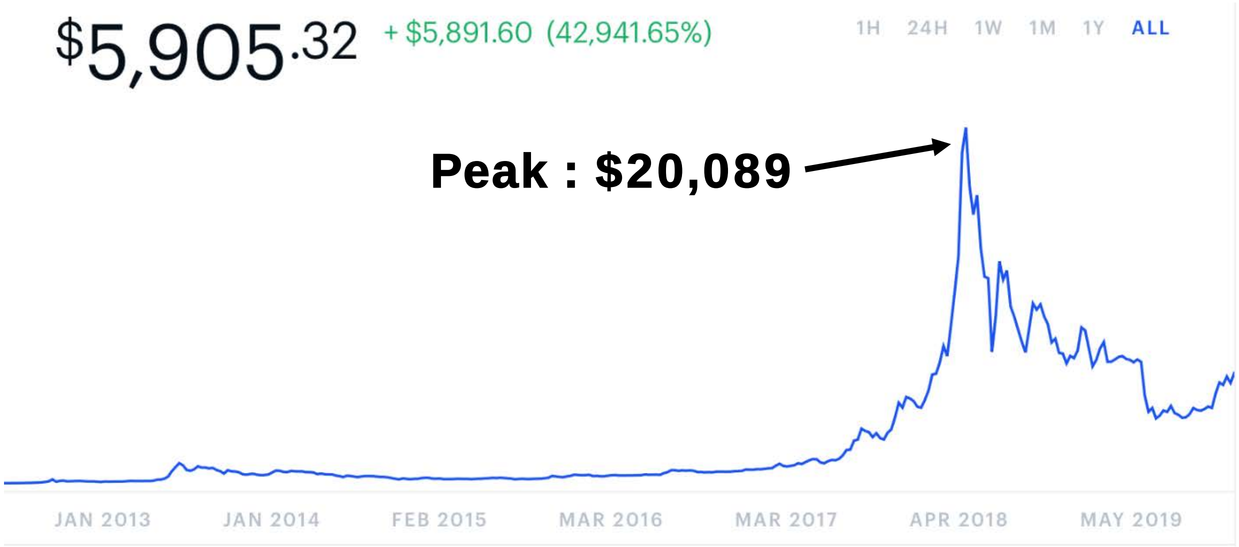
# BitCoin and Blockchain

# The rise of cryptocurrencies

- Bitcoin Price (USD) – Source : coinbase.com



**Peak : $20,089**

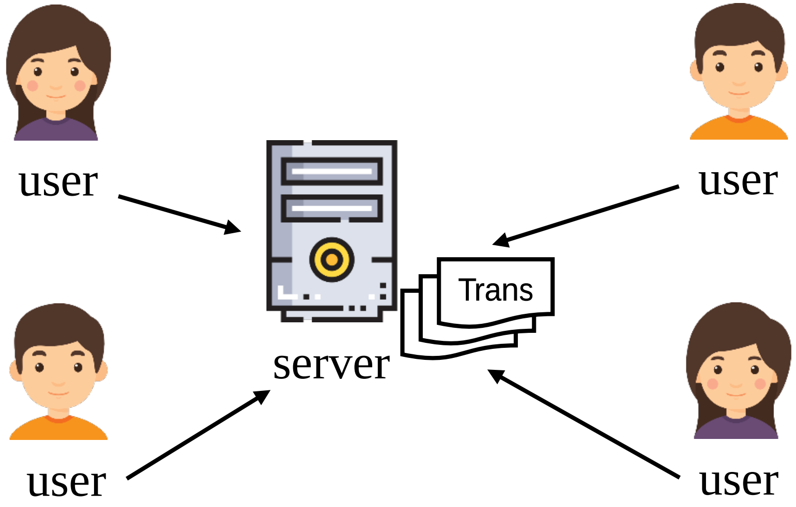
- Bitcoin sparked research into multiple challenging areas and applications
  - more than 2000+ cryptocurrency startups according to angel.co

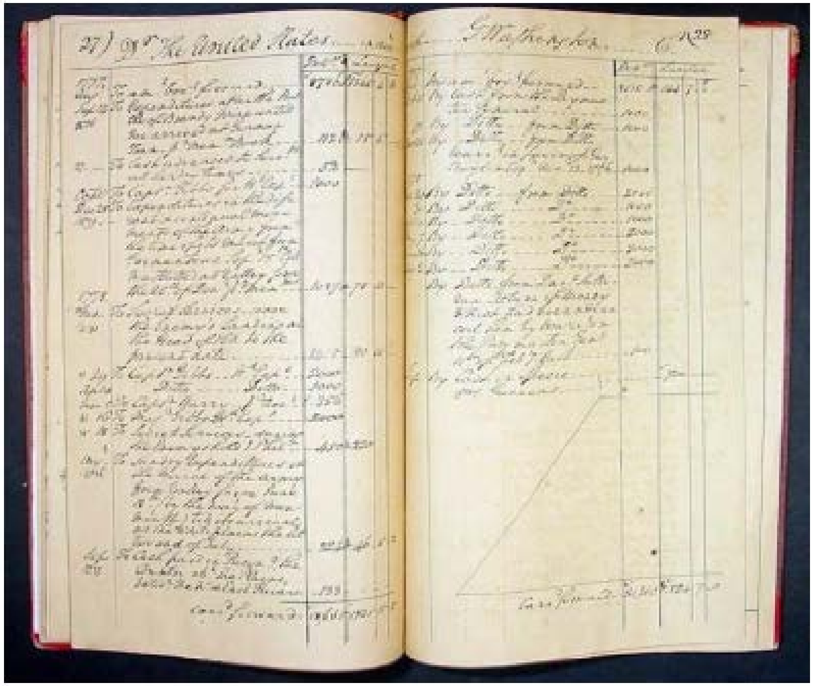
# Properties of Bitcoin

- Decentralization
  - no central authority that controls the entire network
- Non-repudiation
  - participants in the bitcoin network cannot deny their transactions
- Immutability
  - once a transaction is written into the ledger (i.e., blockchain), it cannot be altered
- Pseudonymous
  - no association between bitcoin participants and real-world identities

# A centralized ledger

- E-ledger (list of transactions)
  - a ledger in bitcoin is to trace the transaction-history of a coin
    - No balance of a person/account appears anywhere
  - but, a ledger in a bank maintains the current balance all the time

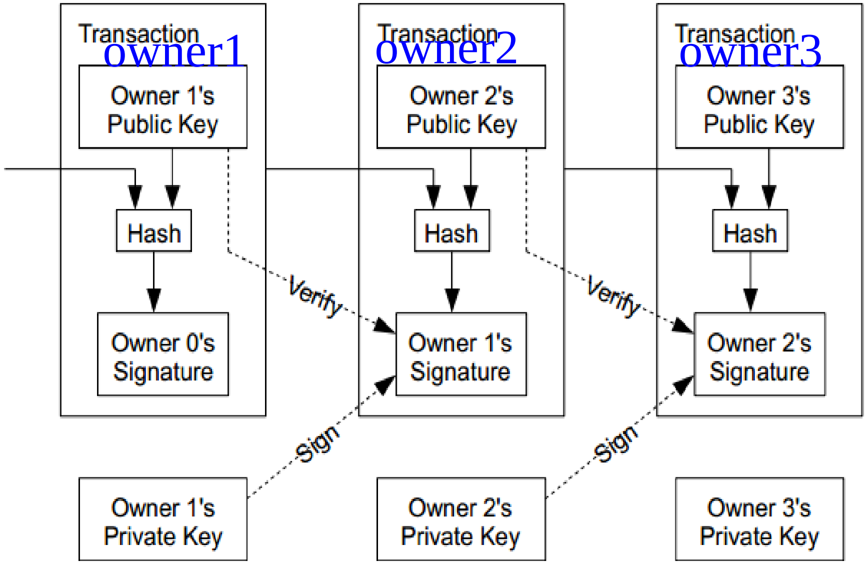




# Non-repudiation: sign transactions

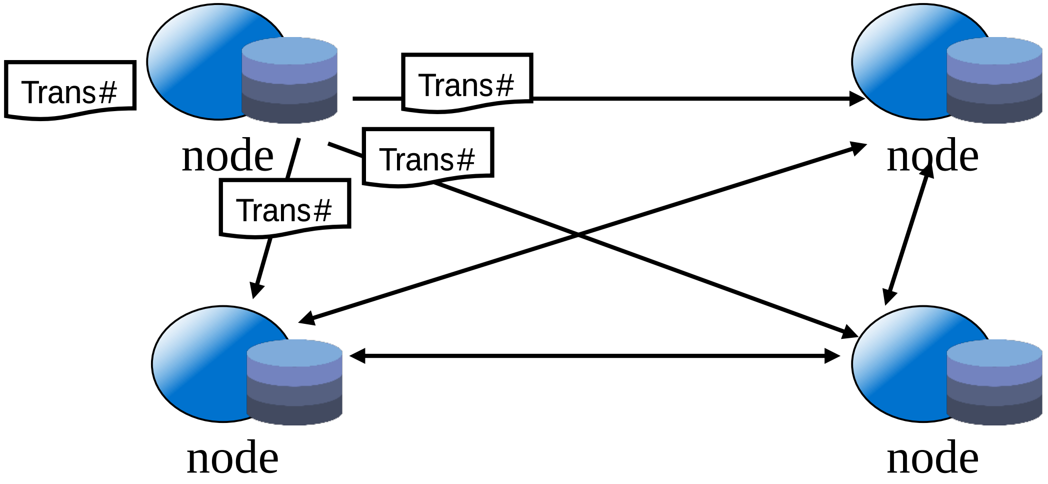
- Digital coin == chain of digital signatures
- Ownership transfer of a coin:
  - Each person is identified by his public key in the cyber world
  - *A* transfers a coin to *B*: *A* signs the trans. using its private key
  - Sign(*Prev trans + New owner's public key*) // '+': concatenate 2 msgs
- Anyone can verify the transfer from the (n-1)th owner to the nth

- But, who is responsible to keep the history of transactions in a decentralized system?



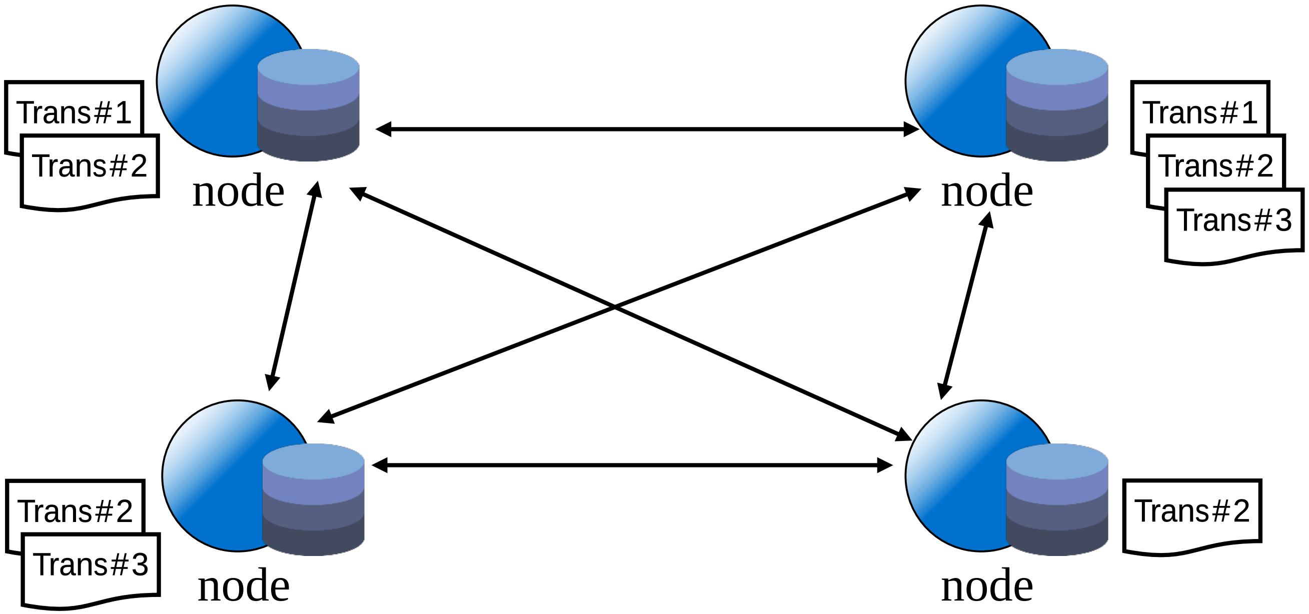
# A decentralized ledger

- Challenges in decentralized systems:
  - no authority keeps the transaction history
  - people may fake a transaction or double spend a coin by taking advantages of network delay
- To prevent fraud and double-spending:
  - each transaction is broadcast to all nodes
  - a transaction is confirmed only after verification (by whom?)



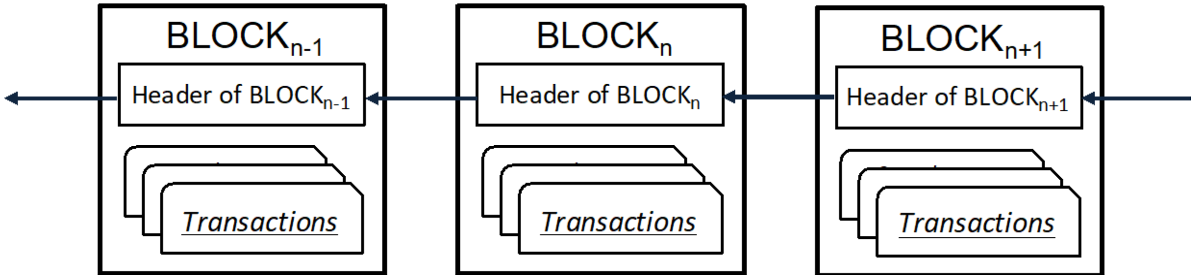
# Consistency of a distributed ledger

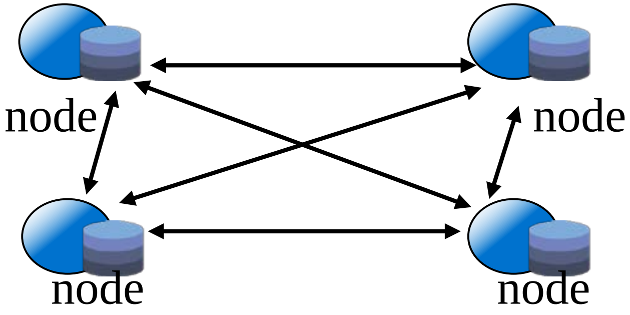
- Nodes receive different sets of trans at any time-point due to different network delays
- How to organize and verify the transactions to make a consistent distributed ledger?



# Blockchain and transactions

- Blockchain, a chain of blocks, is a distributed ledger, recording all trans in the system
  - each block contains of a set of verified trans
- Each node (mining node) selects a set of trans from its local pool, verifies them, generates a new block, and links the new block to the chain
- Other nodes, upon receiving this new block, will accept the new block by further linking their new blocks to it
  - by “accept a block”, it means to verify the trans again in the block to prevent the creator of the block from making any fraud trans

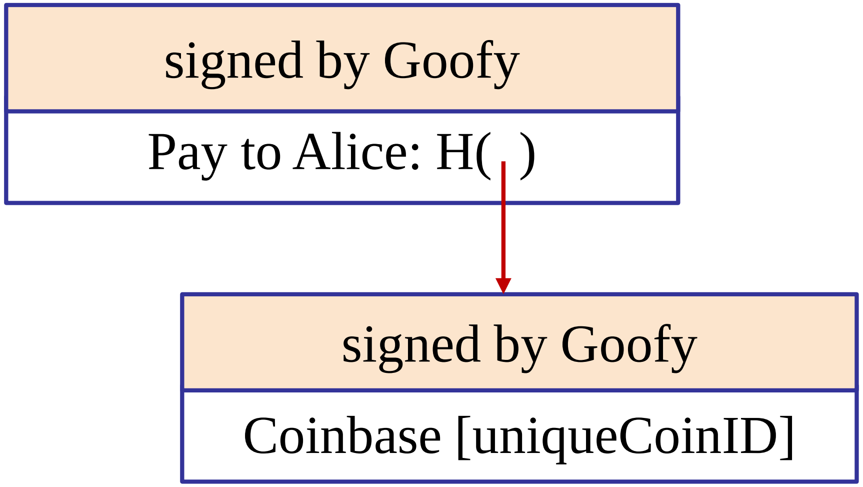




# Transaction flow

- The coin was created for Goofy by the *Coinbase transaction* (discussed later) and Goofy is the owner
- Transactions over a coin are chained up

A coin’s owner can spend/transfer it


signed by Goofy

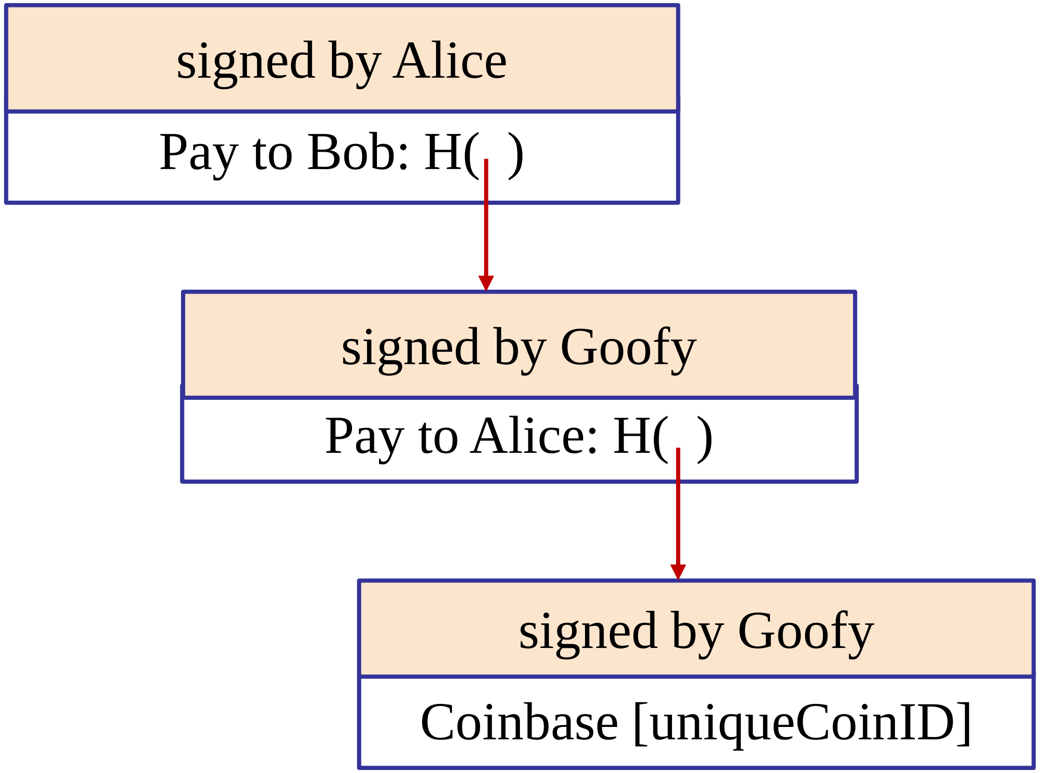
Pay to Alice: H( )

signed by Goofy

Coinbase [uniqueCoinID]

# Chain of transaction flow

The recipient can pass on the coin again



signed by Alice

Pay to Bob: H( )

signed by Goofy

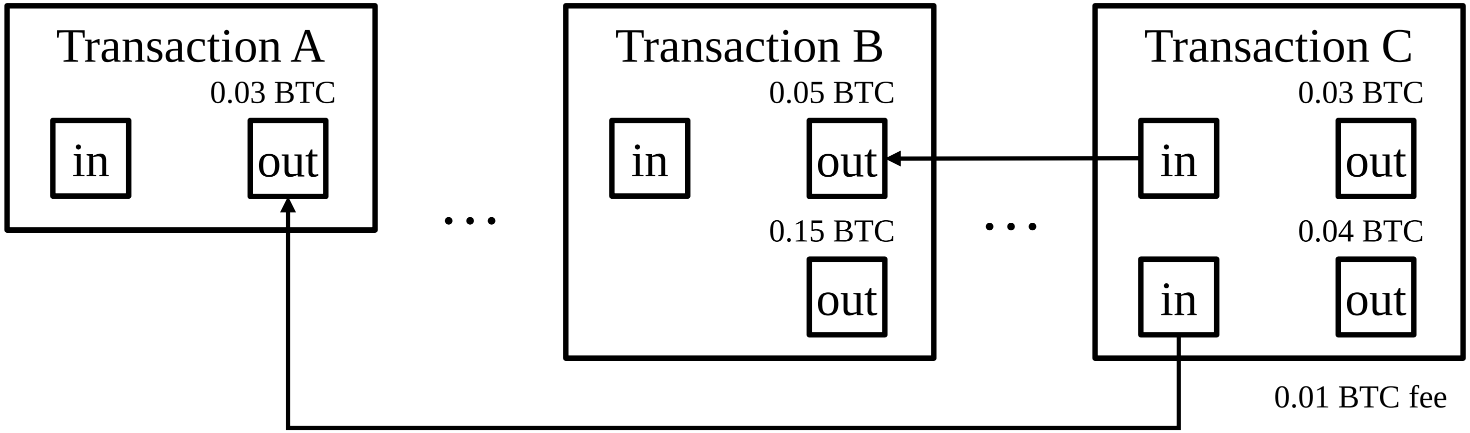
Pay to Alice: H( )

signed by Goofy

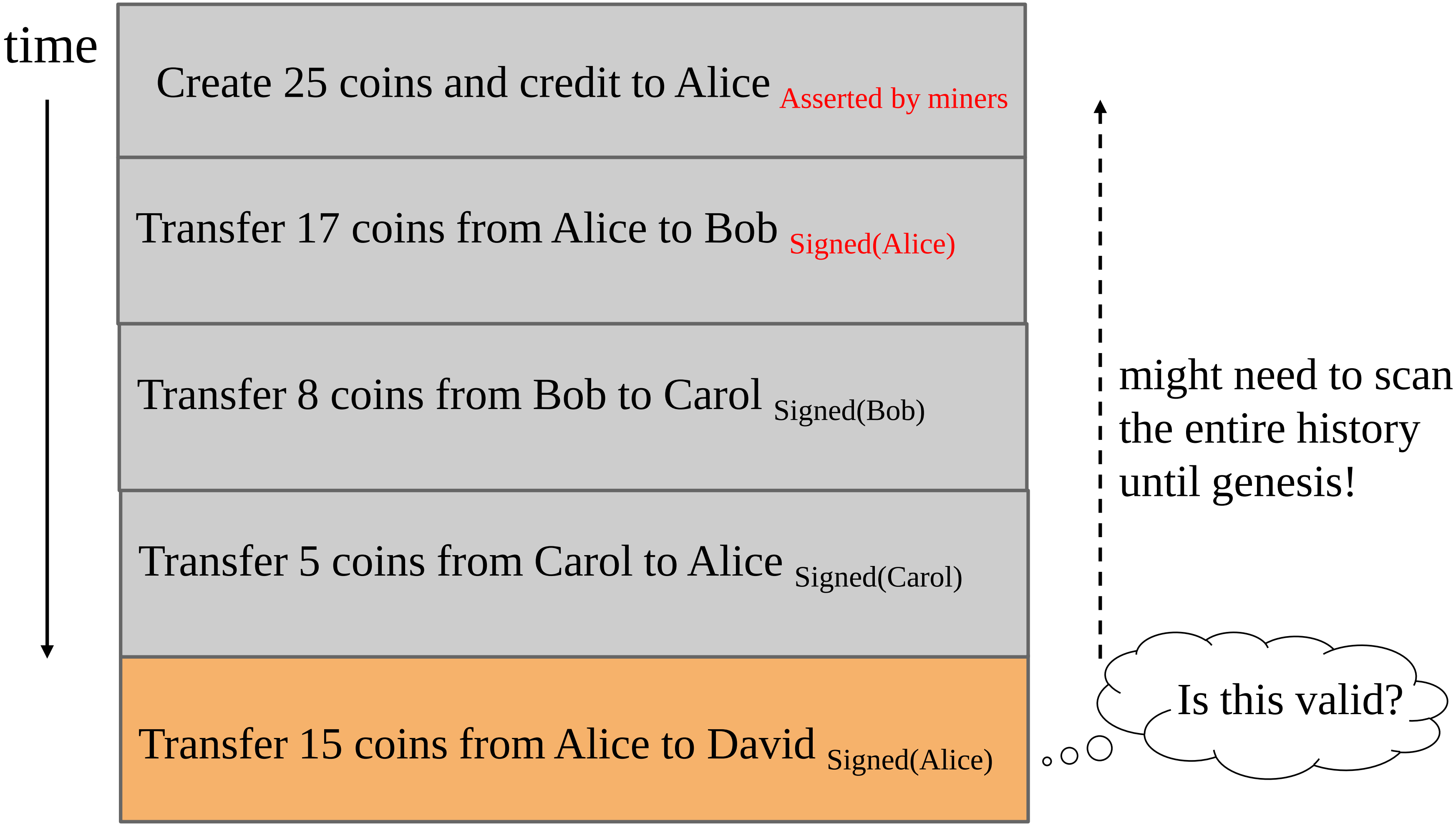
Coinbase [uniqueCoinID]

# Full transaction chain: A ledger

- The full chain is a complete ledger/ history of all trans
  - the input of the current trans points to the output of an earlier trans, indicating the source of the trans
- The history of the full blockchain reveals the state/ ownership of all bitcoins (BTC)
- The ledger is structured in terms of transactions
  - no explicit “account balance”



# Trans-based ledger: without in/out pointer



time

Create 25 coins and credit to Alice Asserted by miners

Transfer 17 coins from Alice to Bob Signed(Alice)

Transfer 8 coins from Bob to Carol Signed(Bob)

Transfer 5 coins from Carol to Alice Signed(Carol)

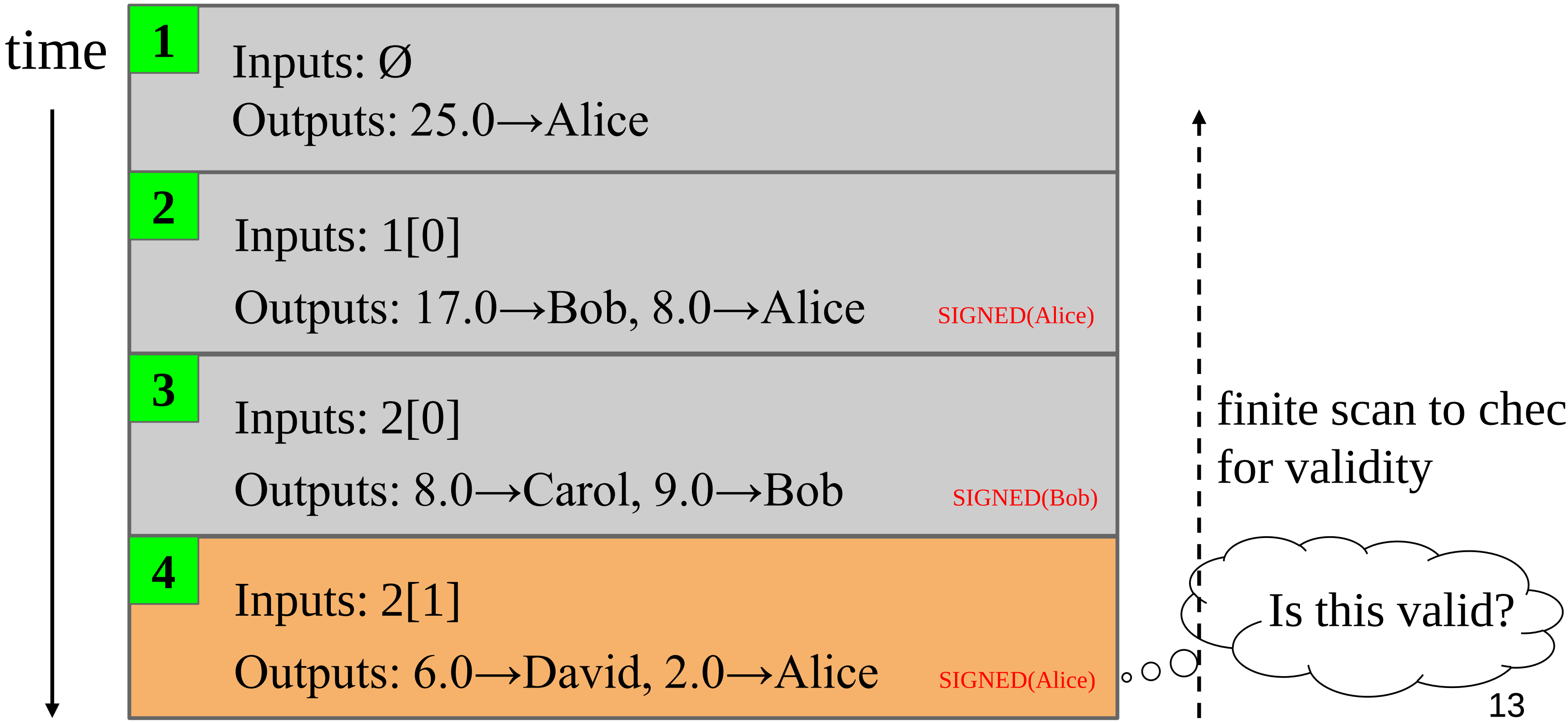
Transfer 15 coins from Alice to David Signed(Alice)

might need to scan the entire history until genesis!

Is this valid?

# Trans-based ledger with in/out pointer (Bitcoin)

- Each trans has inputs /outputs
  - inputs specifies source of coins; outputs the recipients of coins
- Easy to check if a transaction is valid (owner has sufficient coins?)



time

1

Inputs: Ø

Outputs: 25.0→Alice

2

Inputs: 1[0]

Outputs: 17.0→Bob, 8.0→Alice

SIGNED(Alice)

3

Inputs: 2[0]

Outputs: 8.0→Carol, 9.0→Bob

SIGNED(Bob)

4

Inputs: 2[1]

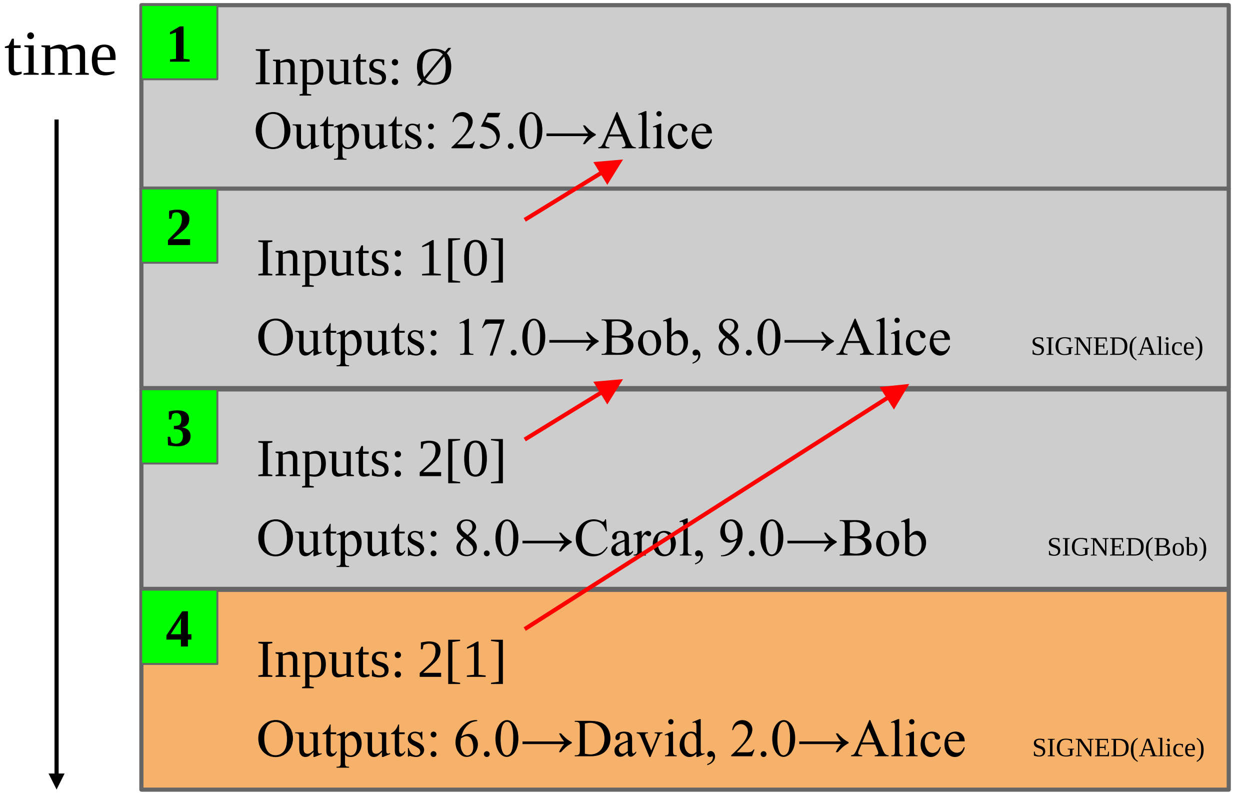
Outputs: 6.0→David, 2.0→Alice

SIGNED(Alice)

finite scan to check for validity

Is this valid?

# Input/output link of transactions



time

1

Inputs: Ø

Outputs: 25.0→Alice

2

Inputs: 1[0]

Outputs: 17.0→Bob, 8.0→Alice

SIGNED(Alice)

3

Inputs: 2[0]

Outputs: 8.0→Carol, 9.0→Bob

SIGNED(Bob)

4

Inputs: 2[1]

Outputs: 6.0→David, 2.0→Alice

SIGNED(Alice)

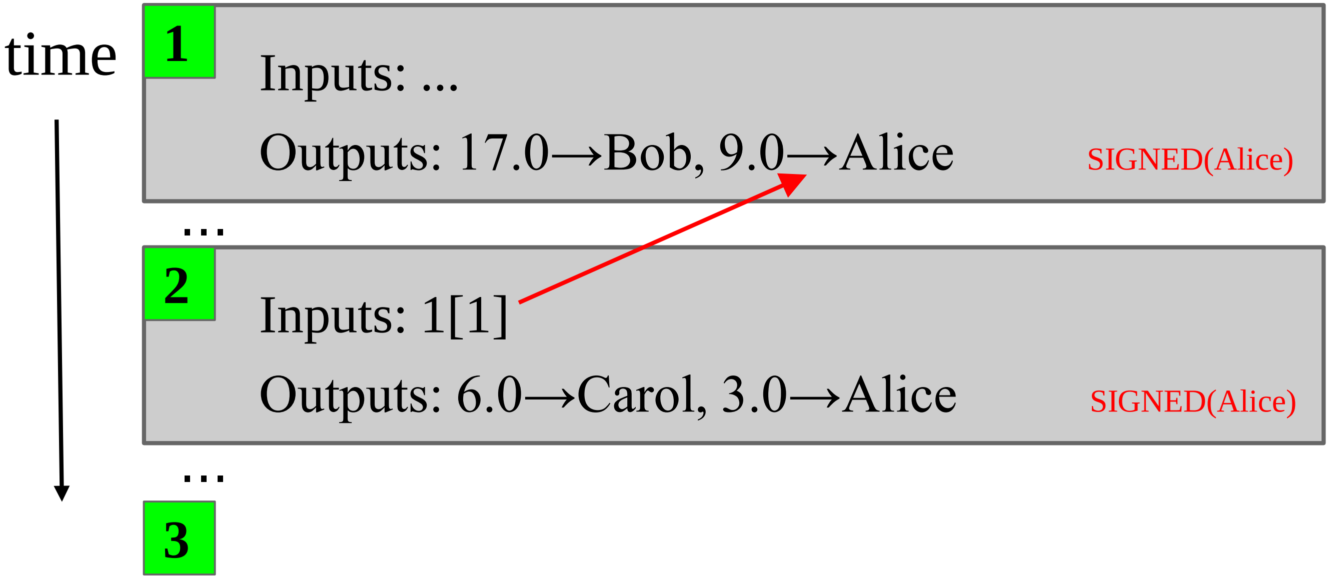
we implement this with hash pointers

SIMPLIFICATION: only one transaction per block

# A transaction with change:

## input value > transfer-value

- Alice has 9 coins and transfers 6 to Carol, and Alice still has 3 coins left
- The transaction has two outputs: one for transferring to Carol and the other for transferring back to Alice
- The total inputs always equal to the total outputs of a trans



time

1

Inputs: ...

Outputs: 17.0→Bob, 9.0→Alice

SIGNED(Alice)

…

2

Inputs: 1[1]

Outputs: 6.0→Carol, 3.0→Alice

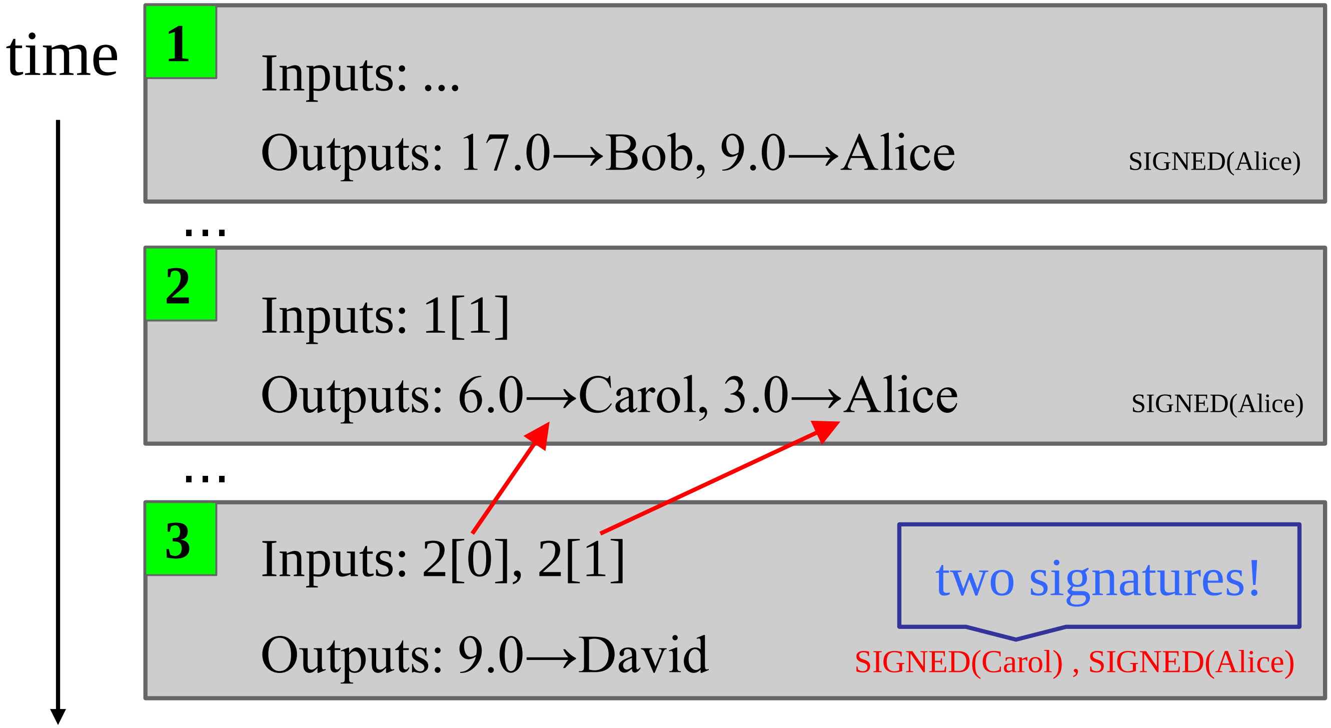
SIGNED(Alice)

…

3

# Joint payment

- *inputs* can come from multiple sources
  - the transaction needs to be signed by all input owners



time

1

Inputs: ...

Outputs: 17.0→Bob, 9.0→Alice

SIGNED(Alice)

...

2

Inputs: 1[1]

Outputs: 6.0→Carol, 3.0→Alice

SIGNED(Alice)

...

3

Inputs: 2[0], 2[1]

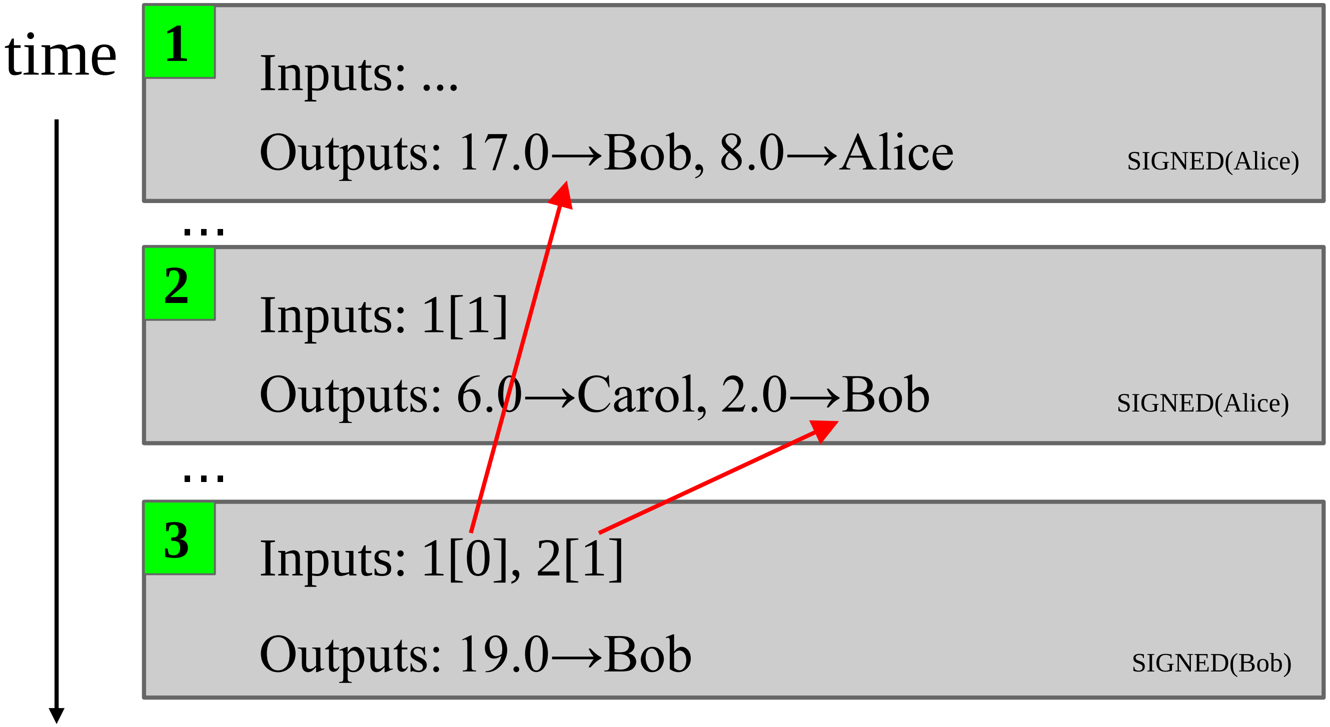
Outputs: 9.0→David

two signatures!

SIGNED(Carol) , SIGNED(Alice)

# Merge multiple outputs

- Merge outputs of multi-trans for the same owner
  - simplify the input of future trans, and
  - make it easy to verify balance of an owner
- The system can do auto-merge



time

1

Inputs: ...

Outputs: 17.0→Bob, 8.0→Alice

SIGNED(Alice)

…

2

Inputs: 1[1]

Outputs: 6.0→Carol, 2.0→Bob

SIGNED(Alice)

…

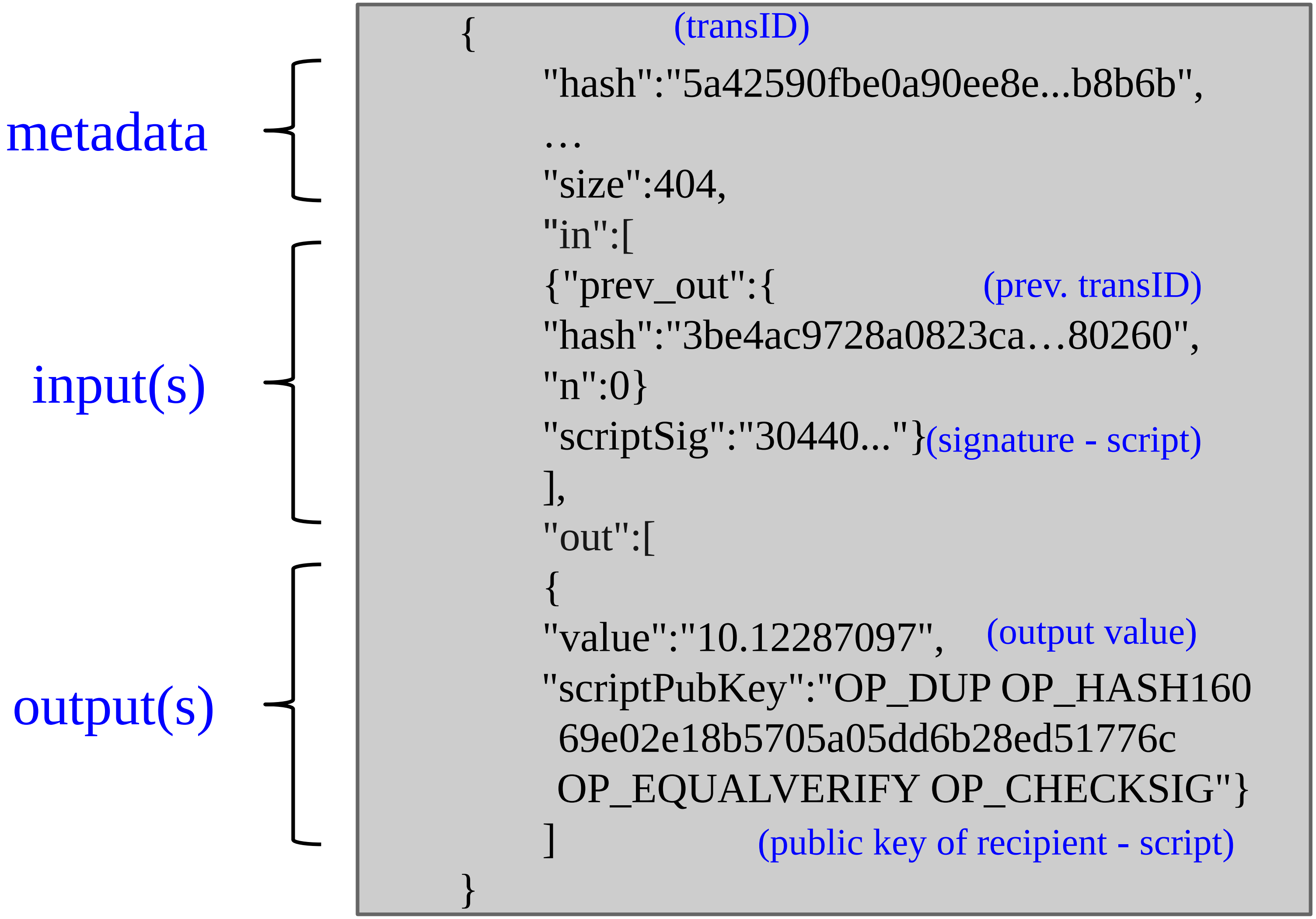
3

Inputs: 1[0], 2[1]

Outputs: 19.0→Bob

SIGNED(Bob)

# Transaction syntax



metadata

input(s)

output(s)

```
{                       (transID)
        "hash":"5a42590fbe0a90ee8e...b8b6b",
        …
        "size":404,
        "in":[
        {"prev_out":{                    (prev. transID)
        "hash":"3be4ac9728a0823ca…80260",
        "n":0}
        "scriptSig":"30440..."}(signature - script)
        ],
        "out":[
        {
        "value":"10.12287097",    (output value)
        "scriptPubKey":"OP_DUP OP_HASH160
         69e02e18b5705a05dd6b28ed51776c
         OP_EQUALVERIFY OP_CHECKSIG"}
        ]               (public key of recipient - script)
}
```

# Coinbase transaction

metadata

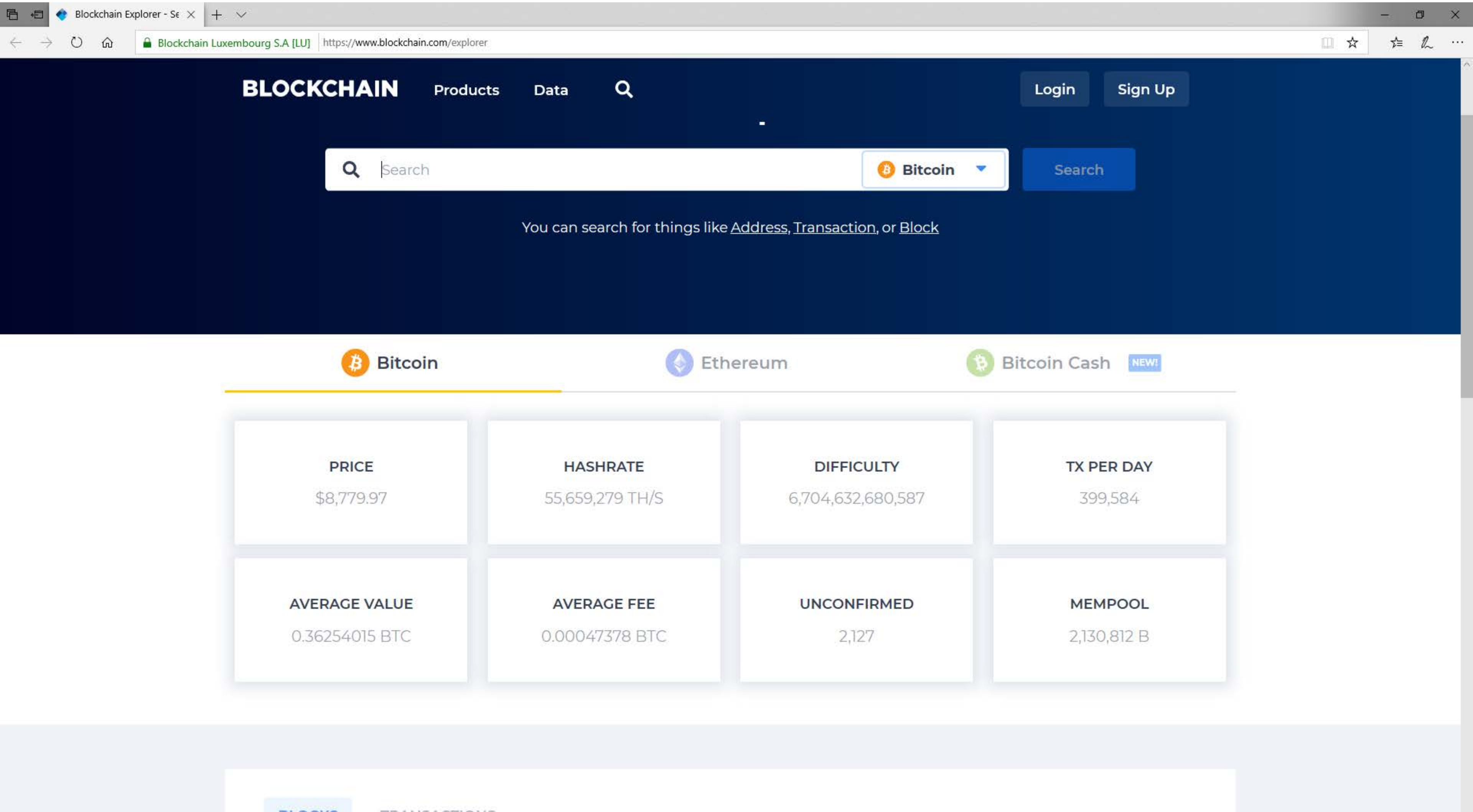
input(s)

output(s)

```
{
        "hash":"5a42590fbe0a90ee8e...b8b6b",
        …
        "size":404,
        "in":[
        {"prev_out":{        (null transID)
        "hash":"00000000000…000000",
        "n": 4294967295}
        "coinbase":"..."}  (arbitrary)
        ],
        "out":[
        {                    (block reward + trans fees)
        "value":"12.52287097",
        "scriptPubKey":"OP_DUP OP_HASH160
         69e02e18b5705a05dd6b28ed51776c
         OP_EQUALVERIFY OP_CHECKSIG"}
        ]
}
```

# Demo: block, transaction in blockchain

- Demo at https://www.blockchain.com/explorer

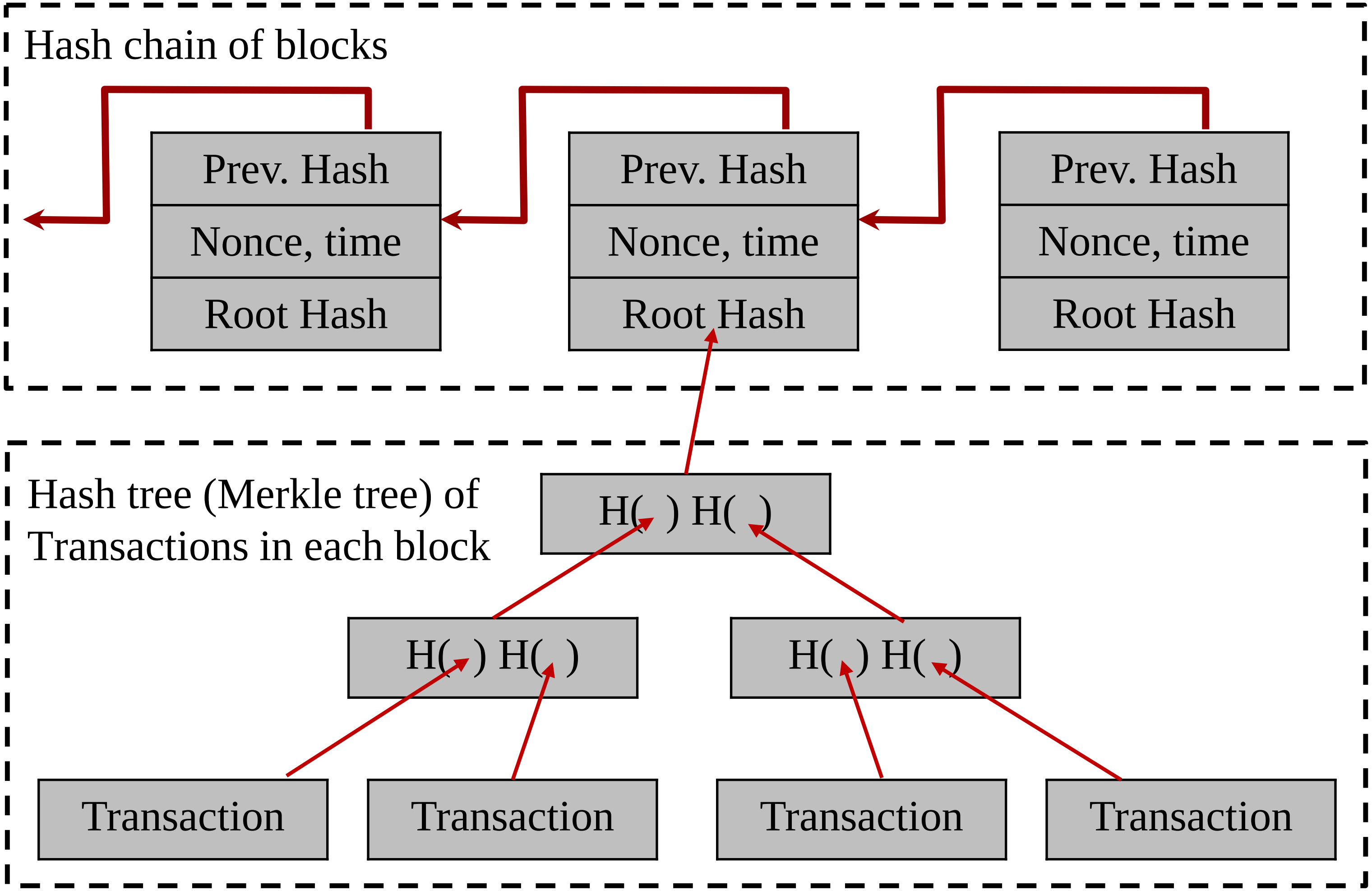


You can search for things like Address, Transaction, or Block

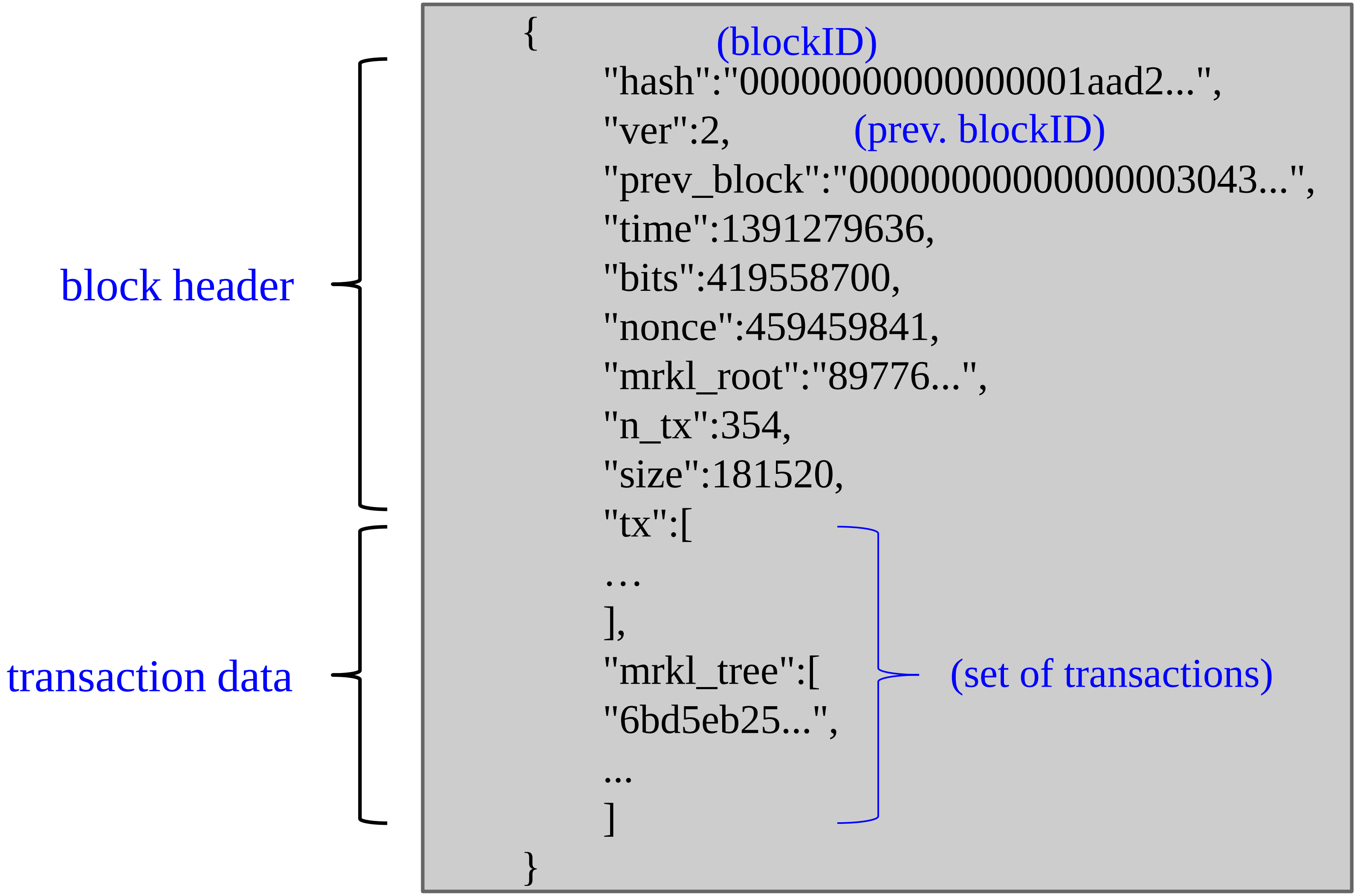
| PRICE | HASHRATE | DIFFICULTY | TX PER DAY |
|---|---|---|---|
| $8,779.97 | 55,659,279 TH/S | 6,704,632,680,587 | 399,584 |
| **AVERAGE VALUE** | **AVERAGE FEE** | **UNCONFIRMED** | **MEMPOOL** |
| 0.36254015 BTC | 0.00047378 BTC | 2,127 | 2,130,812 B |

# Data structure of block: Chain of blocks

- Each block contains a set of verified transactions



# Bitcoin block syntax



block header

transaction data

(blockID)

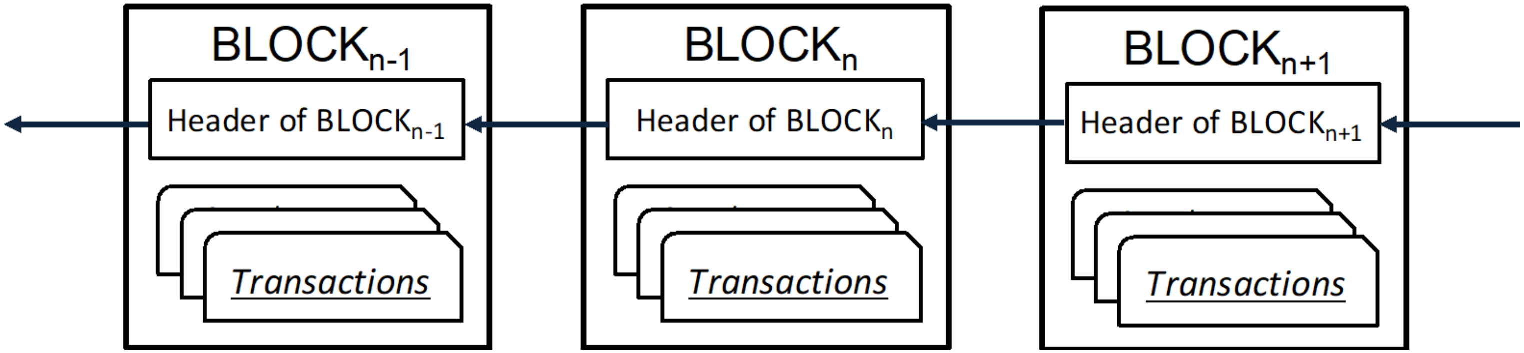
(prev. blockID)

(set of transactions)

```
{
        "hash":"0000000000000001aad2...",
        "ver":2,
        "prev_block":"00000000000000003043...",
        "time":1391279636,
        "bits":419558700,
        "nonce":459459841,
        "mrkl_root":"89776...",
        "n_tx":354,
        "size":181520,
        "tx":[
        …
        ],
        "mrkl_tree":[
        "6bd5eb25...",
        ...
        ]
}
```

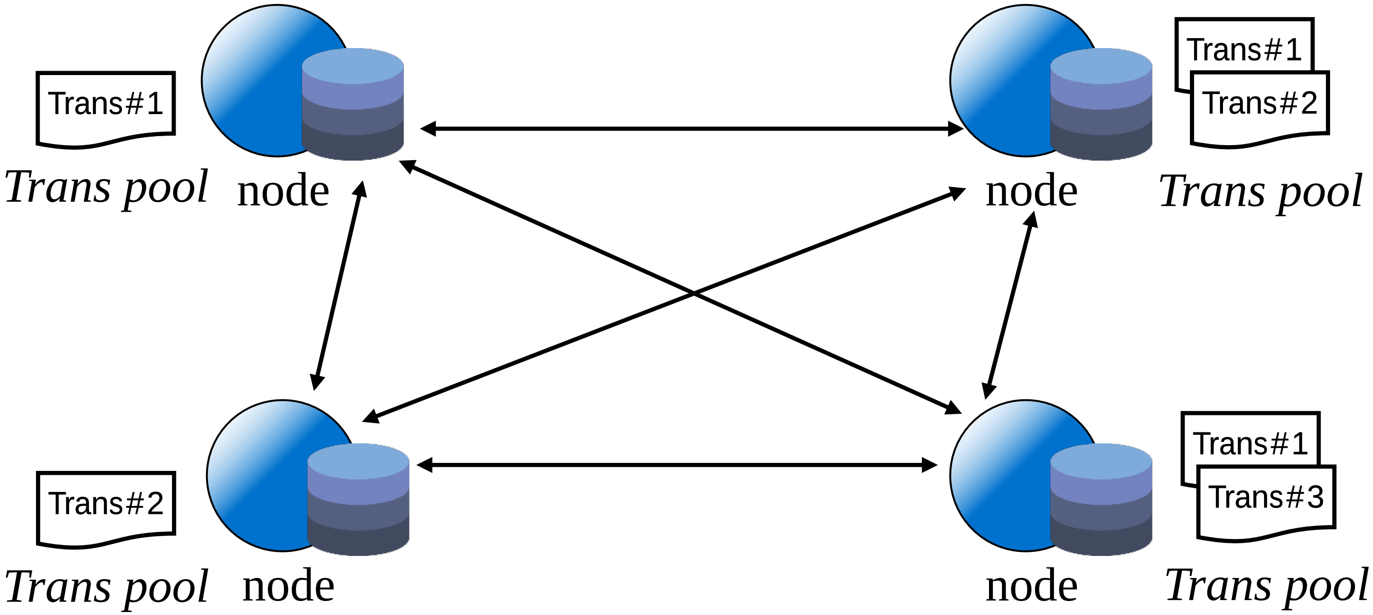
# Immutability and append only of blockchain

- Impossible to alter any transactions in the blockchain:
  - each node keeps a copy of the chain locally and all copies are consistent
  - each transaction is signed and verified



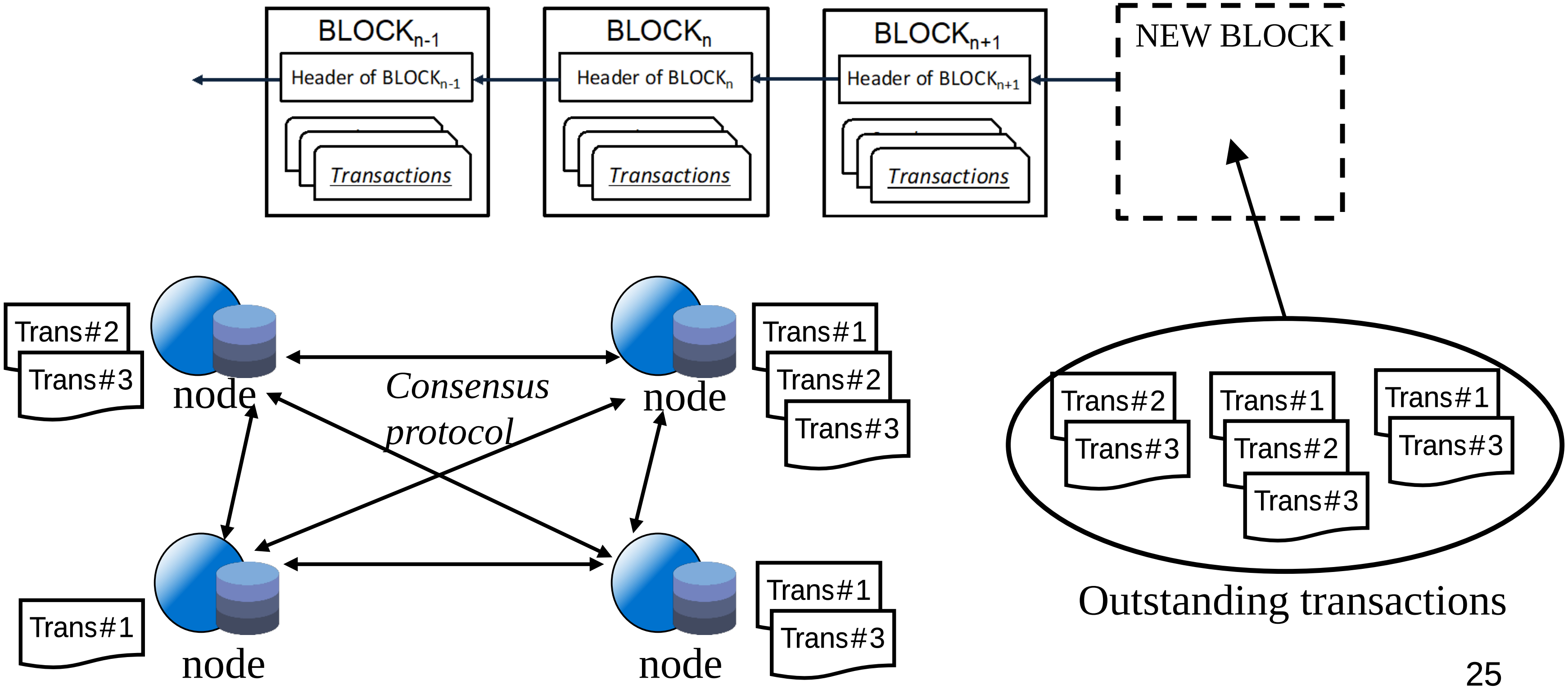
# Inconsistency of trans pools at nodes

- Each transaction is broadcast to all nodes and nodes have different sets of trans due to network delay
- Each node selects a subset of trans from its local pool, verifies them and competes with other nodes to solve PoW
  - A node broadcasts a new block if it successfully solves PoW before others
- A new block is accepted by a node if it builds the next block upon this block

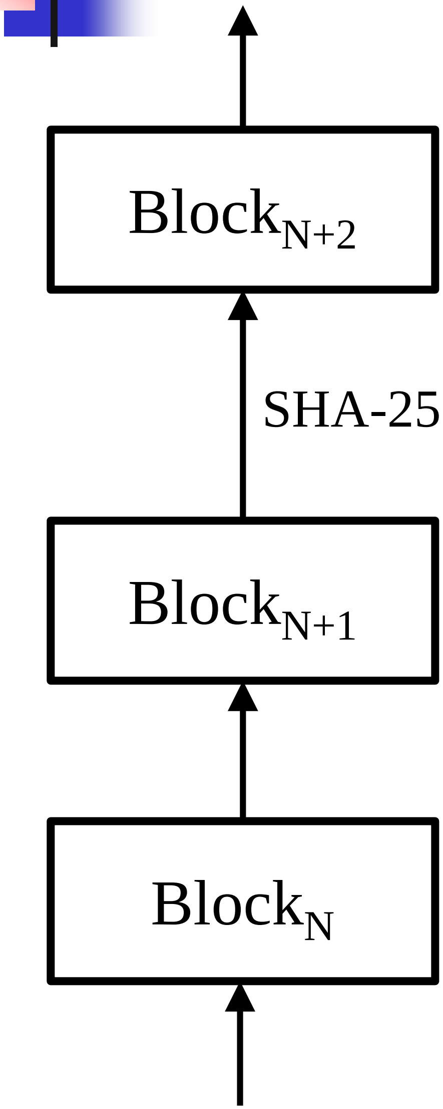


# Distributed consensus: Block mining

- Each miner (i.e., node) has a set of outstanding transactions it has received
- All miners execute a computationally–intensive process to decide which block to be extended



# Block mining: Proof-of-Work (PoW)



$\text{SHA-256\^{}2}(\text{Block}_{N+1}, X_{N+1}, \text{ticket}_{N+1}) = 0x\overbrace{0000000000000}^{\text{Mining difficulty}}c67aa..$

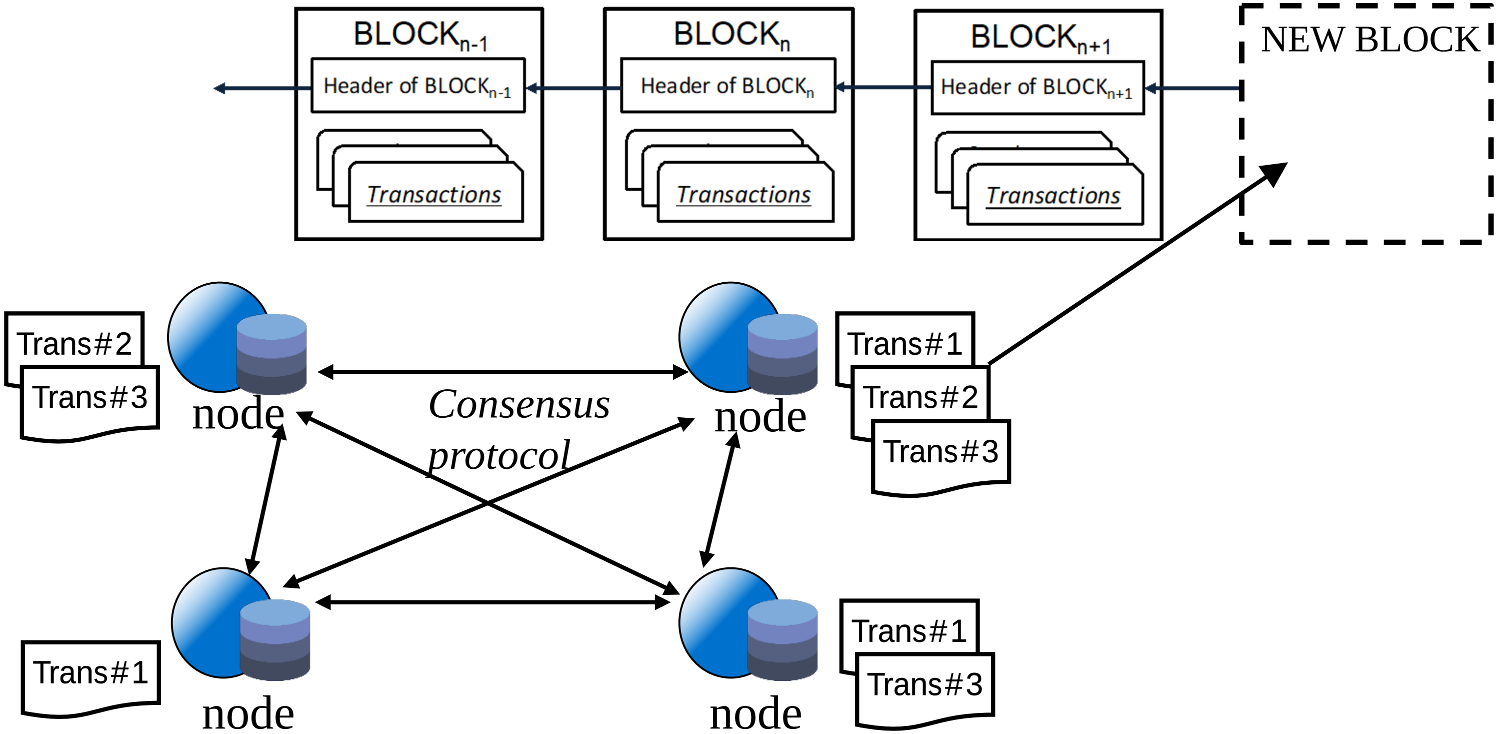
Mining problem: Find a ticket that produces a hash value less than target Z

$\boxed{\text{SHA-256\^{}2}(\text{Block}_{Prev}, X_N, \text{ticket}_N) \overset{?}{<} Z}$

software version, hash (Merkle-tree root) of trans, and current time

# Mining a new block: verify transactions and PoW

- Each miner picks a set of trans from its local pool & verifies them
- Computes the PoW and if successful:
  - link the block to the local chain, and
  - broadcast the block to the network

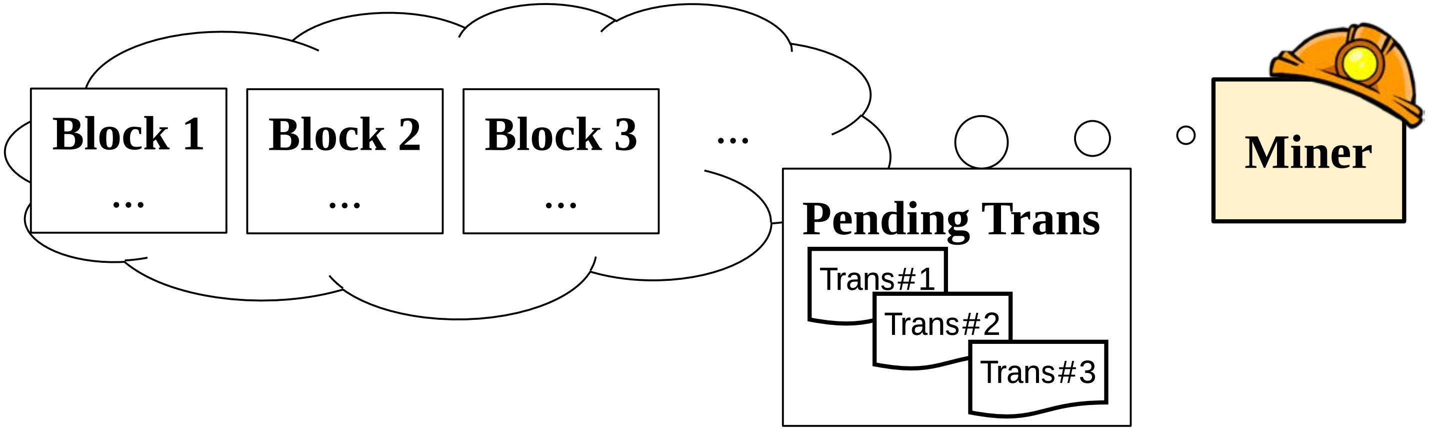


# Example: miners generate a new block

Each attempt has $16^{-3}$ chance of success

`Z = 0x000***...`

`Hash(Block 3 |  …  | 0xb9824 ) = 0x000c3f...`



Block 1
…

Block 2
…

Block 3
…

…

Pending Trans

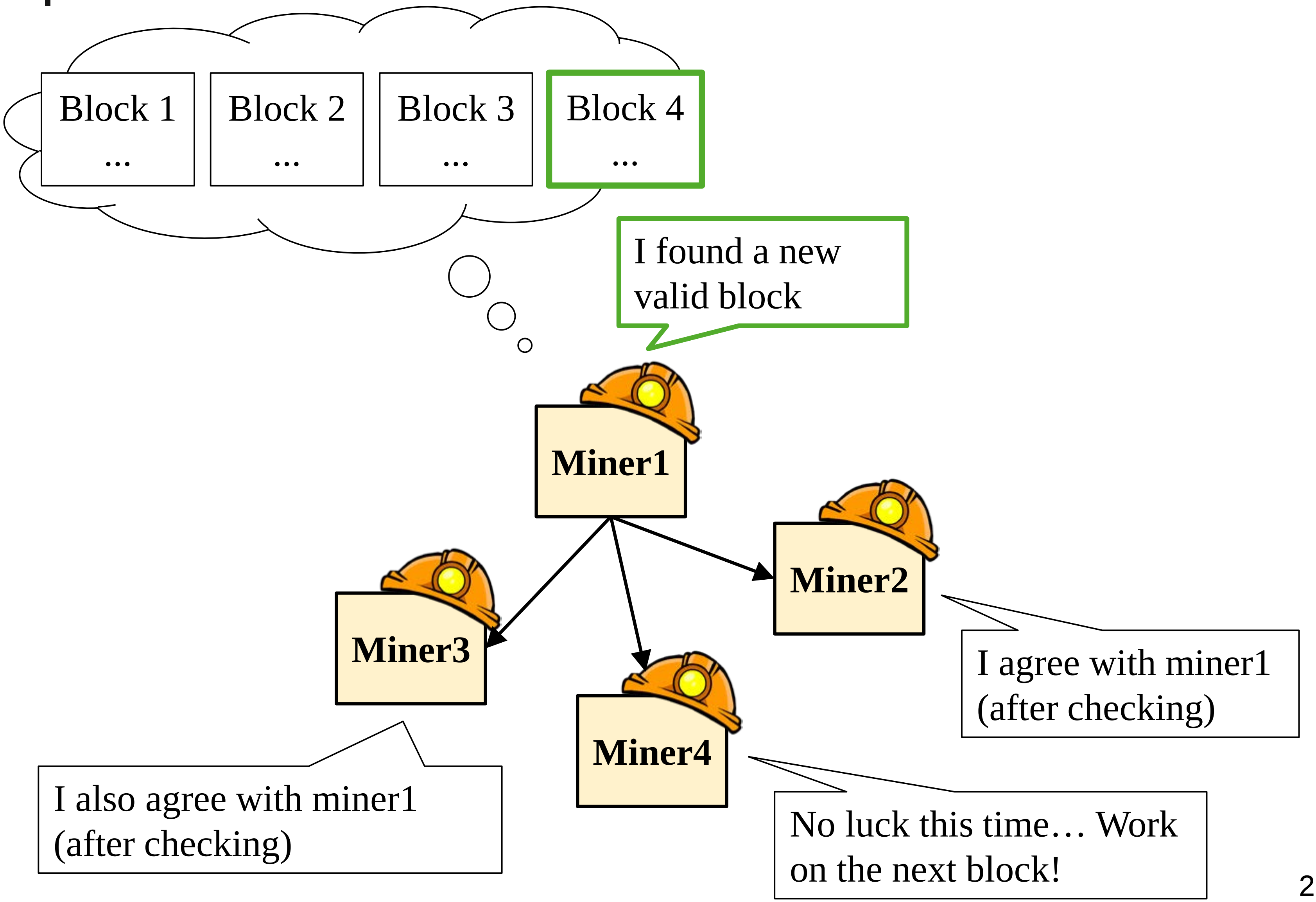
Trans#1

Trans#2

Trans#3

Miner

# What if a miner loses the competition?



Block 1 …

Block 2 …

Block 3 …

Block 4 …

I found a new valid block

Miner1

Miner2

Miner3

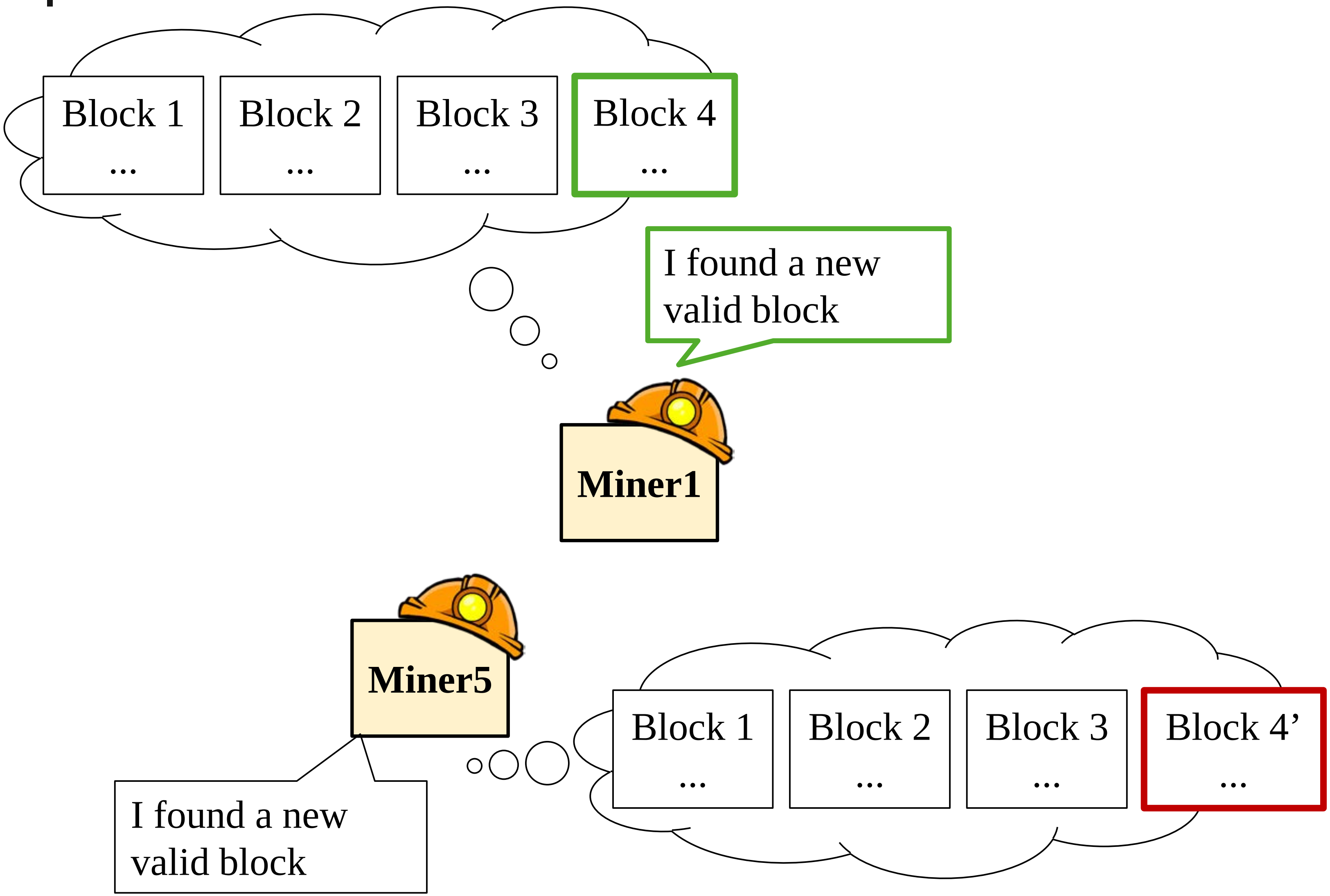
Miner4

I agree with miner1 (after checking)

I also agree with miner1 (after checking)

No luck this time… Work on the next block!

# What if two miners succeed simultaneously?



Block 1 …

Block 2 …

Block 3 …

Block 4 …

I found a new valid block

Miner1

Miner5

I found a new valid block

Block 1 …

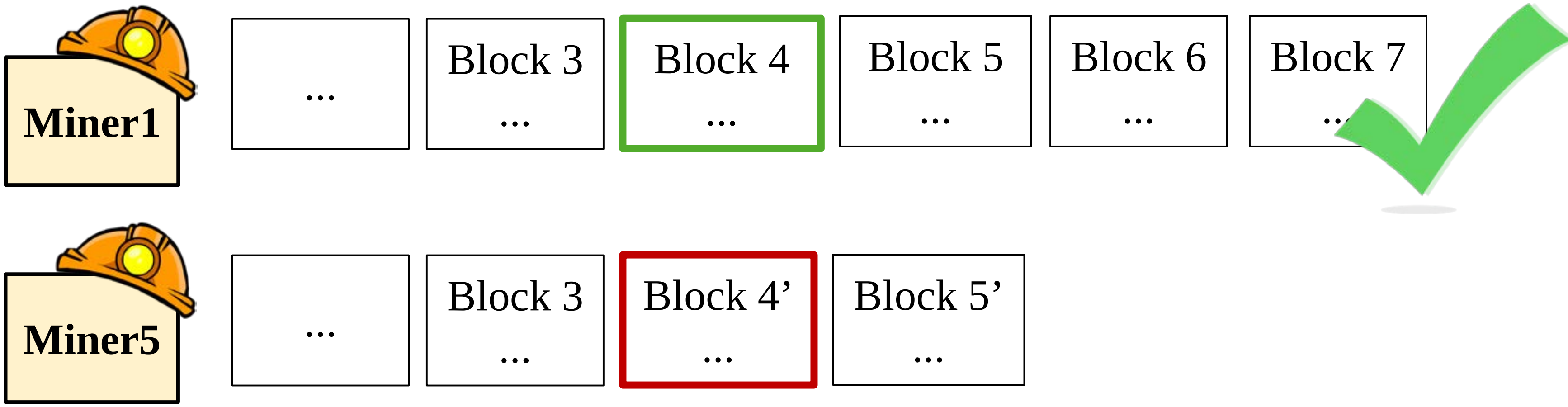
Block 2 …

Block 3 …

Block 4’ …

# Distributed consensus: Longest chain rule

- Two or more nodes may find a correct block simultaneously
  - a node that receives two or more new independent blocks will keep both blocks
    - The chain may temporarily have forks
  - it always works on (follow) a longer chain if there are multiple forks
    - Ties break arbitrarily
  - ~6 blocks ahead to confirm a transaction



Miner1

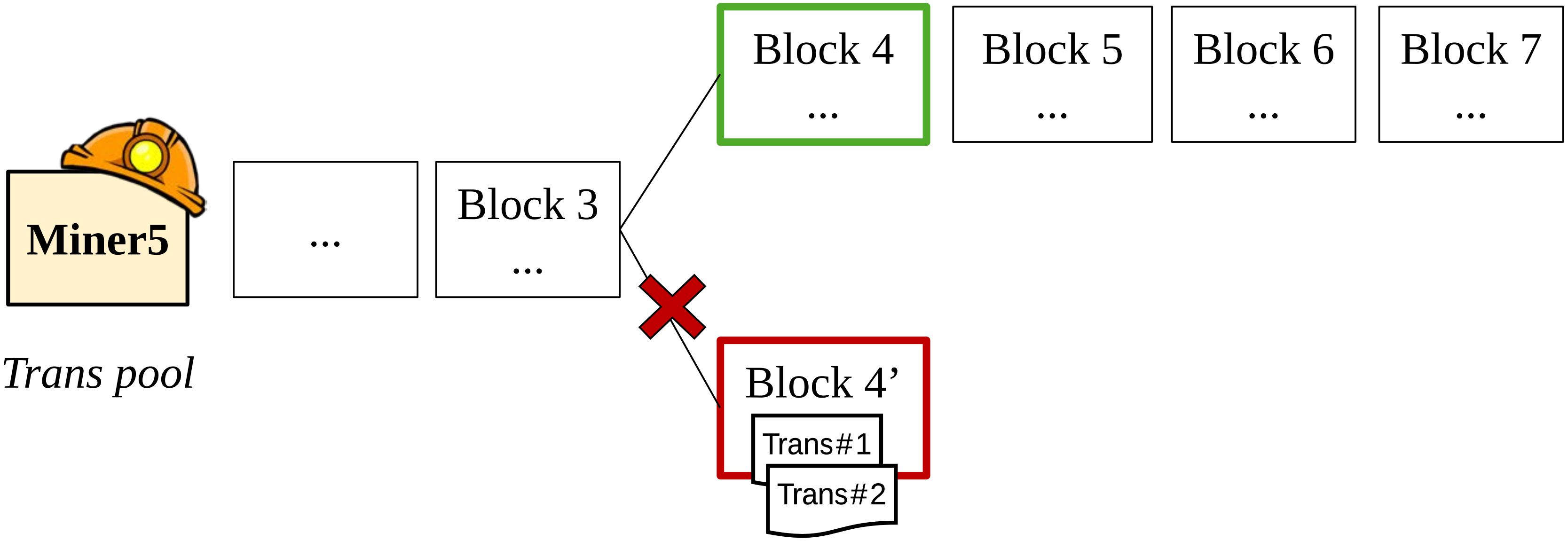
| … | Block 3 … | Block 4 … | Block 5 … | Block 6 … | Block 7 … |
|---|---|---|---|---|---|

Miner5

| … | Block 3 … | Block 4’ … | Block 5’ … |
|---|---|---|---|

# Convergence to the same chain

- With the longest chain rule, all nodes eventually agree on the same blockchain
- Transactions of shorter blocks are put back to the pool
- How to reverse a trans that was already committed?
  - Do I see money credited to my account but later disappeared?

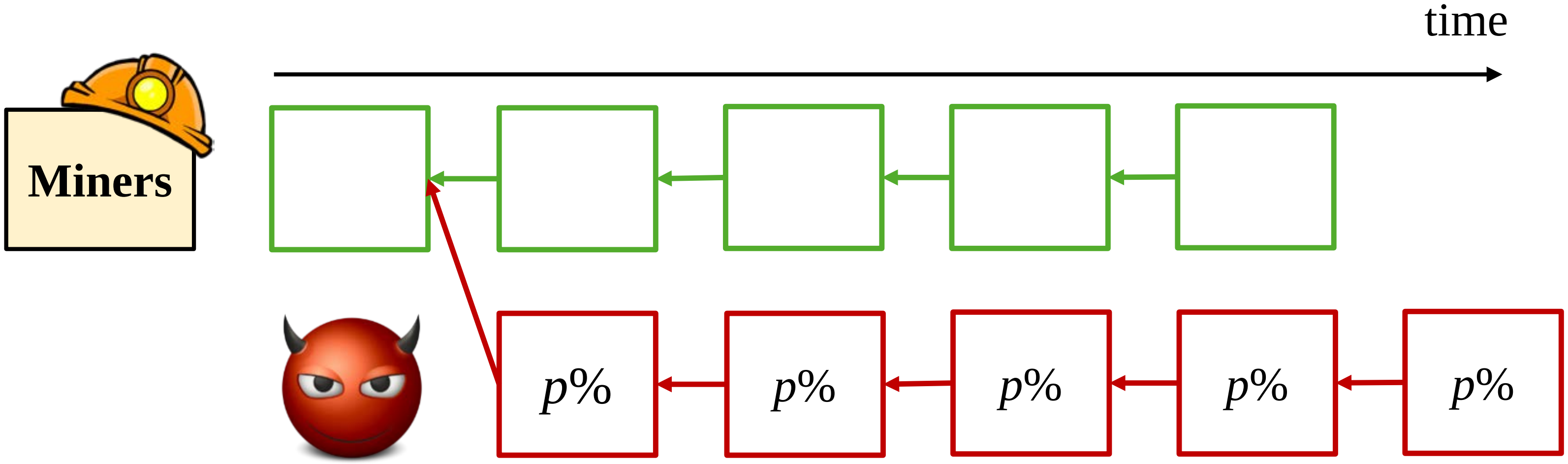


# When can a trans be confirmed in blockchain?

- There is no balance even written in the blockchain
  - The ledger is recorded as the history of transactions
  - When the trans of a lost block falls back to the pool, those trans are no longer in the chain
    - Fall-back trans take no effect, as if nothing happened
- When there are 6 (or more) new blocks grown after this trans, the trans can be regarded as “confirmed”
  - The funds in this transaction are then “committed”

# Impossible to fake a trans in blockchain

- Suppose a node made a fraud transaction and included in a block successfully
- This node has to continuously and successfully mine the next several blocks to make his faked block in the longest chain (even others can check out the fraud)
- But, the probability is very low:
  - suppose the node has *p*% of the total computing power…



# What happens if a miner finds a faked trans?

- It simply doesn’t follow the block for growing a new block
  - no reporting mechanism
  - note: no law-enforcement nor central-authority to catch the offenders in blockchain
- The owner of faked trans won’t be able to keep up with the pace to generate subsequent new blocks
  - the block containing faked trans will be eventually discarded and the faked trans will never take effect in blockchain
- The counter-fraud in blockchain relies on the PoW and is based on the fact: nobody controls over 50% of the total computing power in the world

# Why PoW is essential?

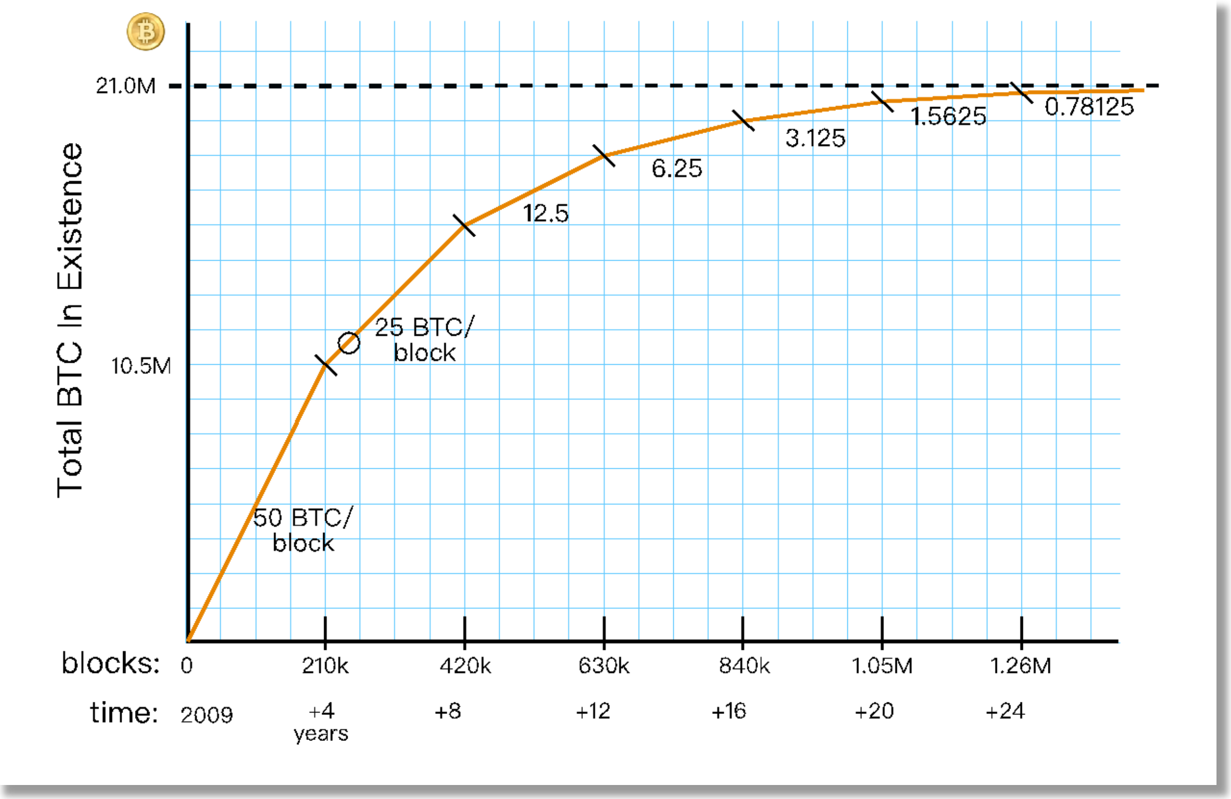
- Spread out the time of nodes competing for generating new blocks in a wider range and with higher randomness
  - The probability for two miners to generate new blocks simultaneously is slim
  - Longer time for PoW makes network delays insignificant in winning out the competition among nodes
- Security reason
  - Prevent Sybil attacks
- Is it possibly to develop a decentralized consensus protocol without using PoW?
  - BFT (Byzantine Fault Tolerance) protocol
  - Proof-of-Stake

# Incentives for miners

- Block Rewards:
  - creator of a new block gets to include a special *coinbase transaction* in the block
    - The creator (typically itself) can choose a recipient address of this trans
- Transaction Fees:
  - a transaction’s output value can be made less than the input value, leaving a transaction fee for the block creator
    - purely voluntary, like a tip
    - transaction fee becomes increasingly important, as block rewards start running out
- Where is Nakamoto’s said 1M coins coming from?

# Maximum number of coins

- Coins are only generated through block mining
- The block reward is cut in half every four years
- Originally, 50 BTC/block; but today, 12.5 BTC/block



# Total number of coins is capped by 21M

- The number of blocks per 4 year cycle:

  6 blocks per hour *
  24 hours per day *
  365 days per year *
  4 years per cycle = 210,240 ~= 210,000

- Sum the block rewards for all years …

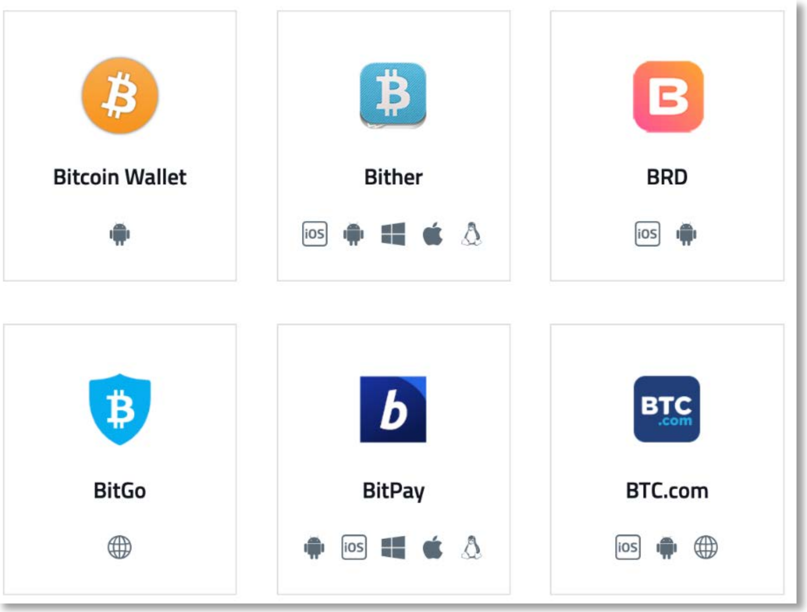
  210,000*(50 + 25 + 12.5 + 6.25 + 3.125 + ... )
  $210{,}000*50(1 + {}^{1}/_{2} + {}^{1}/_{4} + {}^{1}/_{8} + \ldots)$
  210,000*50*2 = 21 million

# Throughput of transactions

- Average time between blocks ≈ 10 minutes
  - nodes automatically re-calculate the difficulty of PoW every 2016 blocks (about every two weeks)
  - adjust difficulty to meet 10-minute goal
- Blocksize is limited to 1M bytes/block
  - at least 250 bytes/trans
  - ~3,500 – 4,000 trans/block
  - ~7 trans/s
- Compare to VISA (2,000-10,000 trans/s), and PayPal (50-100 trans/s)
- How to increase the throughput of Bitcoin?

# Bitcoin wallets

- You don’t need to mine or run a full node to use Bitcoin
- Wallet are applications that permit easy management of Bitcoins
- Bitcoin wallet stores, protects, and allows use of *private key* to make transactions



Bitcoin Wallet

Bither

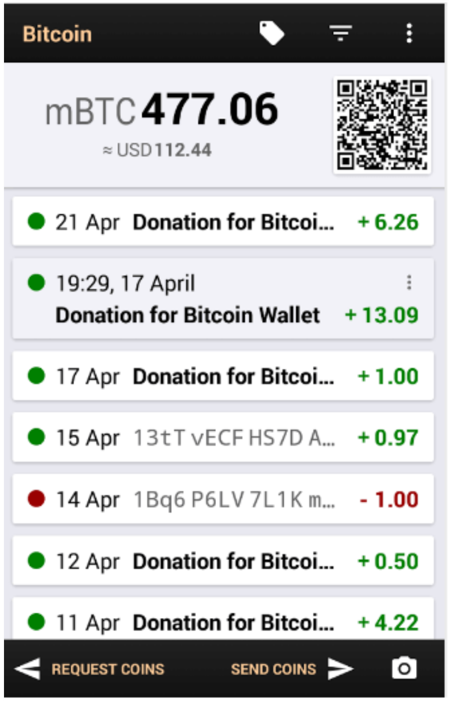
BRD

BitGo

BitPay

BTC.com

https://bitcoin.org/en/choose-your-wallet

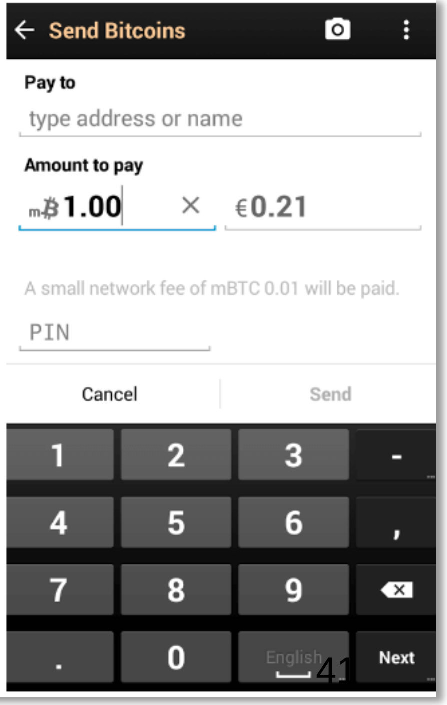


Bitcoin

mBTC 477.06

≈ USD 112.44

| | | |
|---|---|---|
| 21 Apr | Donation for Bitcoi... | + 6.26 |
| 19:29, 17 April<br>Donation for Bitcoin Wallet | | + 13.09 |
| 17 Apr | Donation for Bitcoi... | + 1.00 |
| 15 Apr | 13tT vECF HS7D A... | + 0.97 |
| 14 Apr | 1Bq6 P6LV 7L1K m... | - 1.00 |
| 12 Apr | Donation for Bitcoi... | + 0.50 |
| 11 Apr | Donation for Bitcoi... | + 4.22 |



Send Bitcoins

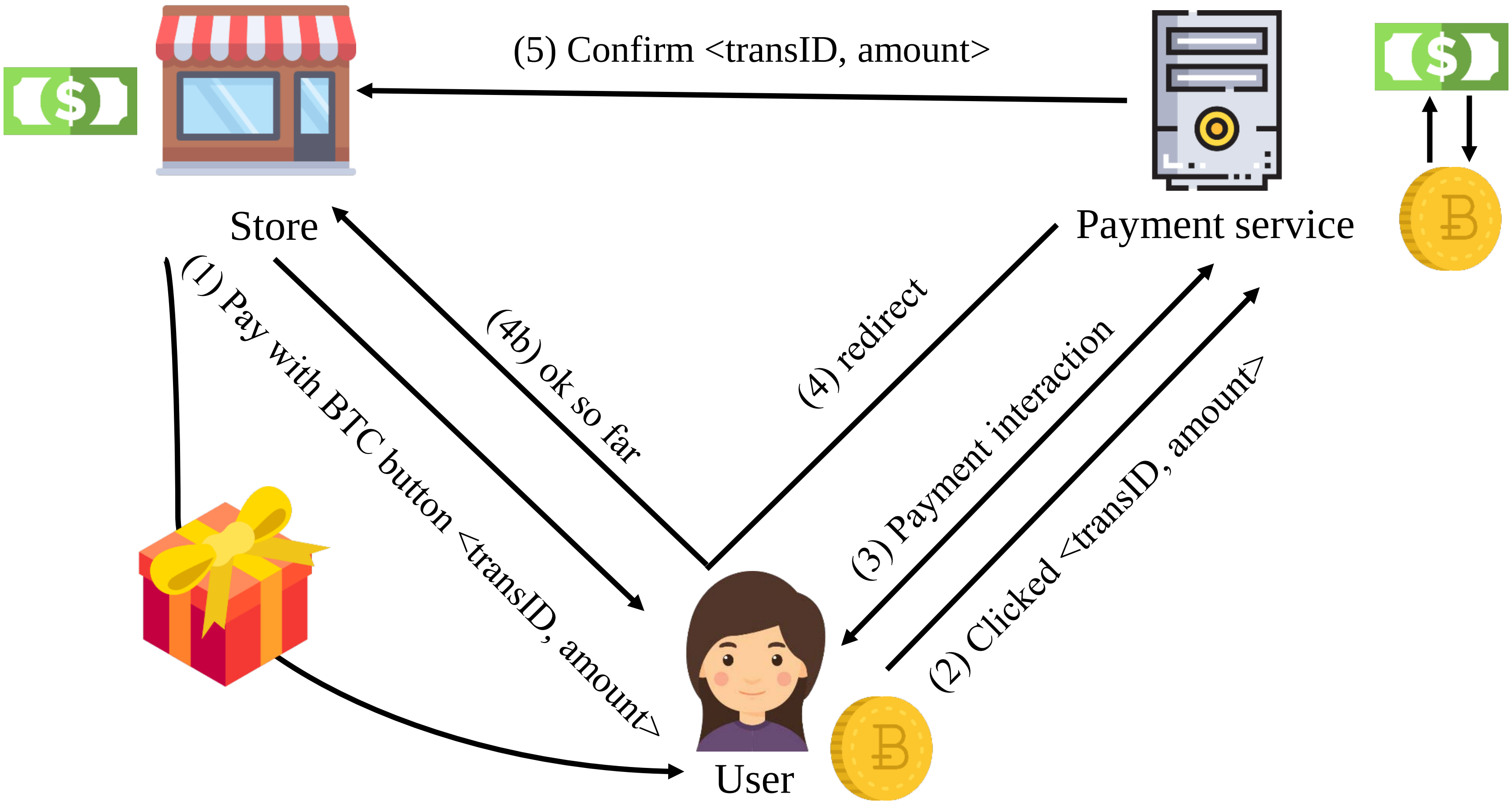
Pay to: type address or name

Amount to pay: m฿ 1.00 €0.21

A small network fee of mBTC 0.01 will be paid.

PIN

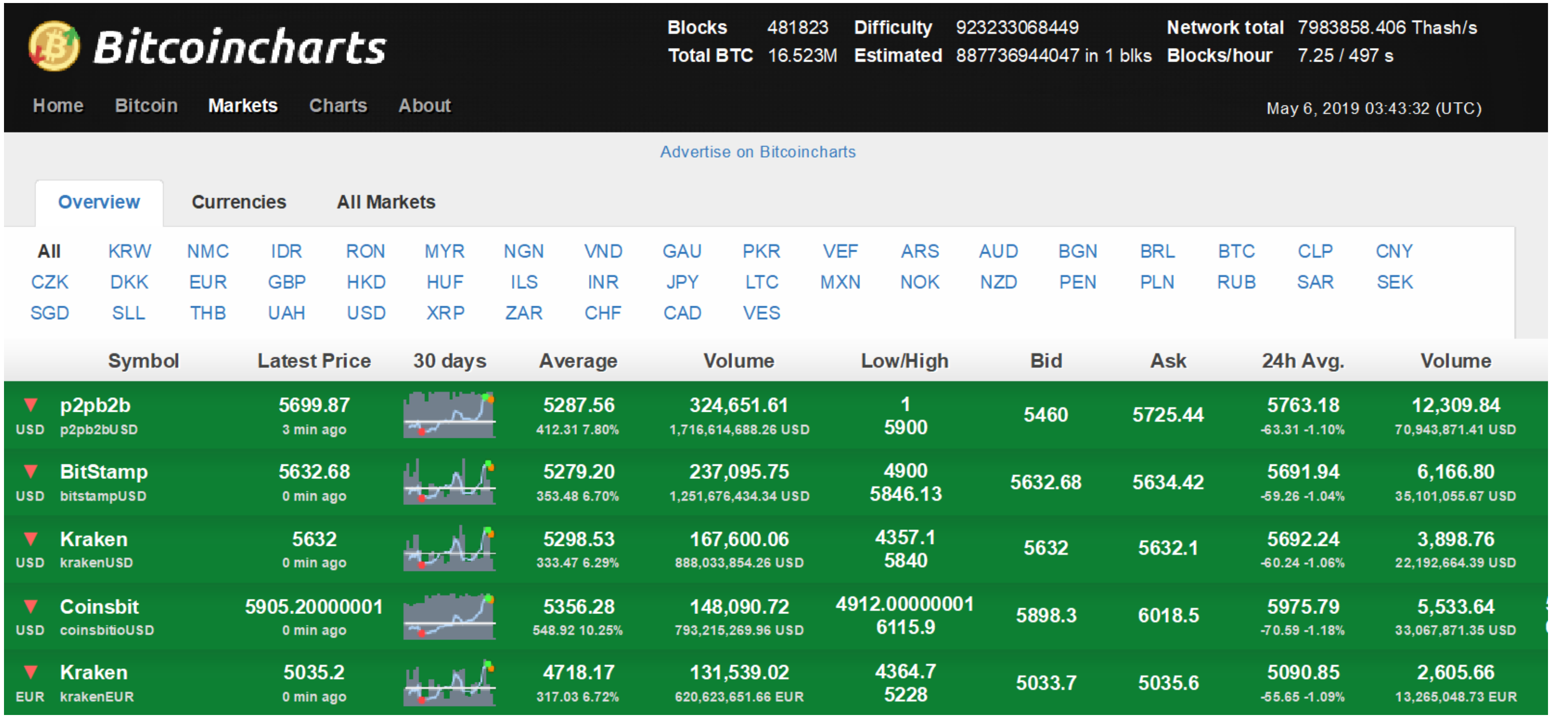
# Bitcoin payment



(5) Confirm <transID, amount>
Store
Payment service
(1) Pay with BTC button <transID, amount>
(4b) ok so far
(4) redirect
(3) Payment interaction
(2) Clicked <transID, amount>
User

# Bitcoin exchange

- There are sites like *bitcoincharts.com* that show the exchange rate with various currencies
- Another option is to meet people to trade bitcoins in real life, such as *localbitcoins.com*



Bitcoincharts

Blocks 481823 Difficulty 923233068449 Network total 7983858.406 Thash/s
Total BTC 16.523M Estimated 887736944047 in 1 blks Blocks/hour 7.25 / 497 s

May 6, 2019 03:43:32 (UTC)

Advertise on Bitcoincharts

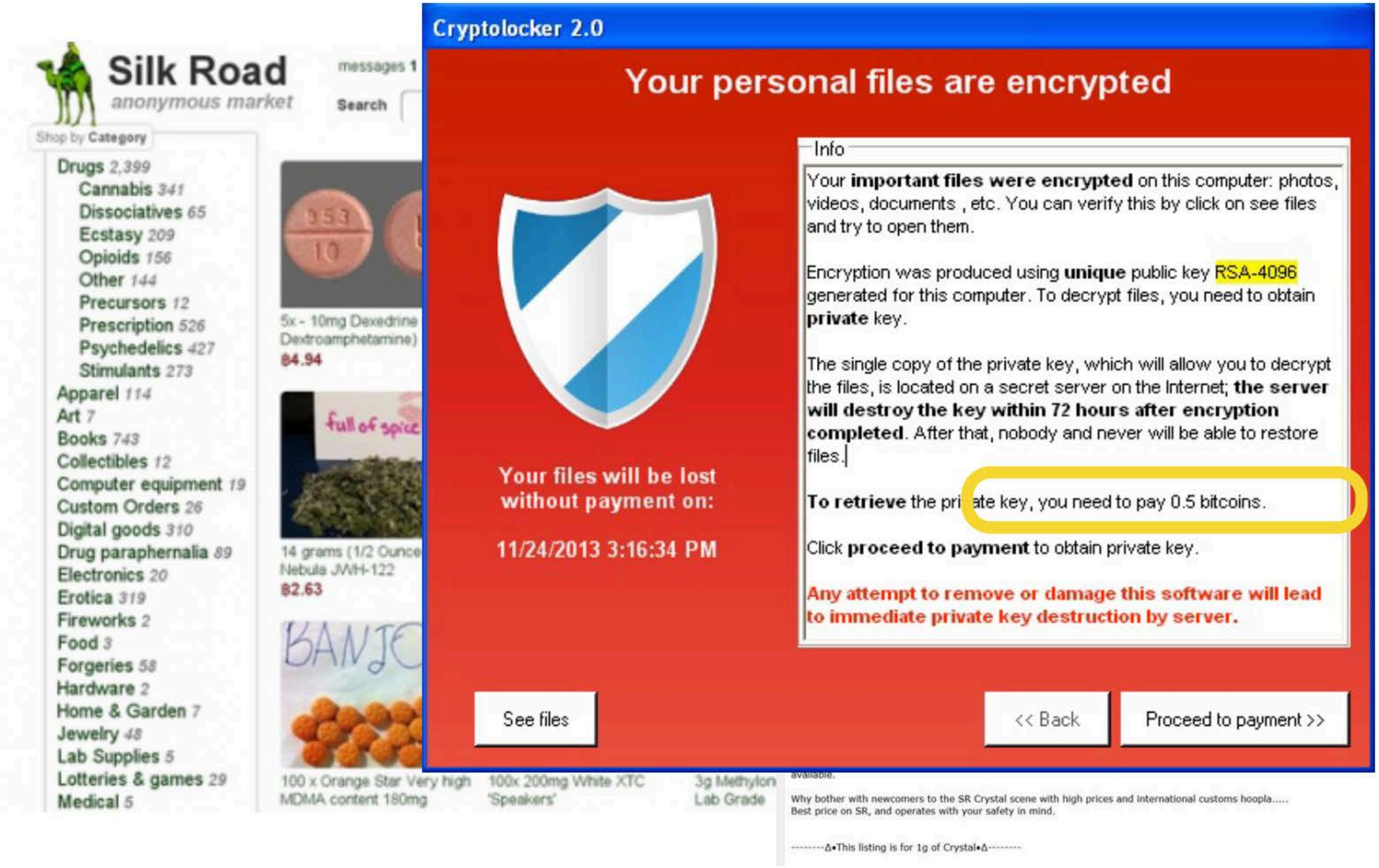
All KRW NMC IDR RON MYR NGN VND GAU PKR VEF ARS AUD BGN BRL BTC CLP CNY
CZK DKK EUR GBP HKD HUF ILS INR JPY LTC MXN NOK NZD PEN PLN RUB SAR SEK
SGD SLL THB UAH USD XRP ZAR CHF CAD VES

| | Symbol | Latest Price | 30 days | Average | Volume | Low/High | Bid | Ask | 24h Avg. | Volume |
|---|---|---|---|---|---|---|---|---|---|---|
| ▼<br>USD | p2pb2b<br>p2pb2bUSD | 5699.87<br>3 min ago | | 5287.56<br>412.31 7.80% | 324,651.61<br>1,716,614,688.26 USD | 1<br>5900 | 5460 | 5725.44 | 5763.18<br>-63.31 -1.10% | 12,309.84<br>70,943,871.41 USD |
| ▼<br>USD | BitStamp<br>bitstampUSD | 5632.68<br>0 min ago | | 5279.20<br>353.48 6.70% | 237,095.75<br>1,251,676,434.34 USD | 4900<br>5846.13 | 5632.68 | 5634.42 | 5691.94<br>-59.26 -1.04% | 6,166.80<br>35,101,055.67 USD |
| ▼<br>USD | Kraken<br>krakenUSD | 5632<br>0 min ago | | 5298.53<br>333.47 6.29% | 167,600.06<br>888,033,854.26 USD | 4357.1<br>5840 | 5632 | 5632.1 | 5692.24<br>-60.24 -1.06% | 3,898.76<br>22,192,664.39 USD |
| ▼<br>USD | Coinsbit<br>coinsbitioUSD | 5905.20000001<br>0 min ago | | 5356.28<br>548.92 10.25% | 148,090.72<br>793,215,269.96 USD | 4912.00000001<br>6115.9 | 5898.3 | 6018.5 | 5975.79<br>-70.59 -1.18% | 5,533.64<br>33,067,871.35 USD |
| ▼<br>EUR | Kraken<br>krakenEUR | 5035.2<br>0 min ago | | 4718.17<br>317.03 6.72% | 131,539.02<br>620,623,651.66 EUR | 4364.7<br>5228 | 5033.7 | 5035.6 | 5090.85<br>-55.65 -1.09% | 2,605.66<br>13,265,048.73 EUR |

# Bitcoin’s dark side

- Bitcoin has stimulated
  - Money laundering
  - Illegal marketplaces and dark web (e.g., Silk Road)
  - Ransomware
  - Theft of Bitcoin wallets
  - Rogue mining
    - E.g., ZeroAccess botnet

# Bitcoin’s dark side



Silk Road

anonymous market

- Drugs 2,399
  - Cannabis 341
  - Dissociatives 65
  - Ecstasy 209
  - Opioids 156
  - Other 144
  - Precursors 12
  - Prescription 526
  - Psychedelics 427
  - Stimulants 273
- Apparel 114
- Art 7
- Books 743
- Collectibles 12
- Computer equipment 19
- Custom Orders 26
- Digital goods 310
- Drug paraphernalia 89
- Electronics 20
- Erotica 319
- Fireworks 2
- Food 3
- Forgeries 58
- Hardware 2
- Home & Garden 7
- Jewelry 48
- Lab Supplies 5
- Lotteries & games 29
- Medical 5

5x - 10mg Dexedrine Dextroamphetamine)
฿4.94

14 grams (1/2 Ounce Nebula JWH-122
฿2.63

100 x Orange Star Very high MDMA content 180mg

100x 200mg White XTC 'Speakers'

3g Methylon Lab Grade

available.

Why bother with newcomers to the SR Crystal scene with high prices and international customs hoopla..... Best price on SR, and operates with your safety in mind.

--------Δ•This listing is for 1g of Crystal•Δ--------

Cryptolocker 2.0

Your personal files are encrypted

Your files will be lost without payment on:

11/24/2013 3:16:34 PM

Info

Your **important files were encrypted** on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.

**To retrieve** the private key, you need to pay 0.5 bitcoins.

Click **proceed to payment** to obtain private key.

**Any attempt to remove or damage this software will lead to immediate private key destruction by server.**

**Tor + Bitcoin = End-to-end anonymity for commercial transactions**

# Summary

- Bitcoin is a native application of blockchain technology
- The blockchain is maintained by a P2P network
  - each transaction is broadcast to the P2P network
  - miners verify transactions and generate new blocks to link to the chain
- The P2P network maintains the consistency of the blockchain via the longest chain rule
  - distributed consensus is enforced via PoW
- Blockchain technology can be applied to P2P environment where there is no central authority and no trust among the peers
  - Financial/banking sectors, insurance services, real-estate transactions, medical data sharing, etc

# References

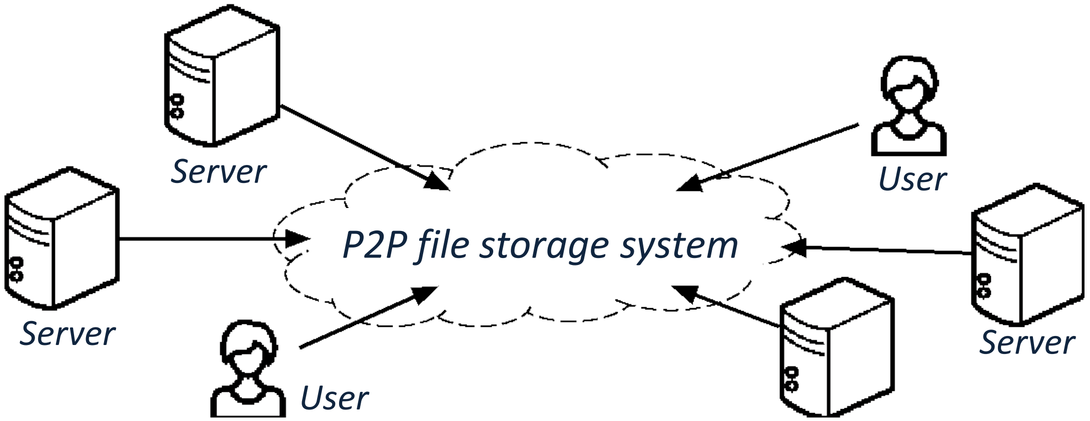
- Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan , Joshua A. Kroll, and Edward W. Felten. “SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies”, in Proc. of IEEE S&P 2015.
- Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. “Bitcoin and Cryptocurrency Technologies”, in Princeton University Press, 2016
- Satoshi Nakamoto. “Bitcoin: A PeertoPeer Electronic Cash System”
- Bitcoin Wiki, online at https://en.bitcoin.it/wiki/Main_Page
- Maurice Herlihy. “Blockchains from a Distributed Computing Perspective ”, 2018

# Exercises

1) Why is it impossible to make a fraud transaction in blockchain?
2) PoW costs a massive amount of resources. Why is it essential in blockchain? Can you replace the PoW by a protocol without heavy computational cost?
3) Why the max number of Bitcoins is capped by 21M?
4) The throughput current bitcoin system is around 7 trans/s, too small. Think about some ways to increase the throughput of bitcoin transactions, and discuss their pros and cons.
5) Think about an application that can use blockchain technology.

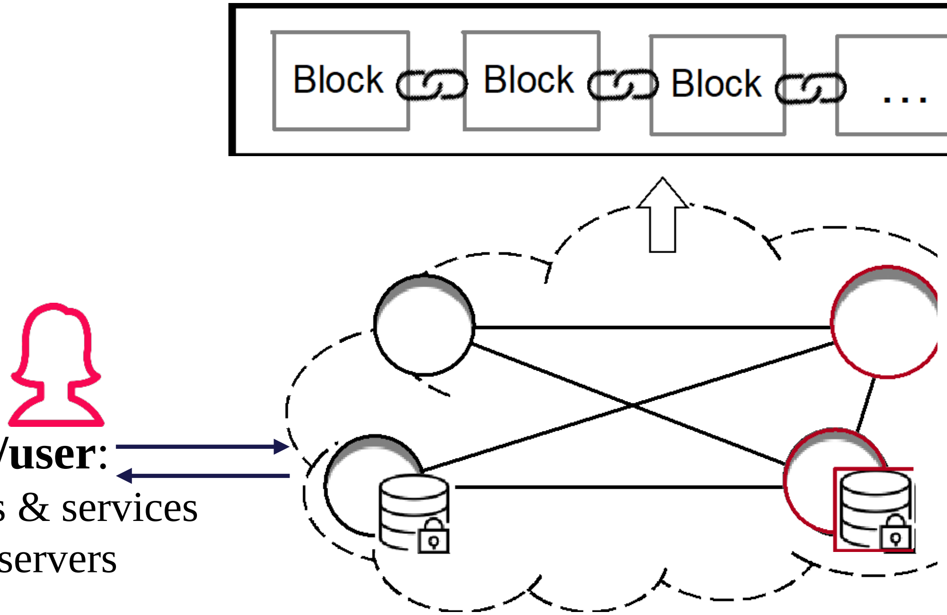
# Case Study: a P2P storage system using blockchain

- Explosive growth of digital data
  - fuelled up by e-health, e-commerce, smart cities, IoT, …
- Mismatch between supply and demand of data storage
  - a vast amount of under-used storages scattered all over the world
  - high demand from users looking for storage space
- P2P storage system:
  - utilize the unused storage space to form a huge global storage system



# Framework of blockchain-based P2P storage system

- P2P storage system



**Data owner/user**: outsource files & services to the storage servers

**Blockchain peers:** verify the correctness of transactions and generate new blocks

**Storage servers:** lease out computing/storage resources to users

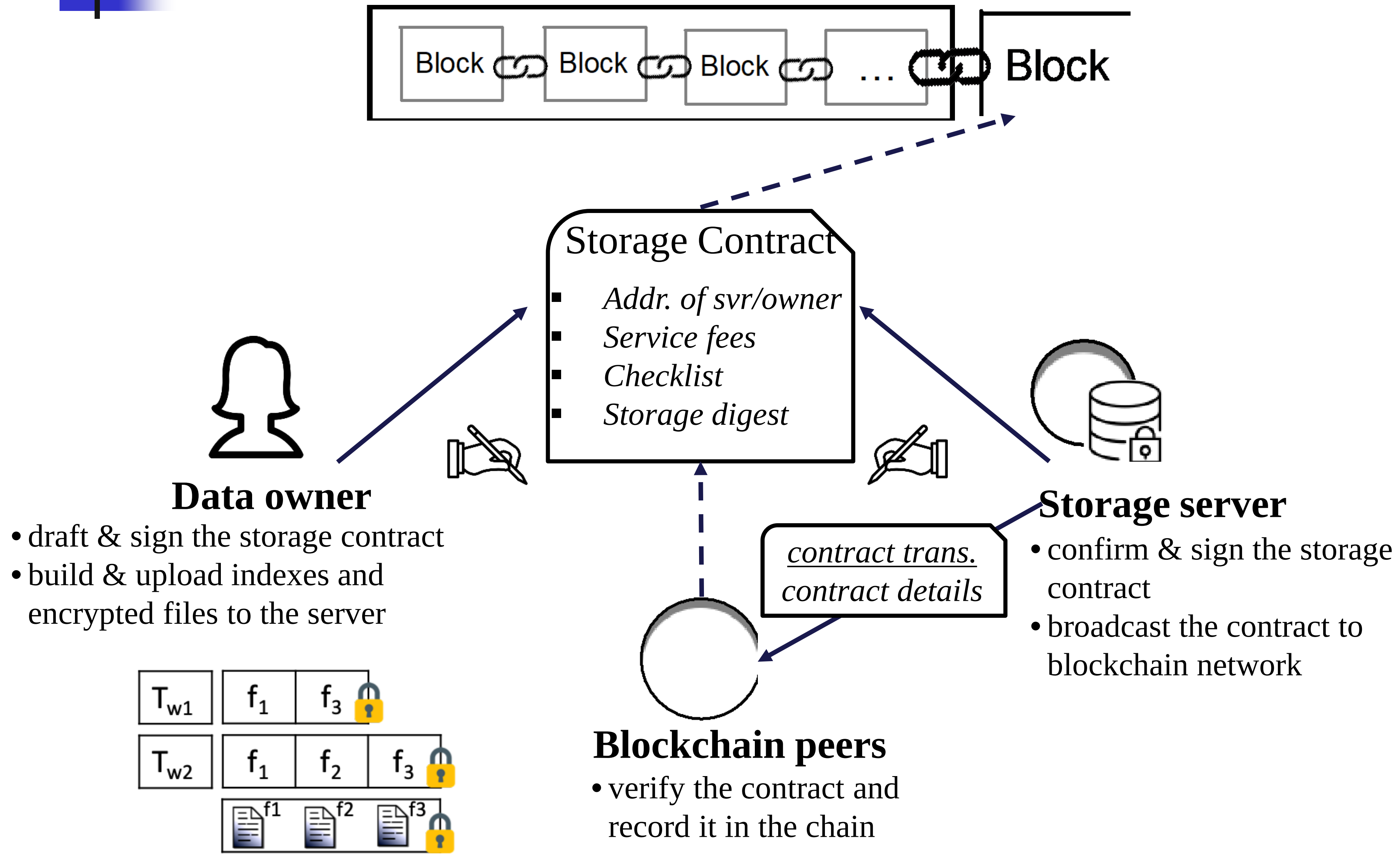
**P2P storage network**

**A secure and fair platform for people to lease computing resources and for users to receive services**

# Framework of a blockchain-based P2P storage system

- Blockchain P2P network consists of storage servers and peers
  - storage servers can be peers
- Data owners/users interact with storage servers via transactions
  - data owners bind with servers via smart contracts
  - data and search indexes are stored off-chain at storage servers
  - all operations between owner/user and server are via transactions
    - contract transactions, data search/update transactions, etc
- Peers verify correctness of transactions and generate new blocks to the blockchain

# Signing a storage contract



Storage Contract

- *Addr. of svr/owner*
- *Service fees*
- *Checklist*
- *Storage digest*

*contract trans.*

*contract details*

**Data owner**

- draft & sign the storage contract
- build & upload indexes and encrypted files to the server

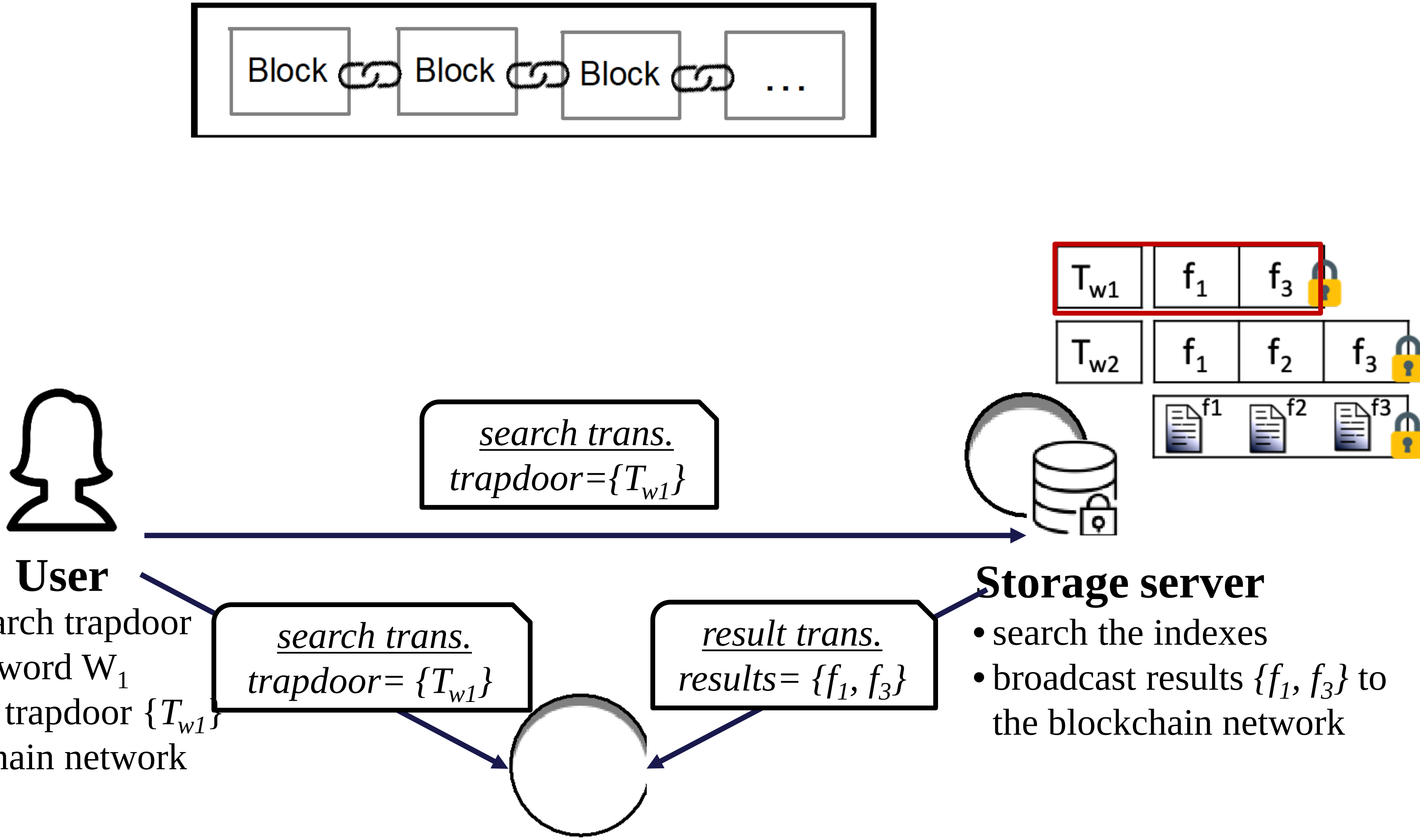
**Storage server**

- confirm & sign the storage contract
- broadcast the contract to blockchain network

**Blockchain peers**

- verify the contract and record it in the chain

# Search transaction



*search trans.*
*trapdoor=*$\{T_{w1}\}$

**User**

- generate a search trapdoor $\{T_{w1}\}$ for keyword $W_1$
- broadcast the trapdoor $\{T_{w1}\}$ to the blockchain network

*search trans.*
*trapdoor=* $\{T_{w1}\}$

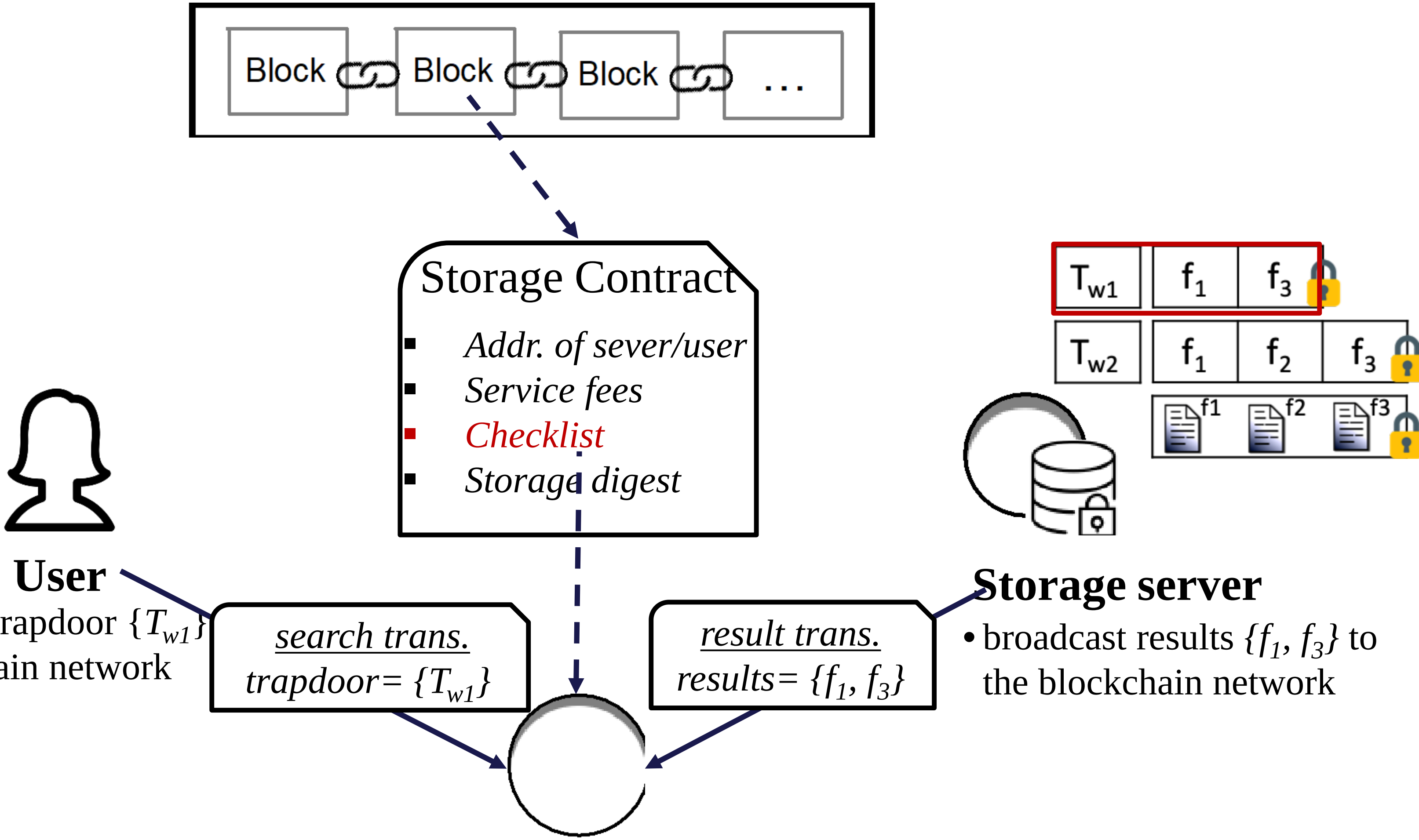
*result trans.*
*results=* $\{f_1, f_3\}$

**Storage server**

- search the indexes
- broadcast results $\{f_1, f_3\}$ to the blockchain network

**Blockchain peers**

# Search result verification



Storage Contract

- *Addr. of sever/user*
- *Service fees*
- *Checklist*
- *Storage digest*

*search trans.*
*trapdoor= $\{T_{w1}\}$*

*result trans.*
*results= $\{f_1, f_3\}$*

**User**

- broadcast the trapdoor $\{T_{w1}\}$ to the blockchain network

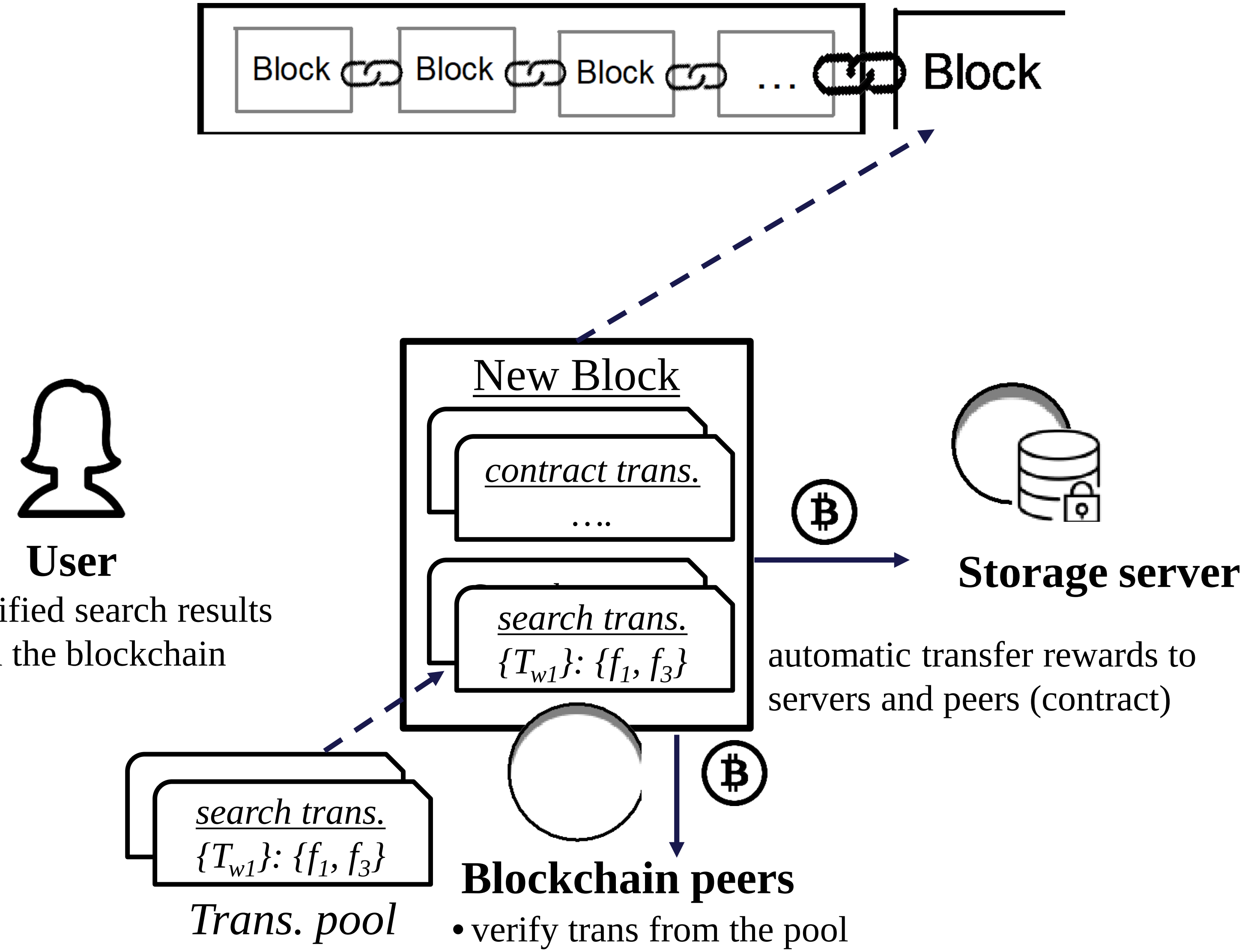
**Storage server**

- broadcast results $\{f_1, f_3\}$ to the blockchain network

**Blockchain peers**

- verify the results against the on-chain checklist

# Generating new blocks to the blockchain



**User**

retrieve verified search results $\{f_1, f_3\}$ from the blockchain

**Storage server**

automatic transfer rewards to servers and peers (contract)

**Blockchain peers**

- verify trans from the pool
- generate a new block to the chain

# A new consensus protocol

- Verification of a search result transaction includes:
  - verifying the search results, and
  - auditing the integrity of the stored file
- Peers compete with each other to generate new blocks

$$\boxed{\text{SHA-256}\text{\textasciicircum}2(\,pk \,||\, T \,||\, Mr(Tx) \,||\, H(\pi) \,||\, Block_{pre}\,) \overset{?}{<} Z \times B_{stc}}$$

*peer ID* *ticket* *transitions* *file-proofs* *Prev. block* *peer's stake*

$Mr(Tx)$: the Merkle-tree root of validated transactions in the new block

$H(\pi)$: the hash value of validated file-proofs

$B_{stc}$ : the peer's stake (amount of deposit it has in the system)

# A hybrid method of proof-of-stake and proof-of-work

- Proof-of-stake gives more advantage to peers with higher stake, reducing the average time for generating a new block
  - a trade-off between randomness and deterministic in block mining
  - increase the throughput of generating new blocks
- Peers perform data auditing as a useful PoW
- The longest chain rule still holds the global consensus among the peers