The Blockchain

Presenters: Dao Yi, Edan Sneh

Vocabulary

Transaction - an atomic unit of data on the blockchain

Block - Object in chain containing multiple transactions and prev and current hash

Node - Process that holds the blockchain

Full Node - Process and holds **entire** blockchain

Miner - Process that runs PoW until 000x…xxx hash is found (depending on blockchain)

Nodes

- Validate transactions **(No double spending)**
- Keep a historic record of transactions (**Store blockchain**)
- Dictate and enforce the rules of the network. (**No bullshit!**)

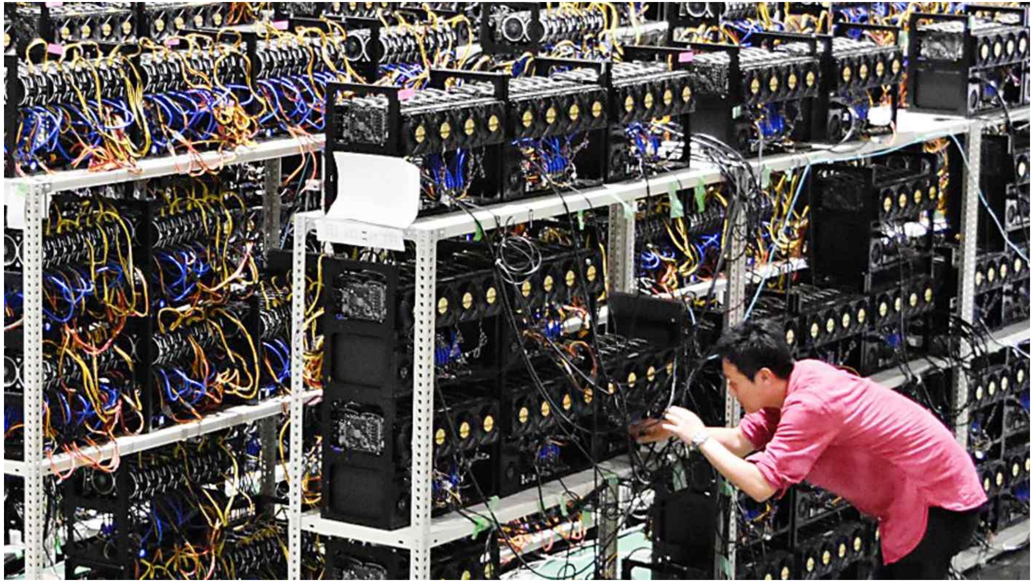
```
RaspiBlitz v1.5  RecklessBlitz
bitcoin Fullnode + Lightning Network + TOR
CPU load 0.40, 0.45, 0.43, temp 51°C 124°F
Free Mem 1322M / 1939M  HDDuse 308G (36%)
ssh admin@192.168.178.95 d22.6MiB u15.4MiB
web admin --> http://192.168.178.95:3000
bitcoin v0.19.1 mainnet Sync OK 100.00%
Public rvxlan6p2guj2ren.onion:8333 11 peers

LND 0.10.0-beta wallet 61148 sat
2/2 Channels 371841 sat 4 peers
Fee Report: 0-0-0 sat (D-W-M)

033edbdfc7f382ab0858b9e4382f171e2ba4c12cd09b8243ad172339cfb2fb
f7b8@b4tnjucd3osmdqddaujn75zf4qbh6lpcztyfvswfmhtkfdxtxp3tq7id.
onion:9735
```

Miners

- Confirm transactions (put transactions into blocks with PoW)
- Secure the blockchain (Keep track of largest chain and continue building it)
- Gain $$$ reward (often transaction fee for solver)



Walkthrough

I want to buy this teddy bear with my bitcoin!

Red’s acc: c766227e7af569848...286e6ef5

Red

Blue

Tx1:
Log - Gave red 1 bc
Hash: **37df**...aef
Prev hash: ???

Tx2:
Log - red gave blue 1 bc
Hash: **ad80**...2e2
Prev hash: **37df**

Blue shouldn't give away his precious teddy bear yet!!

Hash contains red's public key

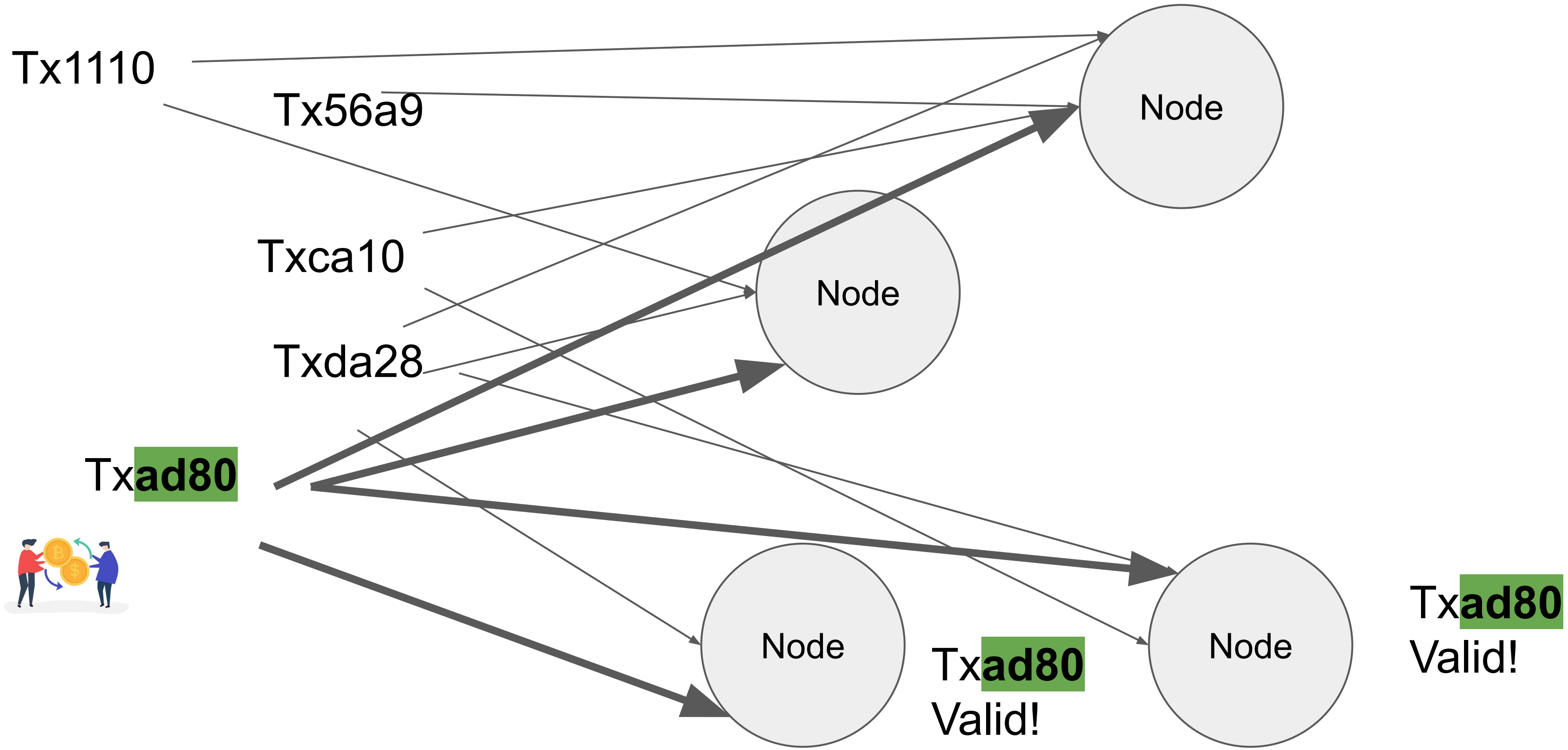
Hash signed with reds private key
Proving red owns coin in Tx1

Tx1:
Log - Gave red 1 bc
Hash: **37df**...aef
Prev hash: ???

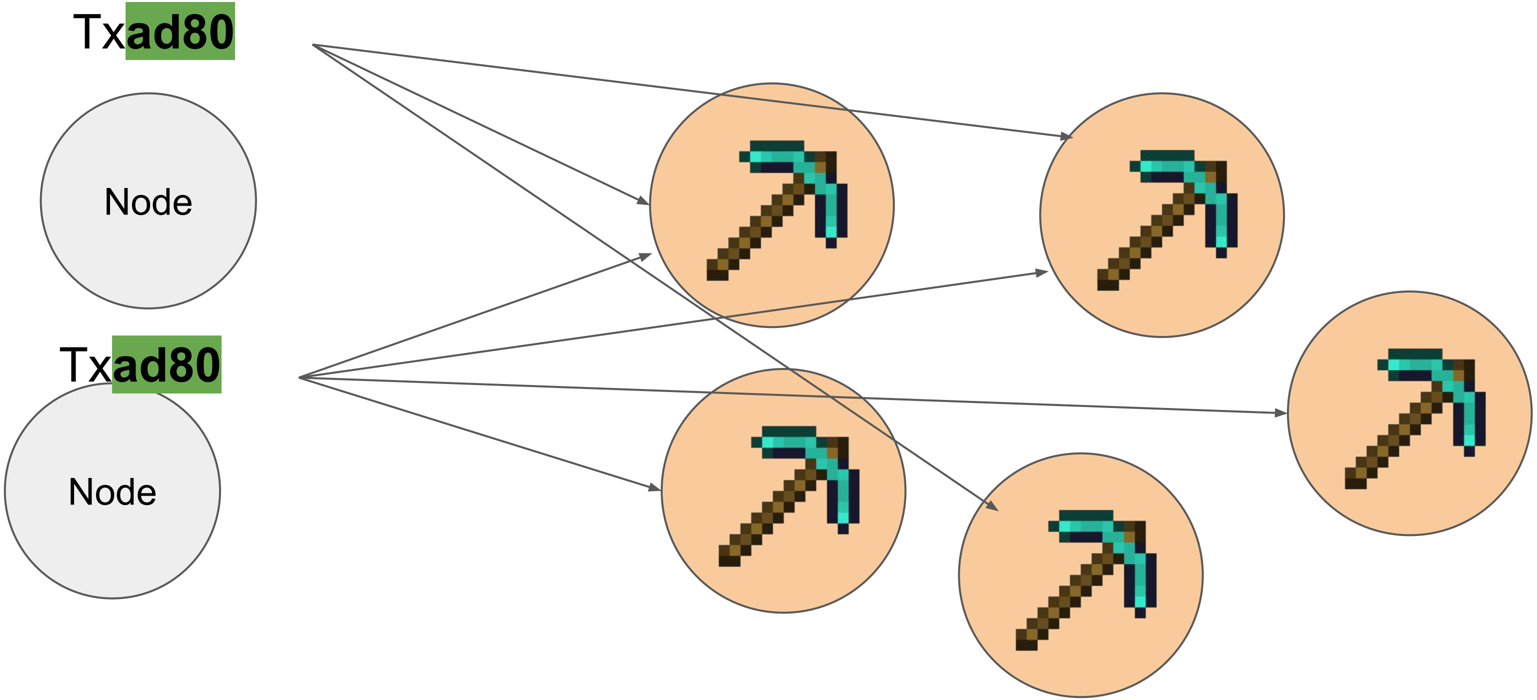
Tx2:
Log - red gave blue 1 bc
Hash: **ad80**...2e2
Prev hash: **37df**

Hash contains blue's public key

Validation


Tx1110
Tx56a9
Txca10
Txda28
Txad80
Node
Node
Node
Node
Txad80
Valid!
Txad80
Valid!

Mining time!



Tx**ad80**

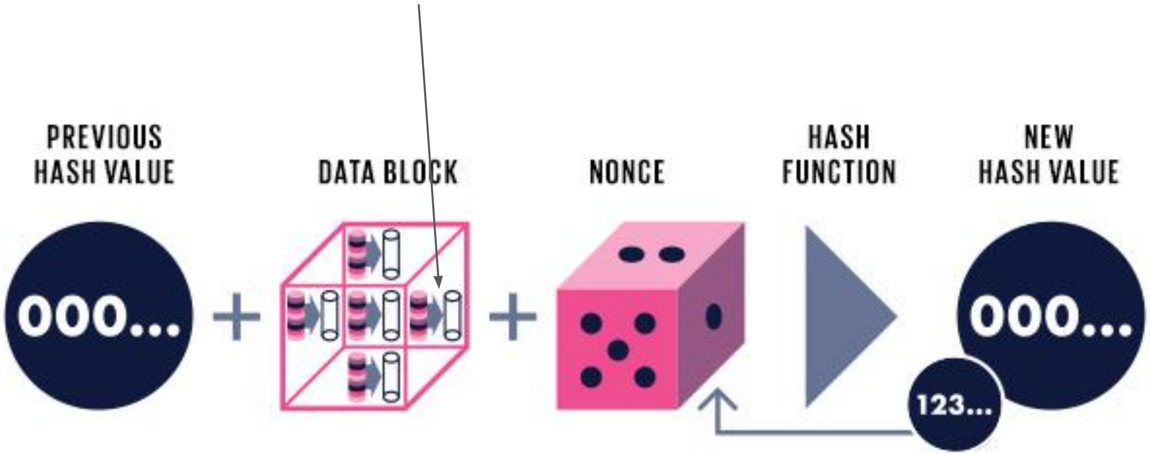
Node

Tx**ad80**

Node

Proof of Work (PoW)

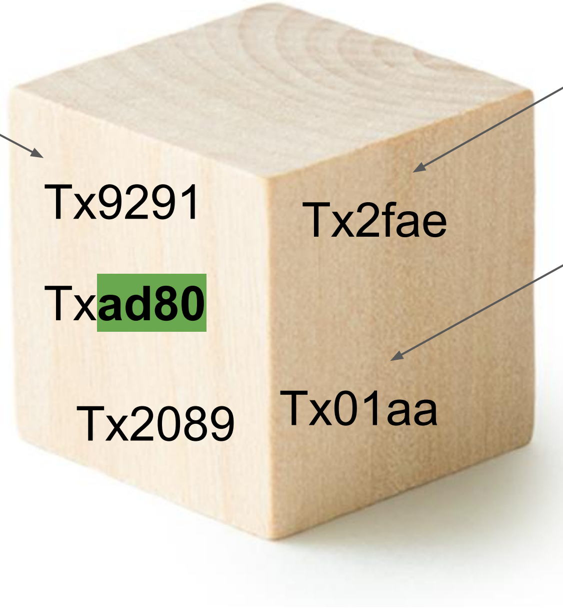
Txad80



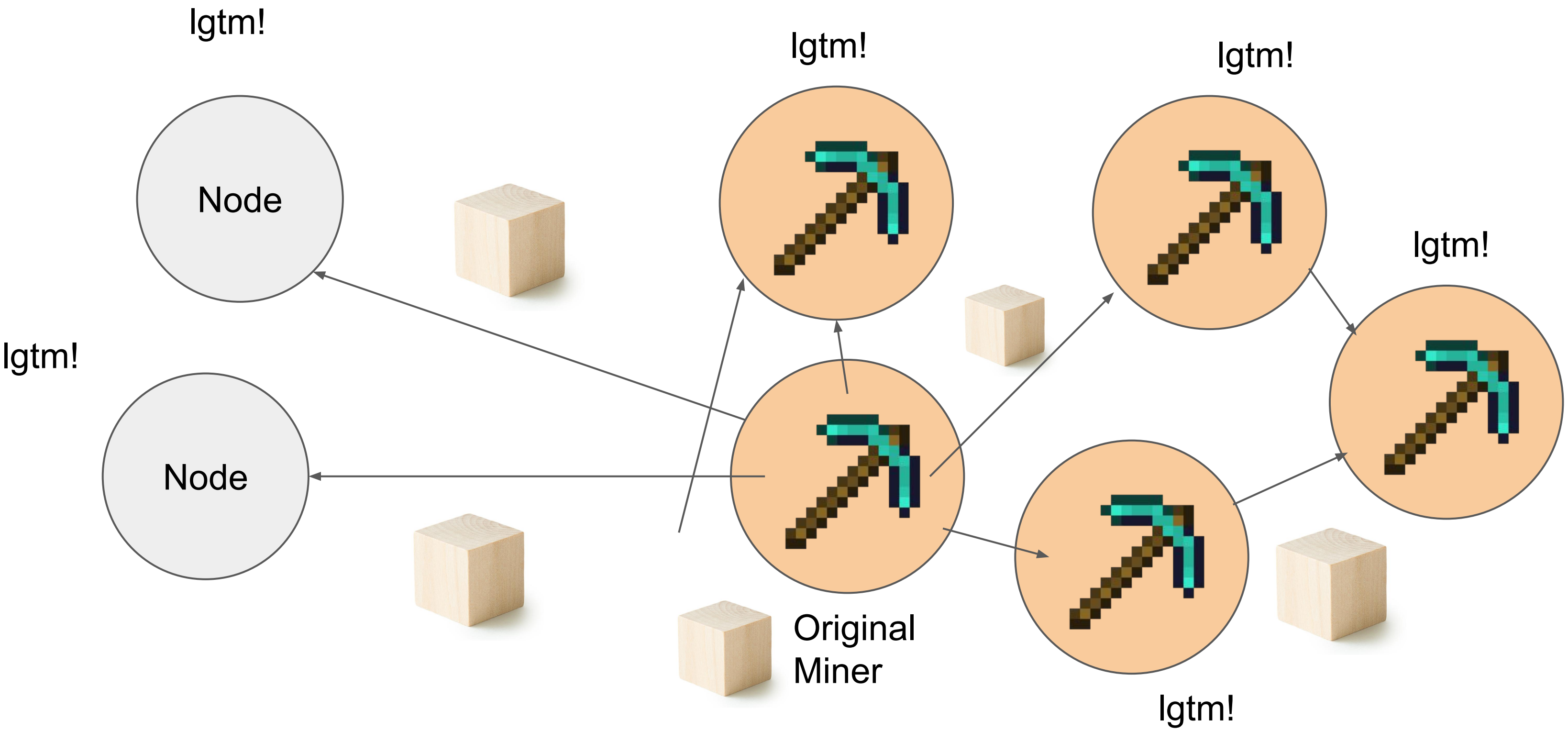
Yay! Red’s transaction has made it into a block

Miner’s cut!

Or empty space
in transactions for
miners address



Verification - Nodes add block to blockchain!



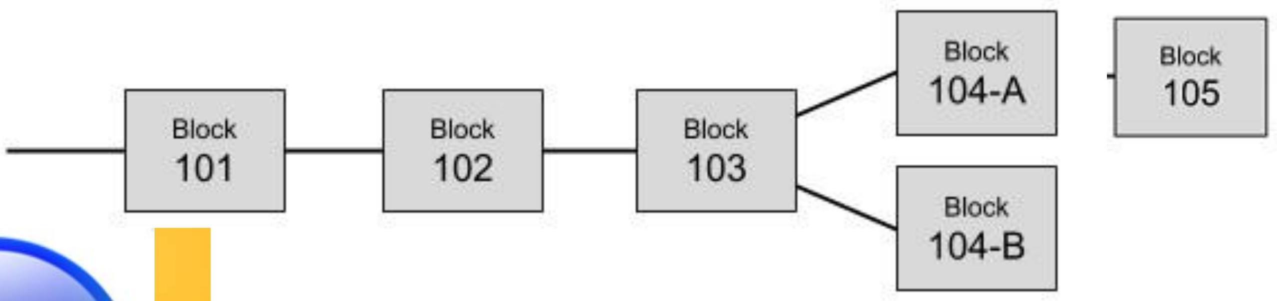
Discuss:

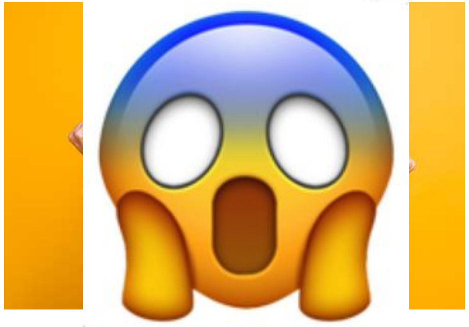
- Should blue hand over their Teddy bear now? Why?
- What are some weaknesses of blockchain?
- Why is decentralization important?
- What are some applications of blockchain?

https://tinyurl.com/btcblk

Transaction validity (Race Attack)

Common practice is to wait until block is 3 deep into chain before accepting. Since top block can change





Transaction on Block 104-B
is gonna make me rich.
Sending money now!

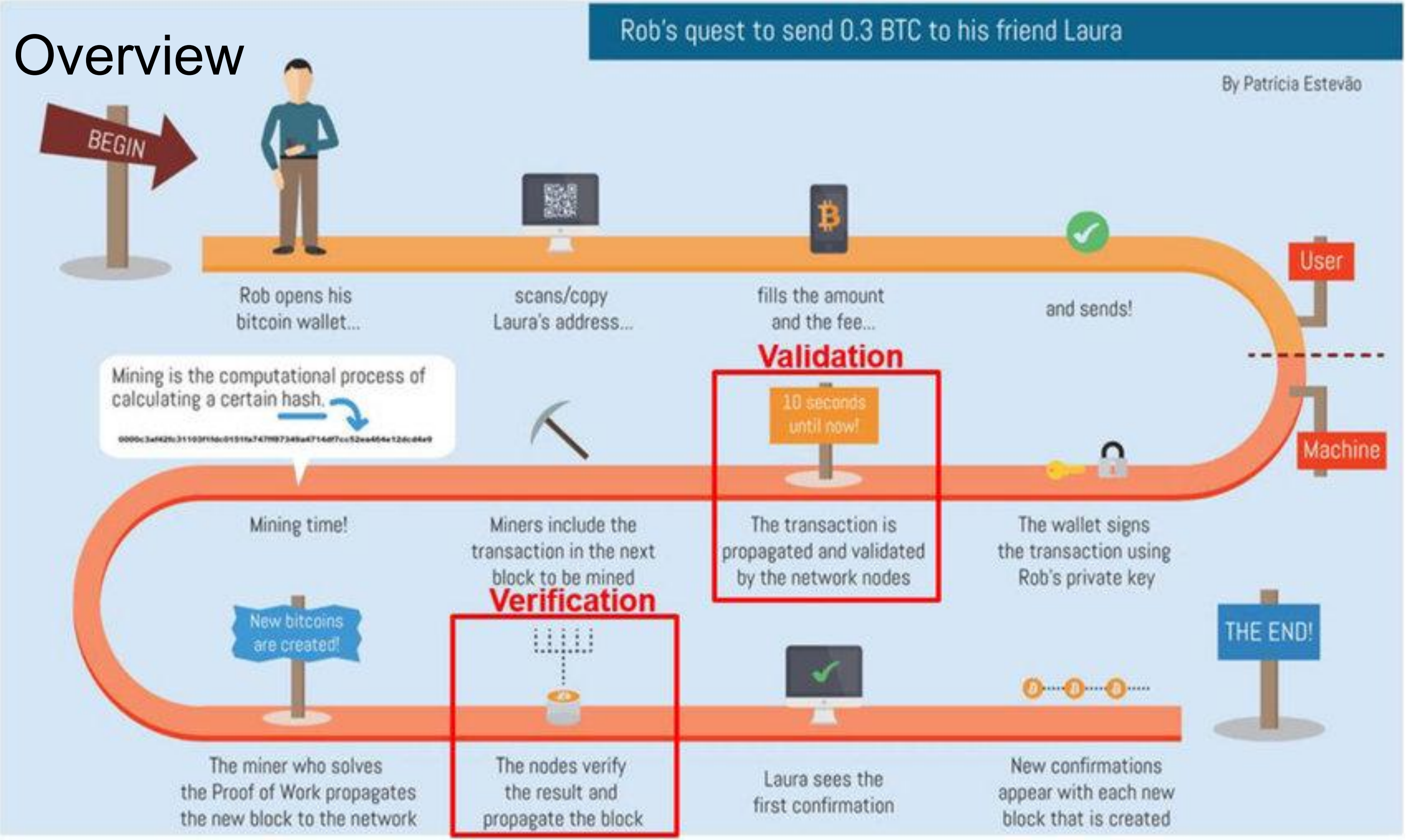
WHOOPS!!!

Blue can now give red teddy bear

Red

Blue

Overview



Rob's quest to send 0.3 BTC to his friend Laura

By Patrícia Estevão

Rob opens his bitcoin wallet...

scans/copy Laura's address...

fills the amount and the fee...

and sends!

Validation

The wallet signs the transaction using Rob's private key

The transaction is propagated and validated by the network nodes

Miners include the transaction in the next block to be mined

Mining time!

Mining is the computational process of calculating a certain hash.

0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

The miner who solves the Proof of Work propagates the new block to the network

Verification

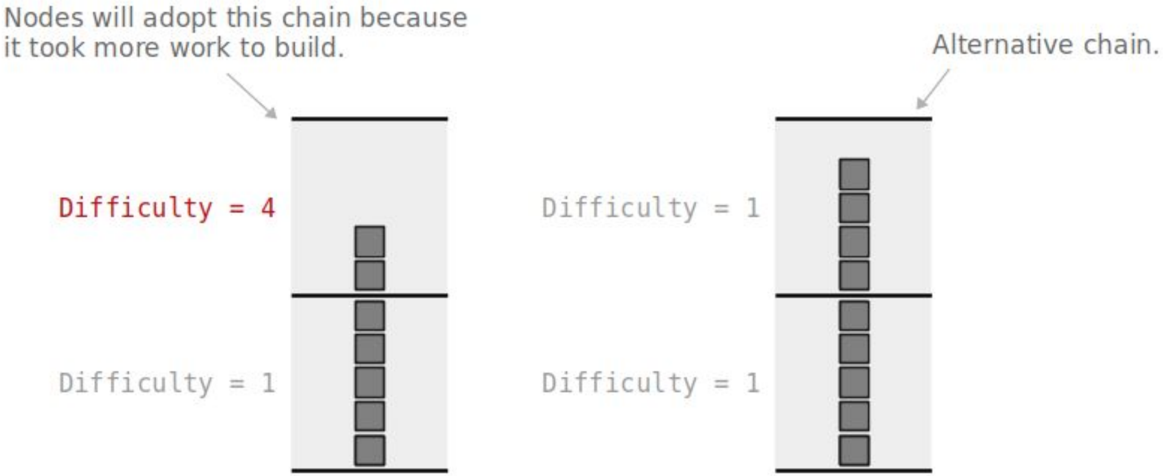
The nodes verify the result and propagate the block

Laura sees the first confirmation

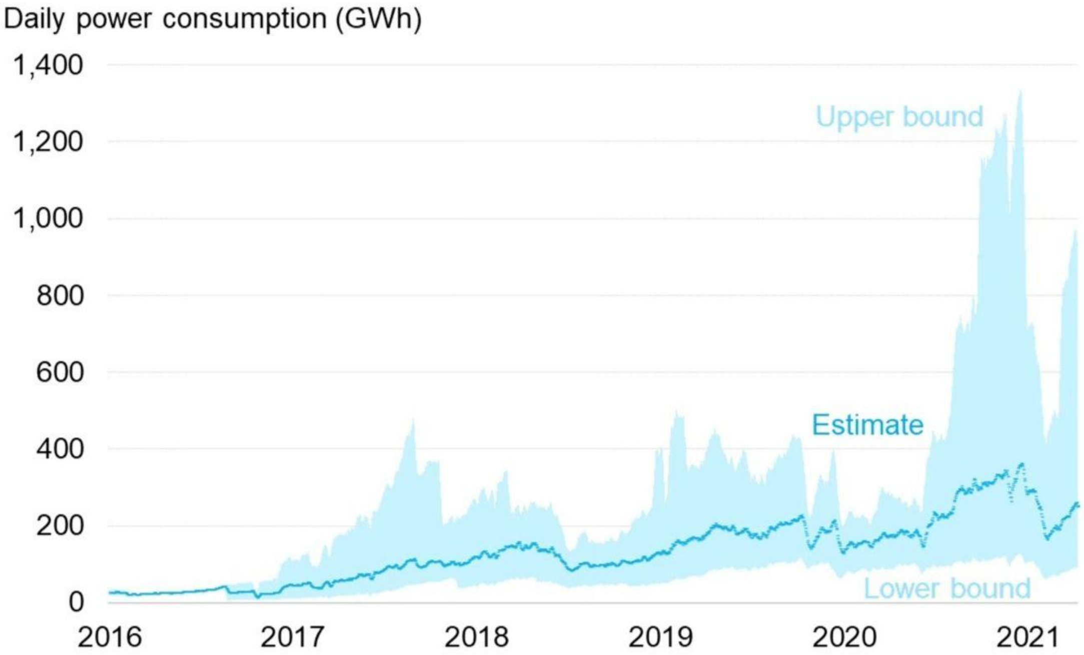
New confirmations appear with each new block that is created

Chainwork

For bitcoin - Longest chain doesn't necessarily mean literal longest, it means chain with the most "chainwork"



Issue - Energy use increases with Moore's law!



On par with a small country

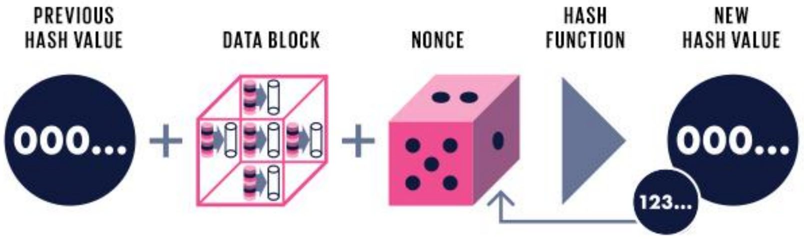
Why bother with PoW?

Solves

- Blockchain conflict
- Node creation and creation time
- Coin generation and distribution
- Incentive

Problems

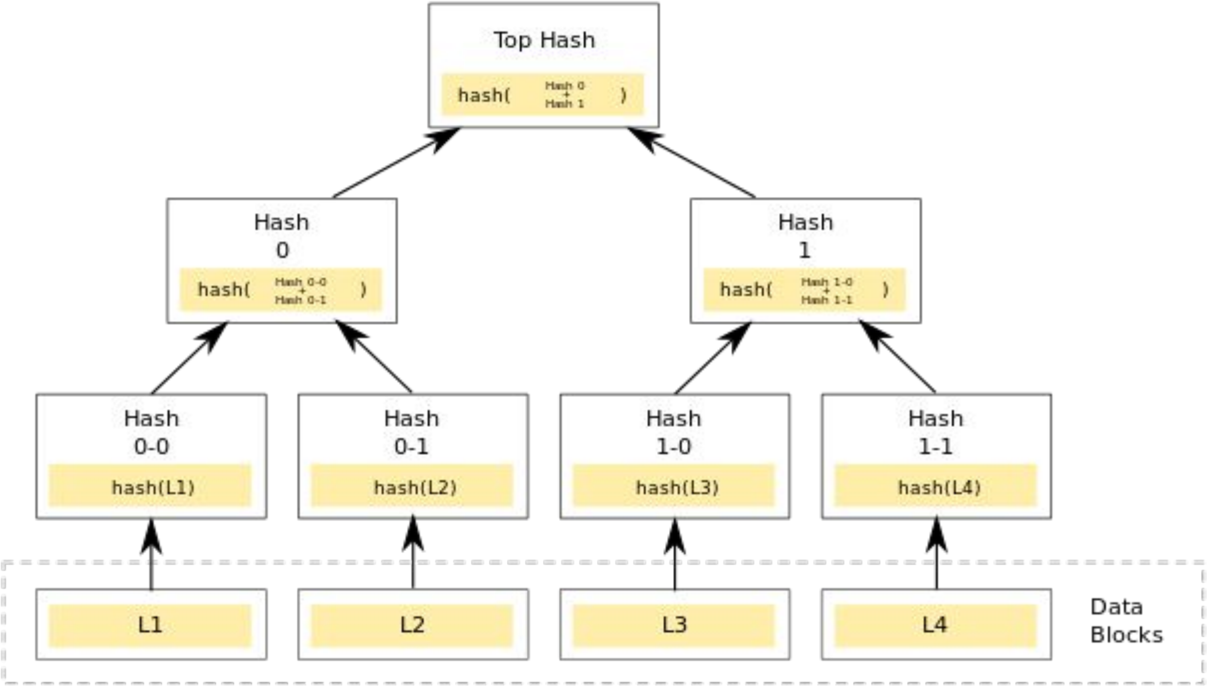
- Energy
- 51% attack
- Mining pool



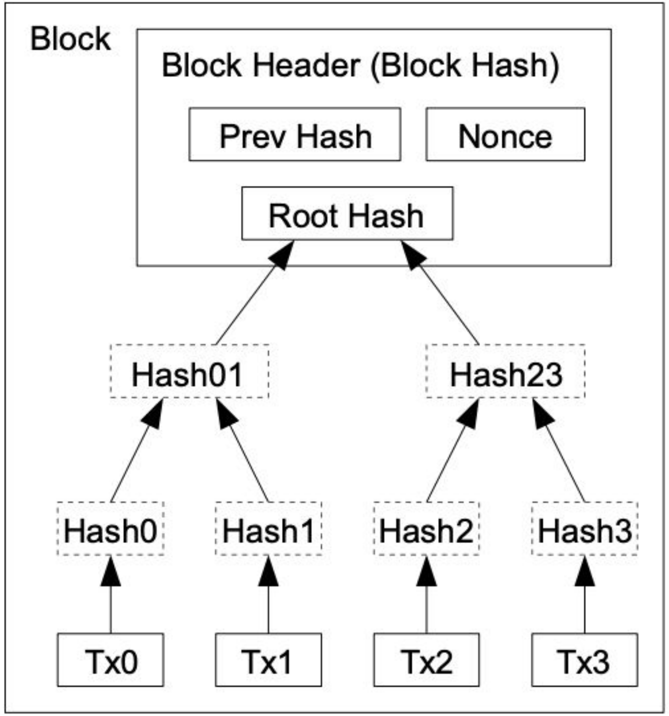
Consensus Mechanism

- Proof of Stake
  - Validators put “collateral” in blockchain. Validators picked at random based on collateral size
  - If validator enters faulty transaction a fraction of collateral is lost.
- Proof of Capacity
  - Instead of cpu power PoC relies on disk space
- Proof of Authority
  - Moderators: block validators
- Practical Byzantine Fault Tolerance
  - f faulty replicas, n-f>f. But f faulty in n-f, so n - 2f > f, n > 3f replicas.
  - Not as decentralized as PoW, performance drop with more replicas.

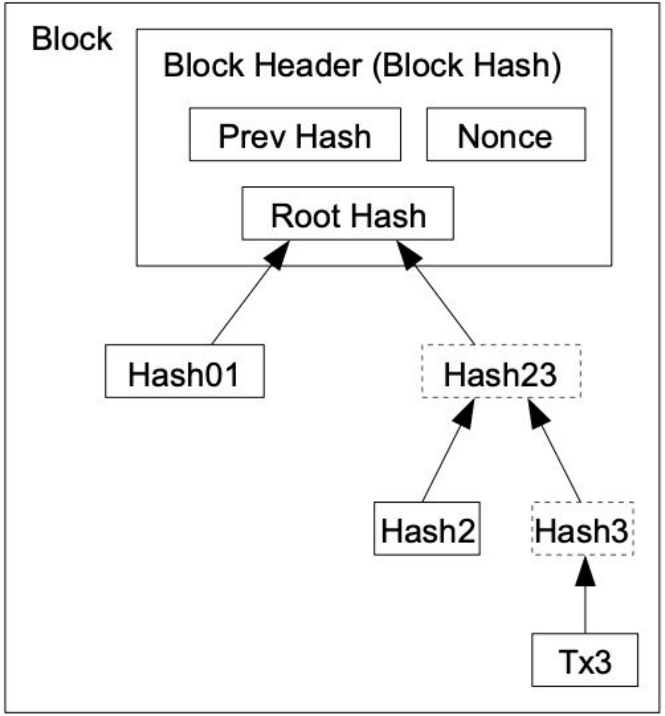
Merkle Tree


Top Hash
hash(Hash 0 + Hash 1)
Hash 0
hash(Hash 0-0 + Hash 0-1)
Hash 1
hash(Hash 1-0 + Hash 1-1)
Hash 0-0
hash(L1)
Hash 0-1
hash(L2)
Hash 1-0
hash(L3)
Hash 1-1
hash(L4)
L1
L2
L3
L4
Data Blocks

Merkle Tree: Pruning

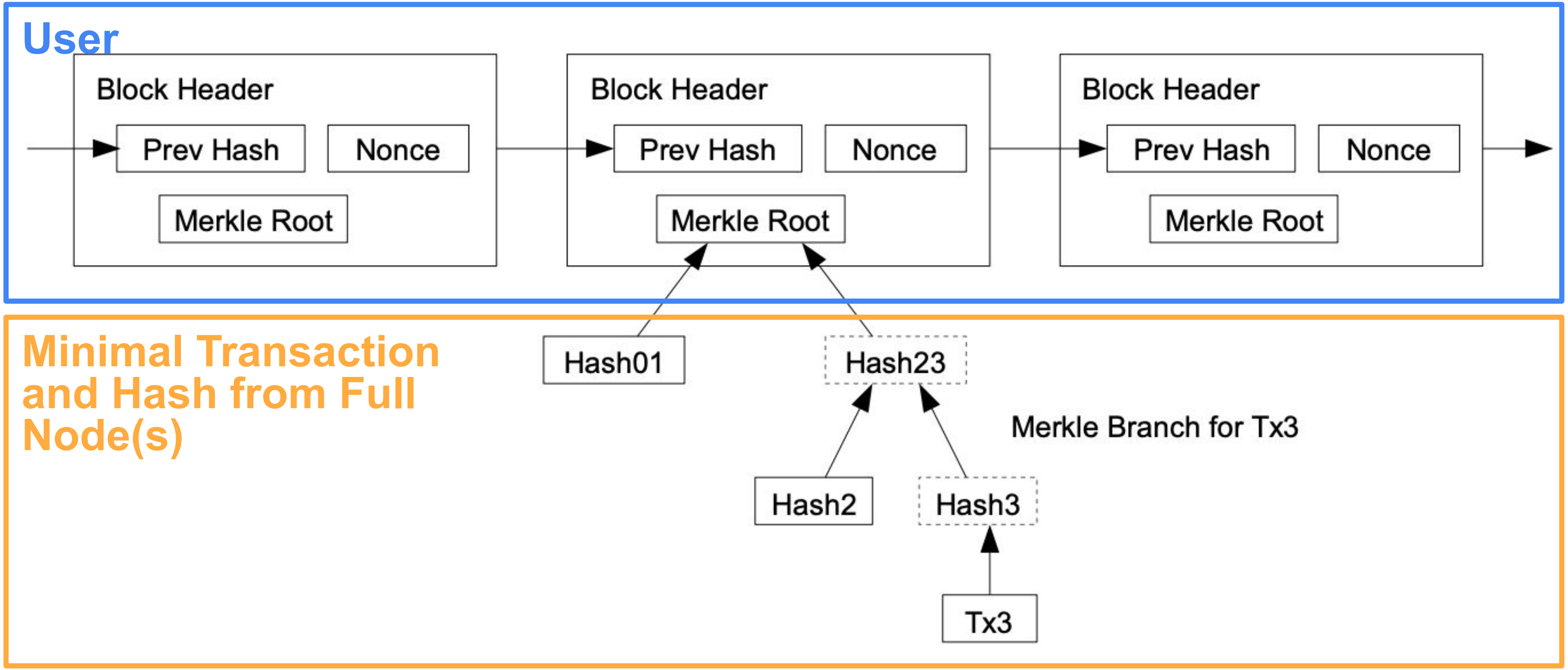


Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

Merkle Tree: Simplified Payment Verification



User

Block Header

Prev Hash

Nonce

Merkle Root

Block Header

Prev Hash

Nonce

Merkle Root

Block Header

Prev Hash

Nonce

Merkle Root

Minimal Transaction and Hash from Full Node(s)

Hash01

Hash23

Merkle Branch for Tx3

Hash2

Hash3

Tx3

Hard, Soft Forks and Chain splits

What happens when things go wrong

Soft fork

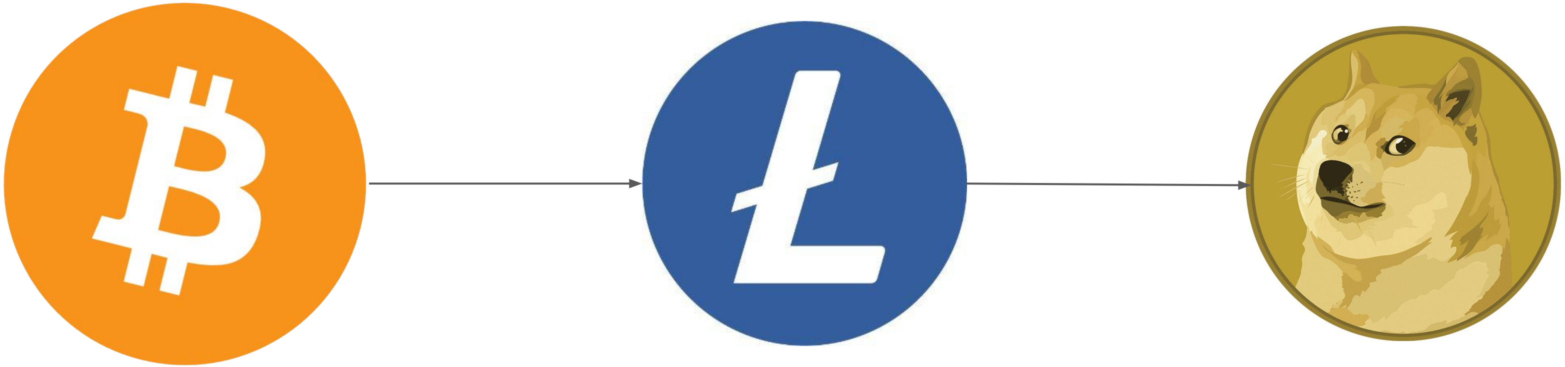
- Backwards compatible
- Previously valid blocks are made invalid.
- Old nodes recognize new block as valid.
- Ex: Decrease **max** block size from 1 MB to 0.5 MB

Only 1 blockchain!

Hard Fork

- Not backwards compatible
- Blocks previously invalid are now valid and previously valid blocks are invalid
- Ex: Change block size from 1MB to a strict 2MB

Multiple Blockchains!



Smart contracts

“A set of promises, specified in digital form, including protocols within which the parties perform on these promises”

The third-party to execute contracts?

- Contract-execution automation on chain
- Core access point between applications and blockchain on Ethereum dApp

More applications, more concepts

- Decentralized Finance (DeFi)
- Non-fungible token (NFT)
  - Opensea.io
- Privacy-Preserving Compute Network
- ...