Transaction created by Bob
Bob → Carol
metadata
input(s)
output(s)
1
Signed by Bob
Recipient is Carol

Bitcoin script execution example

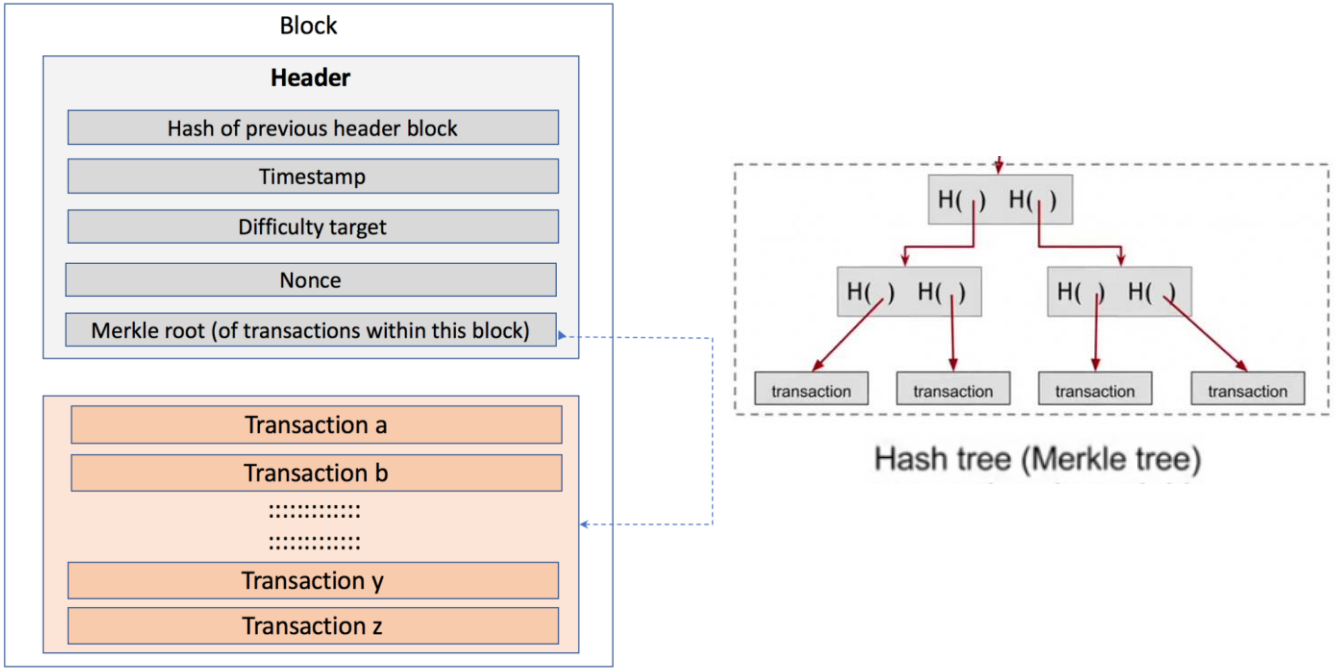


BLOCKCHAIN WORKING PRINCIPLE



HOW THE BLOCKCHAIN WORKS?

Block Structure



BLOCKCHAIN WORKING PRINCIPLE

Transactions

Miners

Block

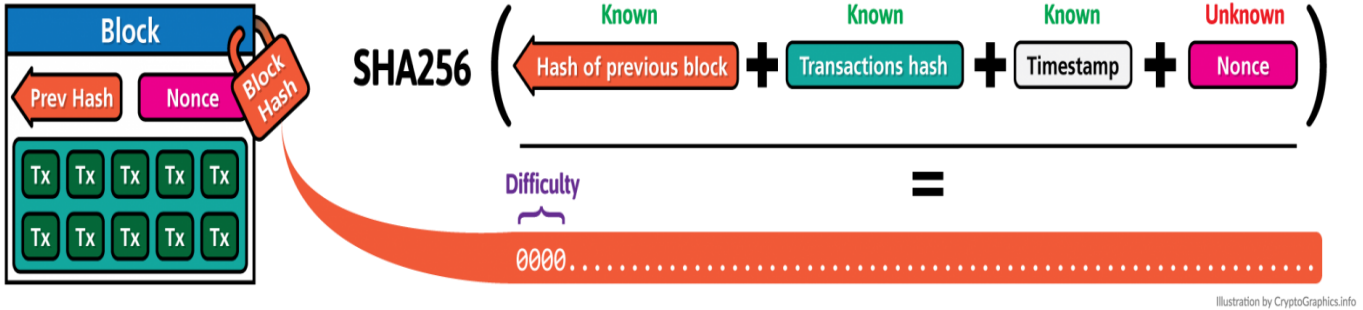
Process starts over

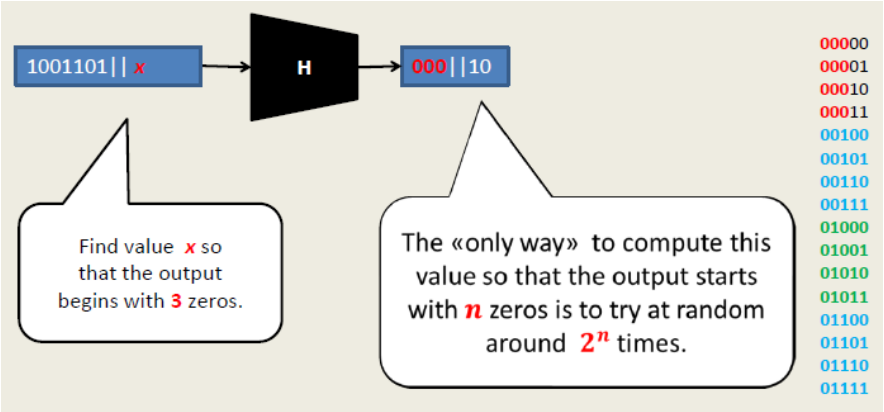
HOW THE BLOCKCHAIN WORKS?

Block Puzzle

Proof of work

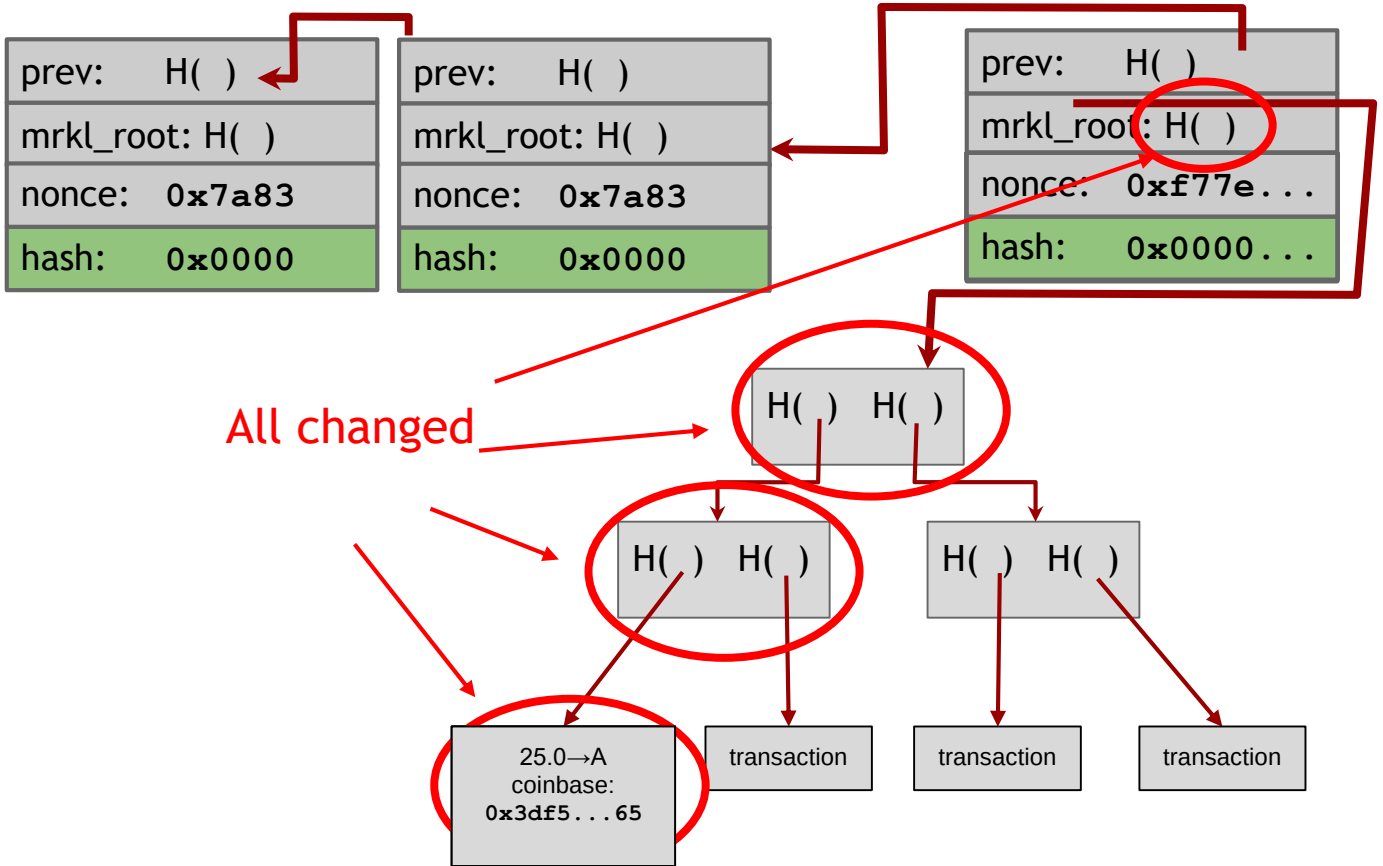
Proof of Work





Proof of Work **[Back2002]**

Mining a block: Proof-of-Work



Forbes Billionaires Innovation Leadership Money Consumer Industry

Ad closed by Google

Report this ad Why this ad?

EDITOR'S PICK | 23,388 views | Apr 19, 2018, 11:09pm

Bitcoin's Energy Consumption Can Power An Entire Country -- But EOS Is Trying To Fix That

Sherman Lee Contributor

I write about deep tech, crypto, and artificial intelligence.

Back to Articles

Bitcoins Energy Consumption An Unsustainable Protocol That Must Evolve?

3

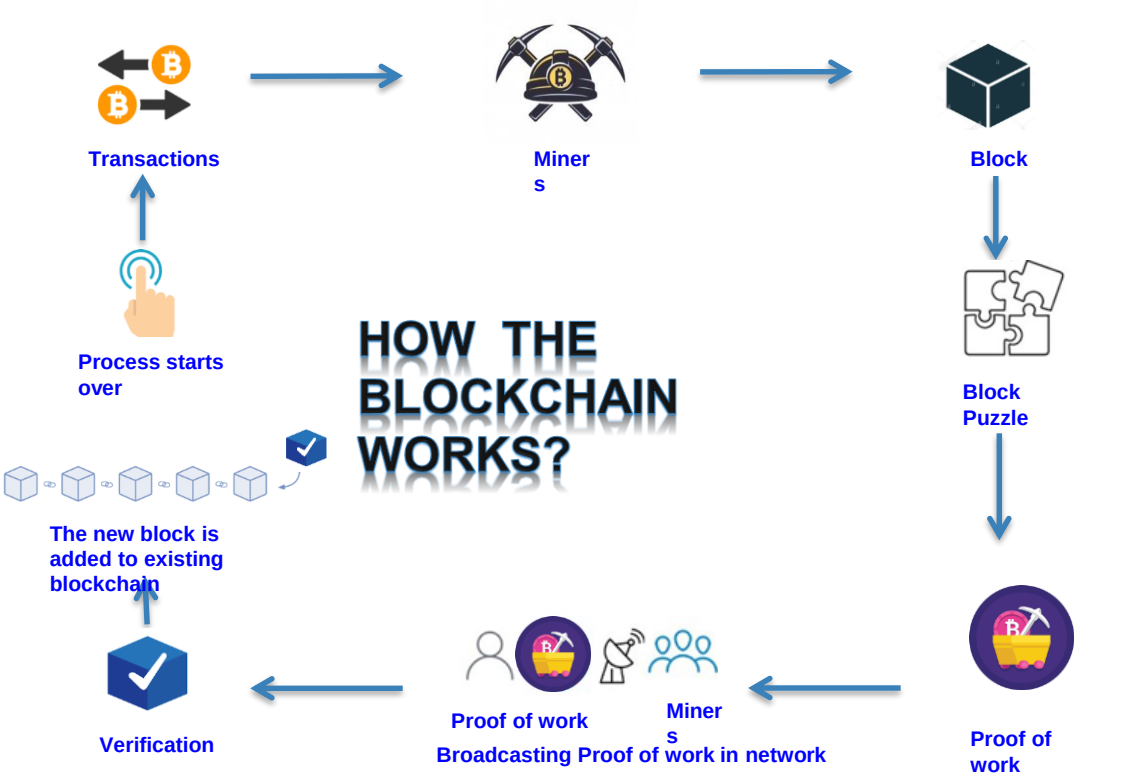
3

By john lilic #Blockchain 101 #Blockchain for Business #Blockchain for Investors

Alternative Consensus

- Proof of Stake
- PBFT
- Raft

BLOCKCHAIN WORKING PRINCIPLE

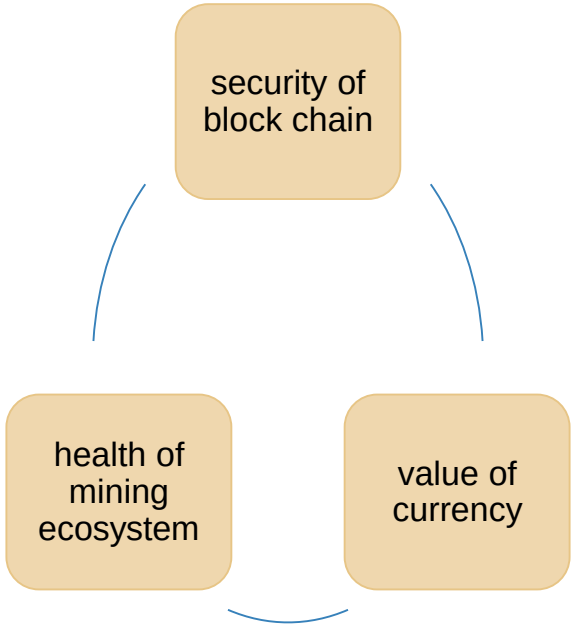


Mining Bitcoins in 6 easy steps

1. Join the network, listen for transactions
    a. Validate all proposed transactions
2. Listen for new blocks, maintain block chain
    a. When a new block is proposed, validate it
3. Assemble a new valid block
4. Find the nonce to make your block valid
5. Hope everybody accepts your new block
6. Profit!

Rewards and Transaction Fees!

Bitcoin is bootstrapped



Thank You !