Bitcoin and Blockchain

Dr. Chen Zhang
Department of Computer Science
The Hang Seng University of Hong Kong

Bitcoin

- Bitcoin: a **decentralized** digital currency and a **peer-to-peer** payment system introduced in 2009 by an anonymous person or group of people using the pseudonym Satoshi Nakamoto. It is the first and most well-known **cryptocurrency**, based on **blockchain** technology.

data from https://www.blockchain.com/explorer/assets/btc

What is cryptocurrency?

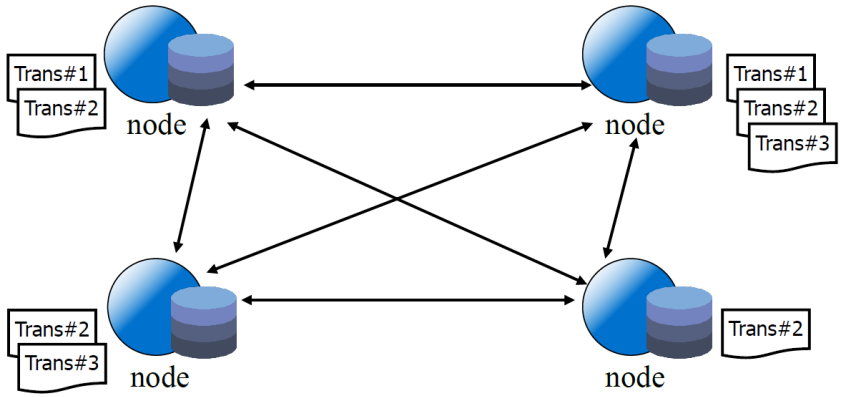
- A cryptocurrency is a digital currency, which is an alternative form of payment created using encryption algorithms.
- The use of encryption technologies means that cryptocurrencies function both as a currency and as a virtual accounting system.
- To use cryptocurrencies, you need a cryptocurrency wallet. These wallets can be software that is a cloud-based service or is stored on your computer or on your mobile device. The wallets are the tool through which you store your **encryption keys** that confirm your identity and link to your cryptocurrency.

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
- In bitcoin, the hash function and digital signature are widely used.

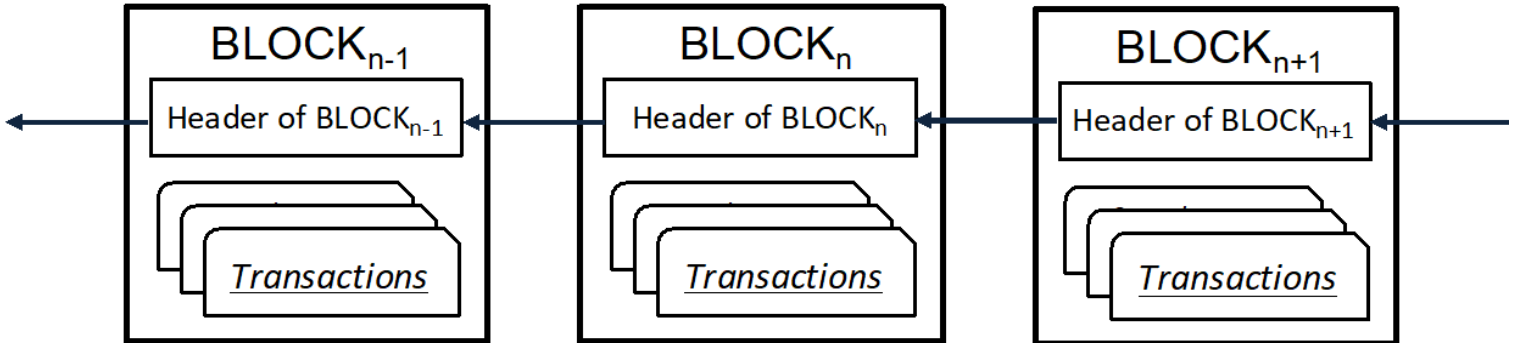
Blockchain – A Decentralized Ledger

- 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
- 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?



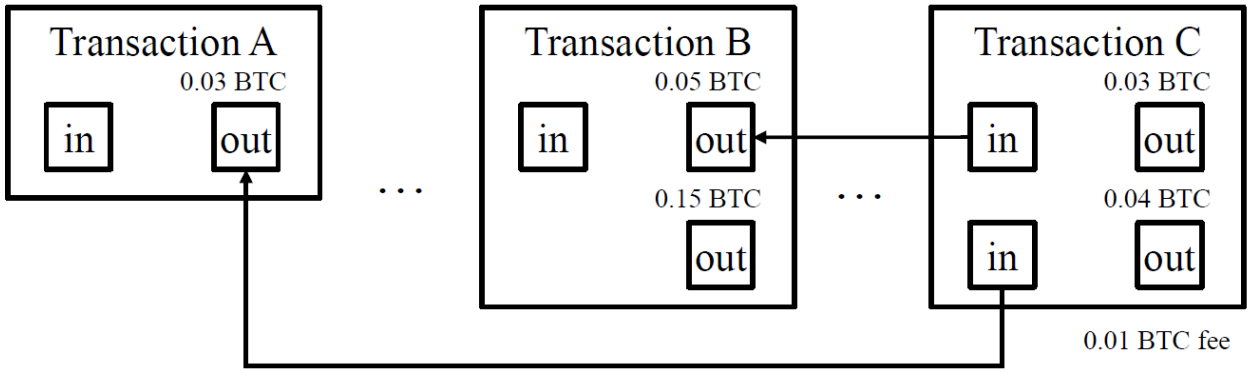
Blockchain and Transactions

- 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

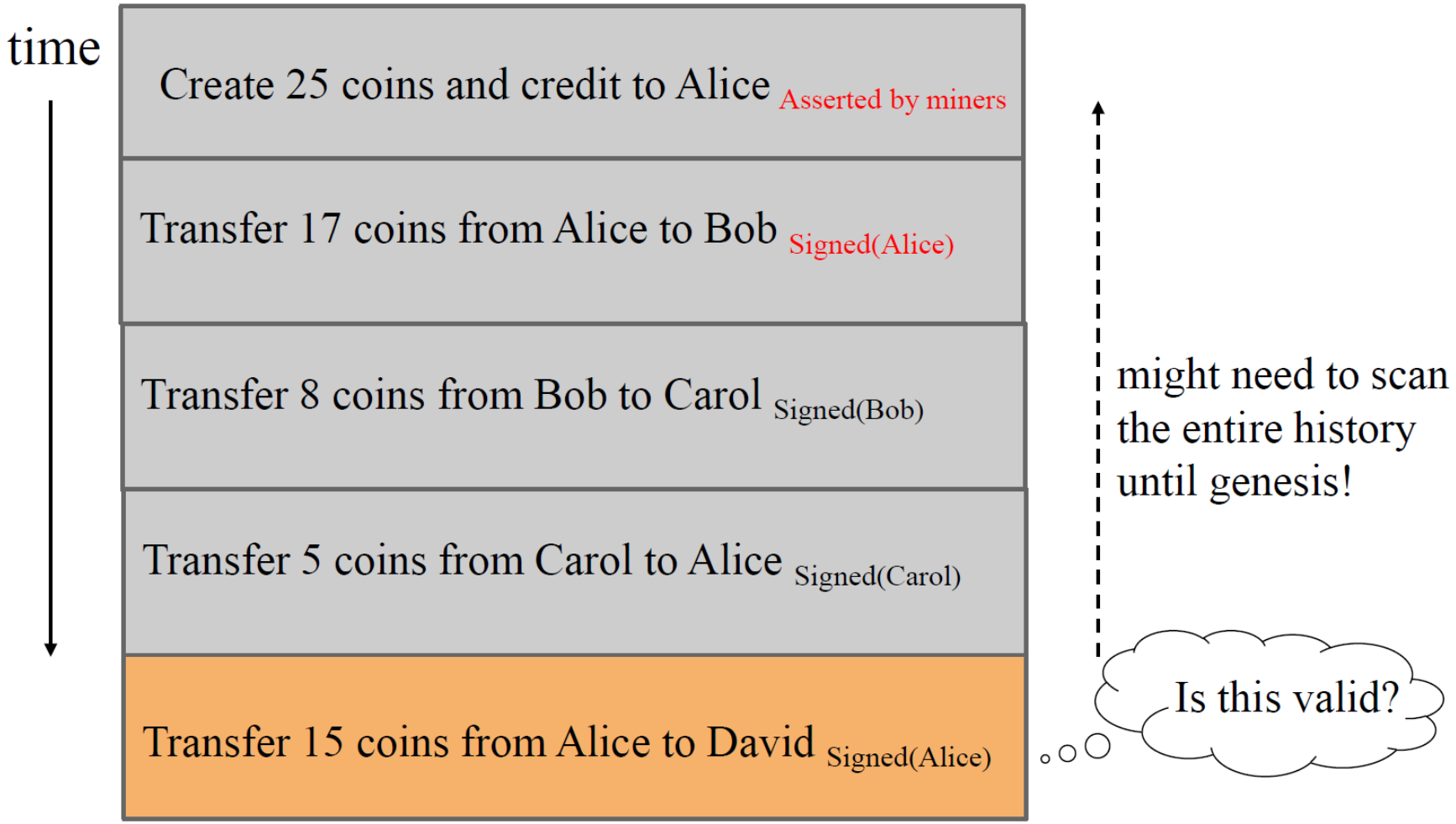


Full Transaction Chain: A Ledger

- 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"

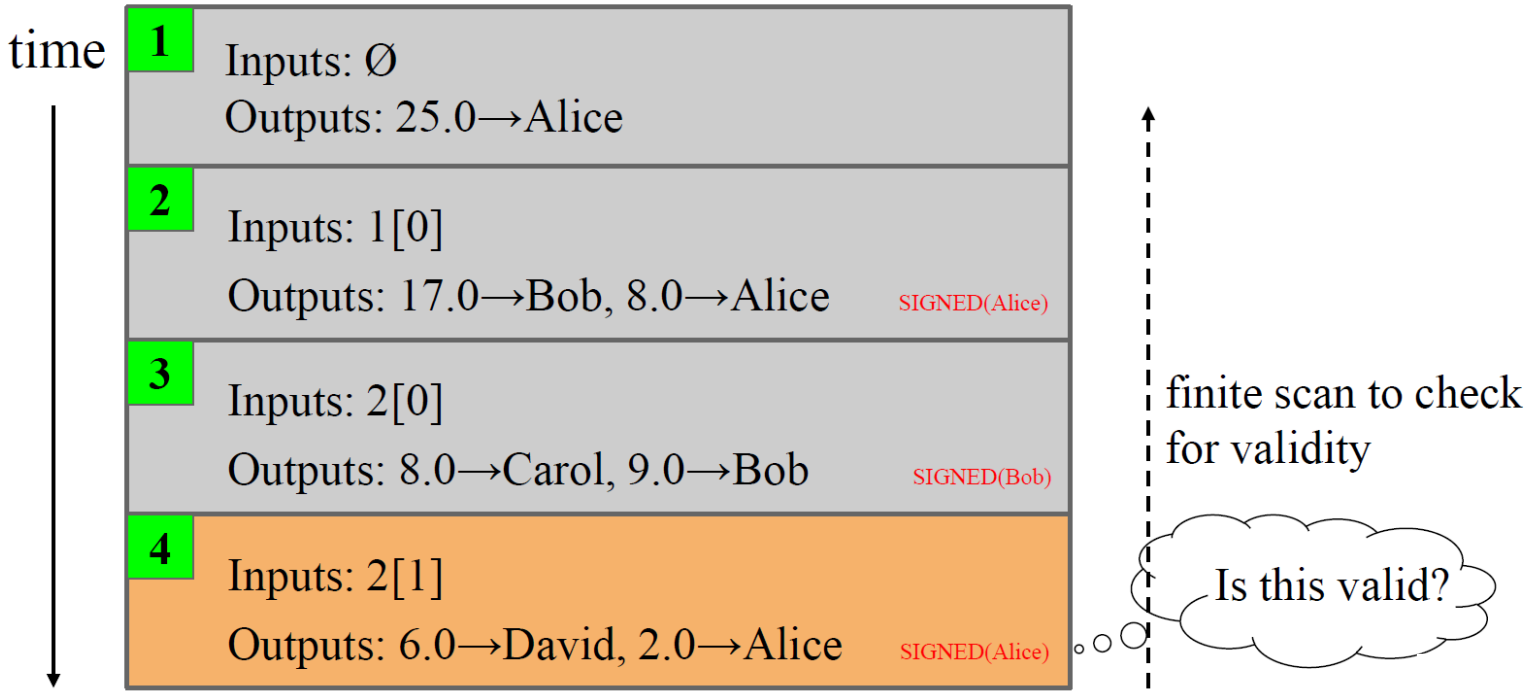


Trans-based Ledger: without in/out pointer

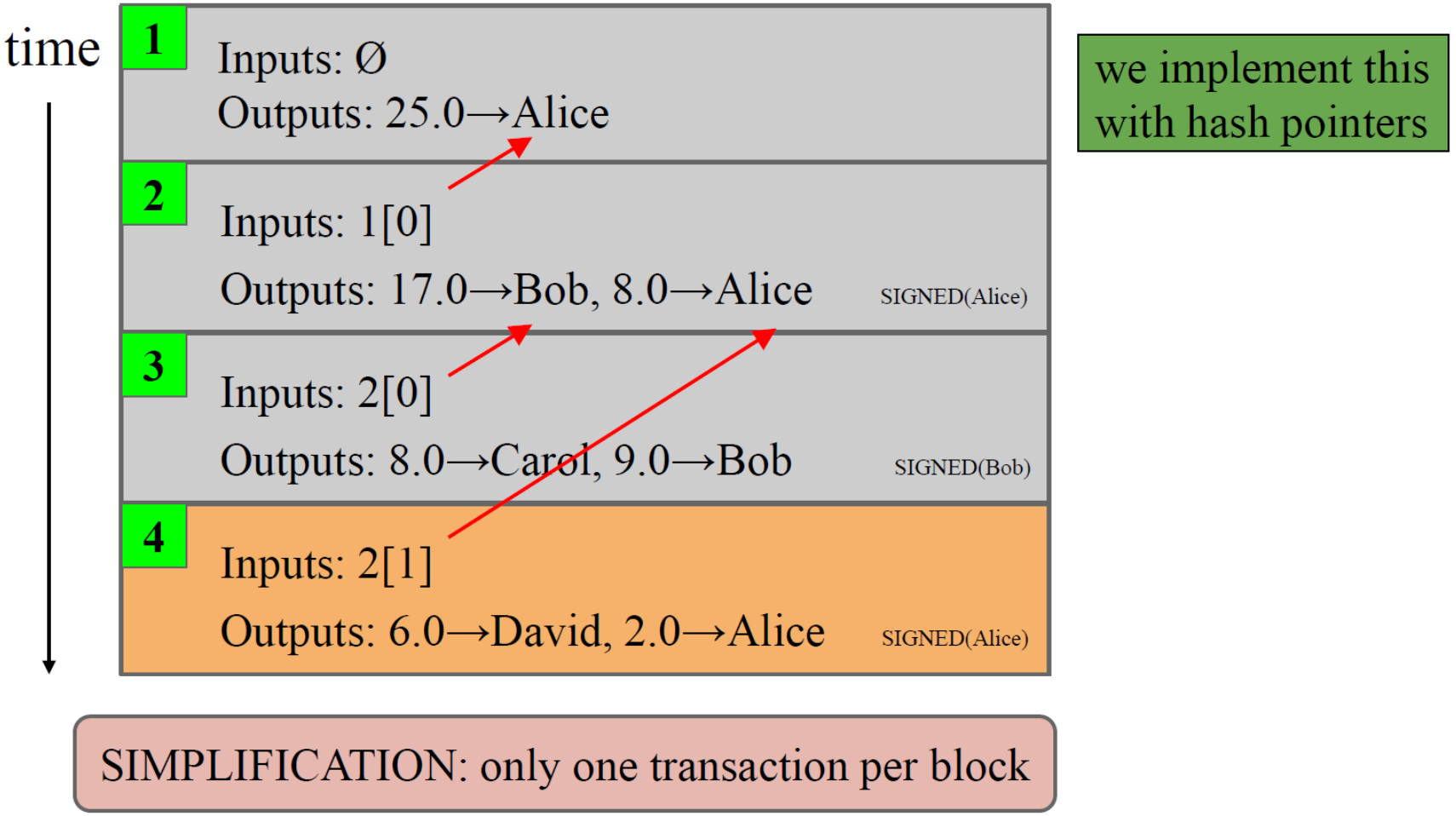


Trans-based Ledger: with in/out pointer (Bitcoin)

- 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?)

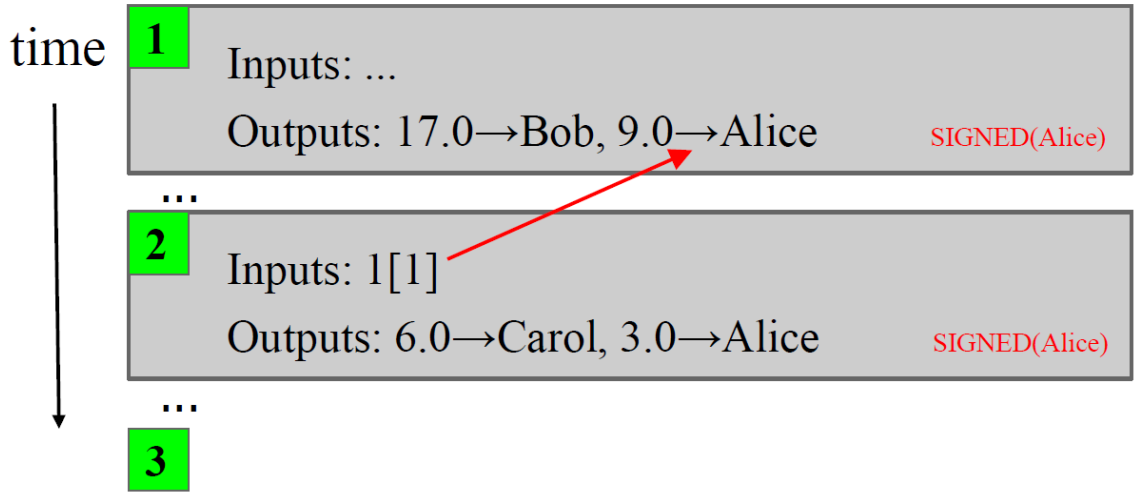


Input/Output Link of Transactions



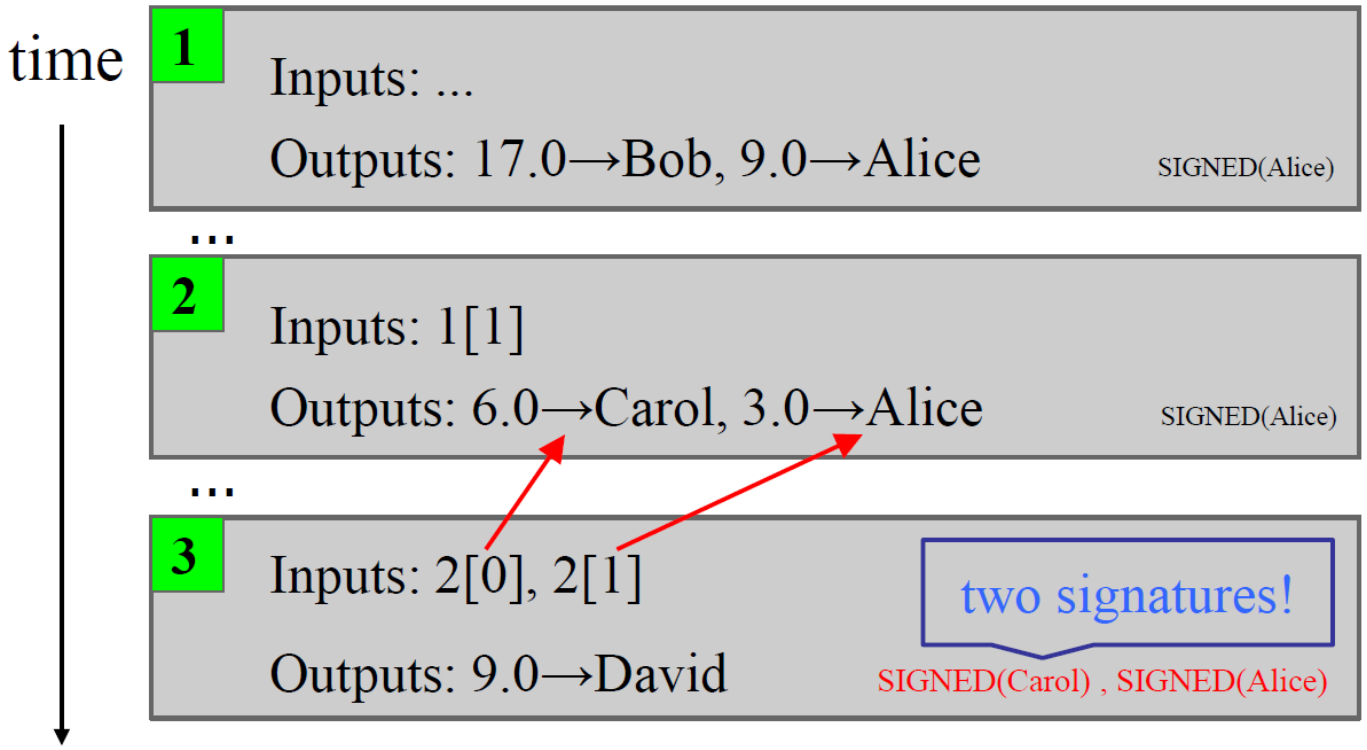
A Transaction with Change: Input Value > Transfer-Value

- 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



Joint Payment

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



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)
}
```

metadata

input(s)

output(s)

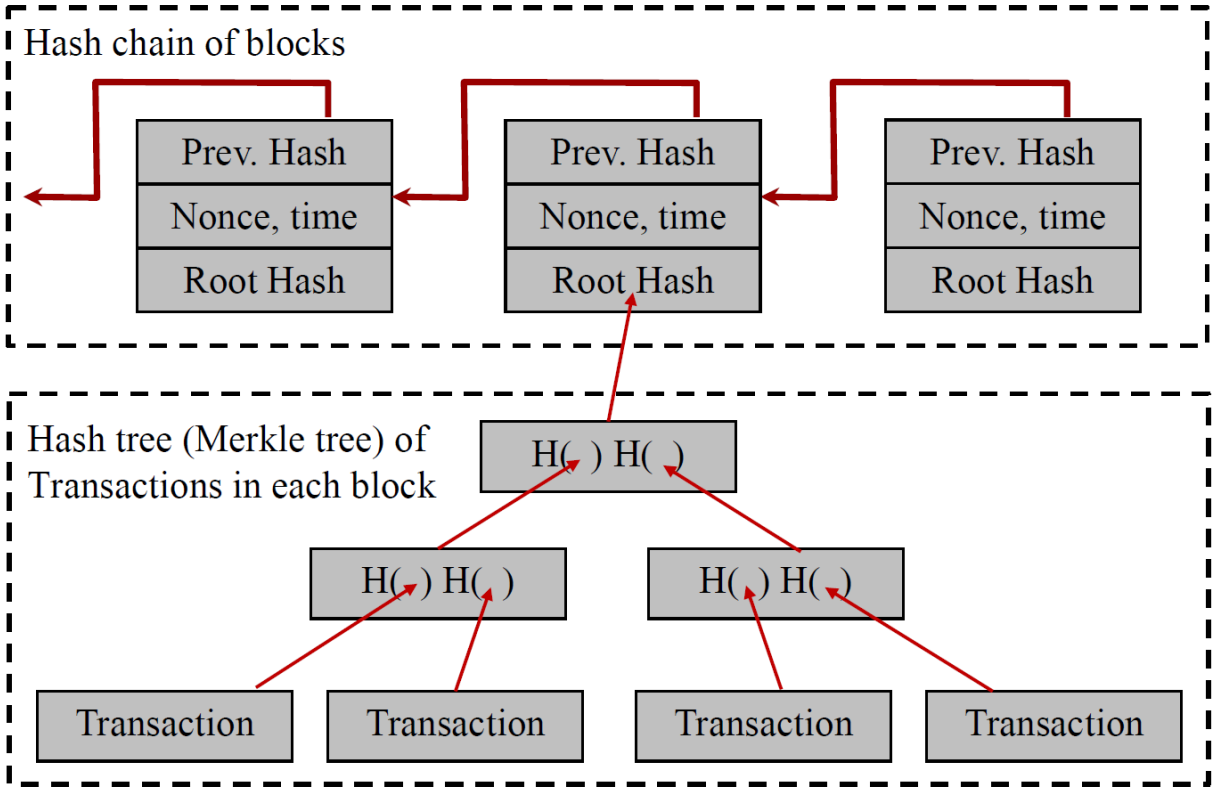
```
{
    "hash":"5a42590fbe0a90ee8e...b8b6b",
    …
    "size":404,
    "in":[
    {"prev_out":{      (null transID)
    "hash":"00000000000…000000",
    "n": 4294967295}
    "coinbase":"..."}  (arbitrary)
    ],
    "out":[
    {                          (block reward + trans fees)
    "value":"12.52287097",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

Coinbase transaction

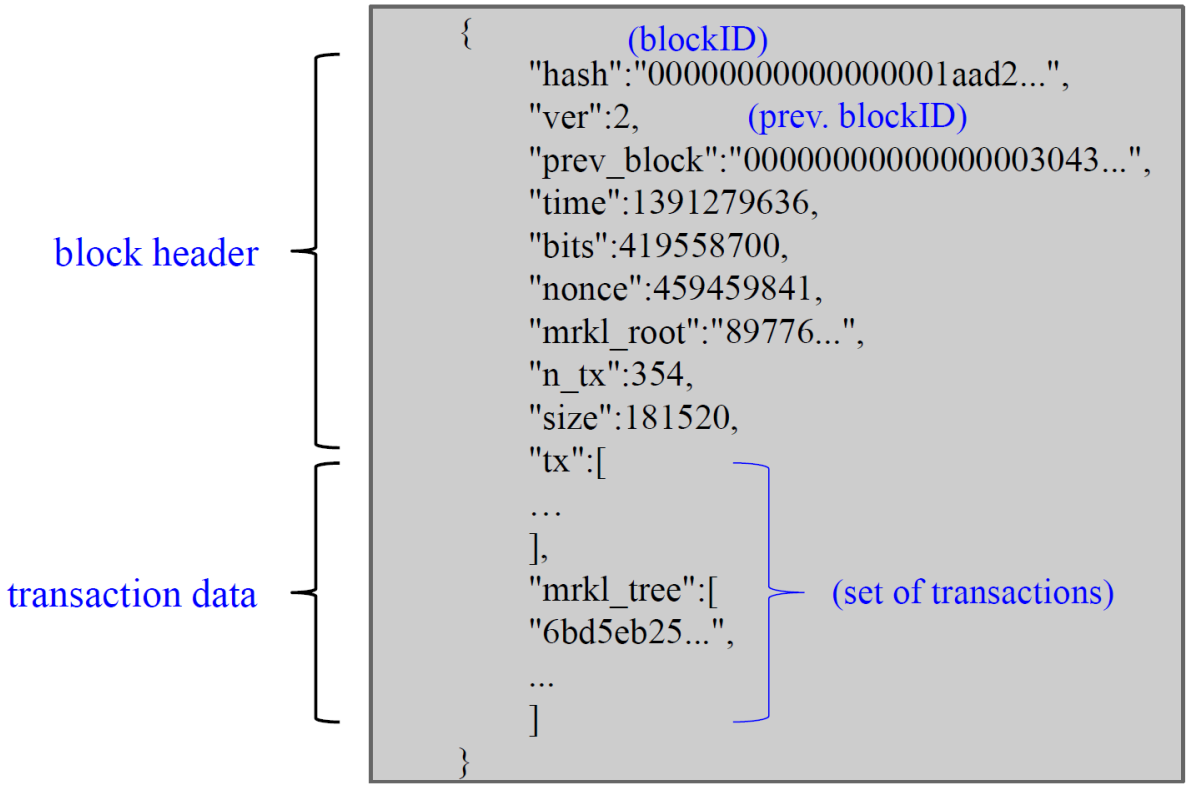
scriptSig (include the signature and public key) and scriptPubKey are used together to verify the effectiveness of the transactions.

Data Structure of Block: Chain of Blocks

- Each block contains a set of verified transactions



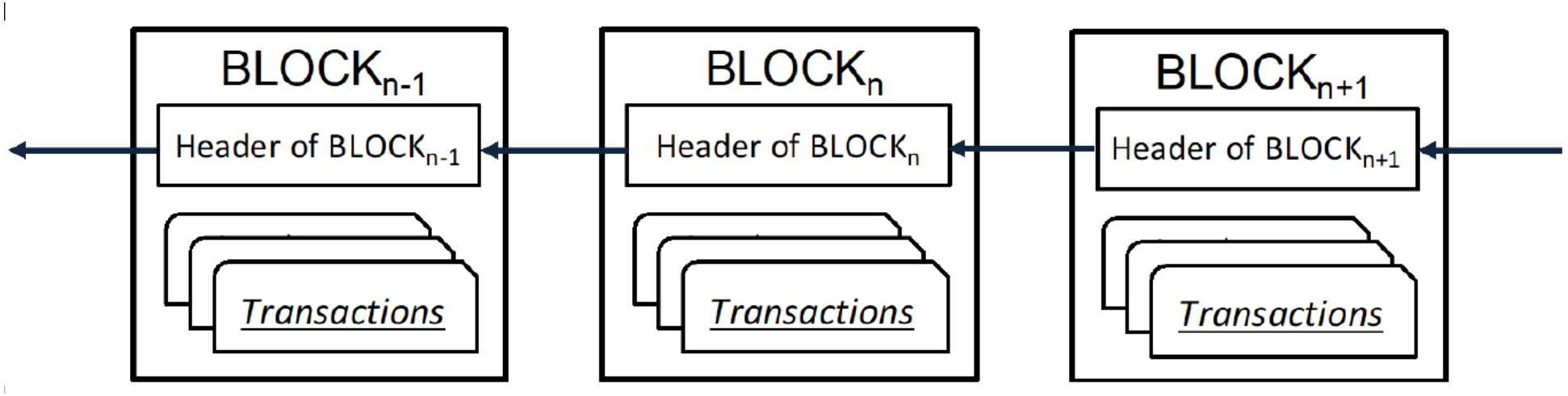
Merkel tree is a type of binary tree



Bitcoin block syntax

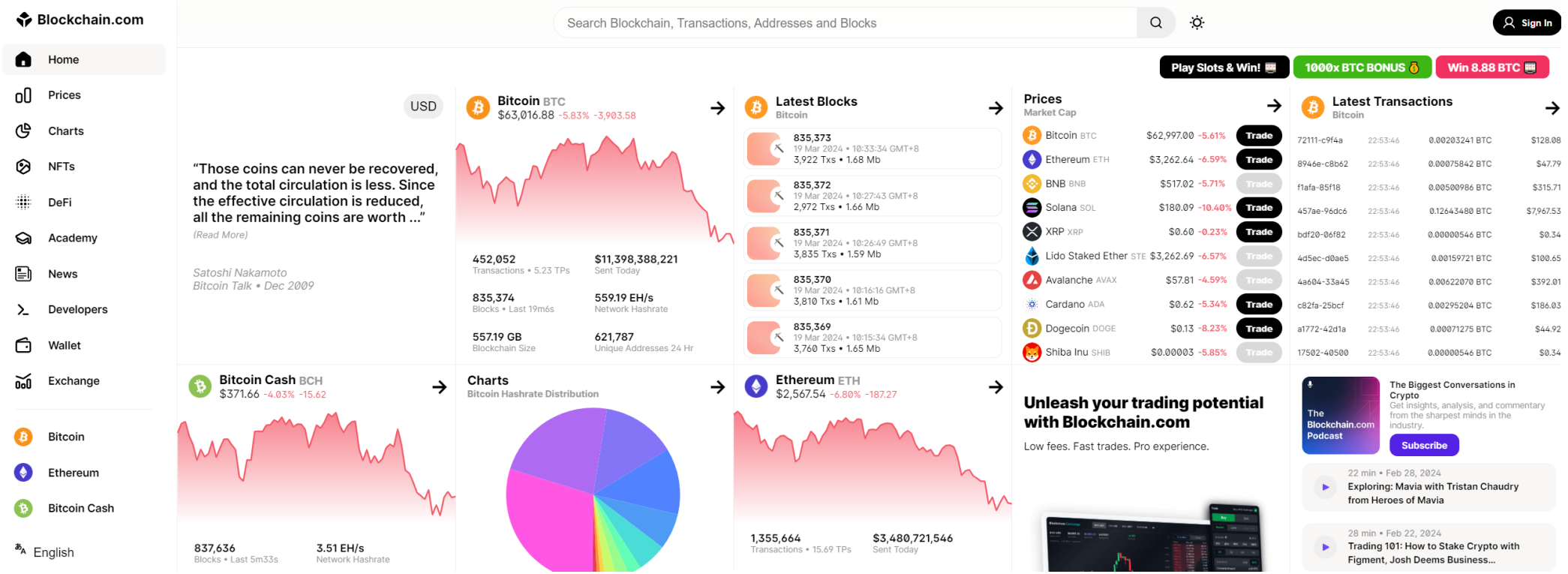
Immutability and Append Only of Blockchain

- 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



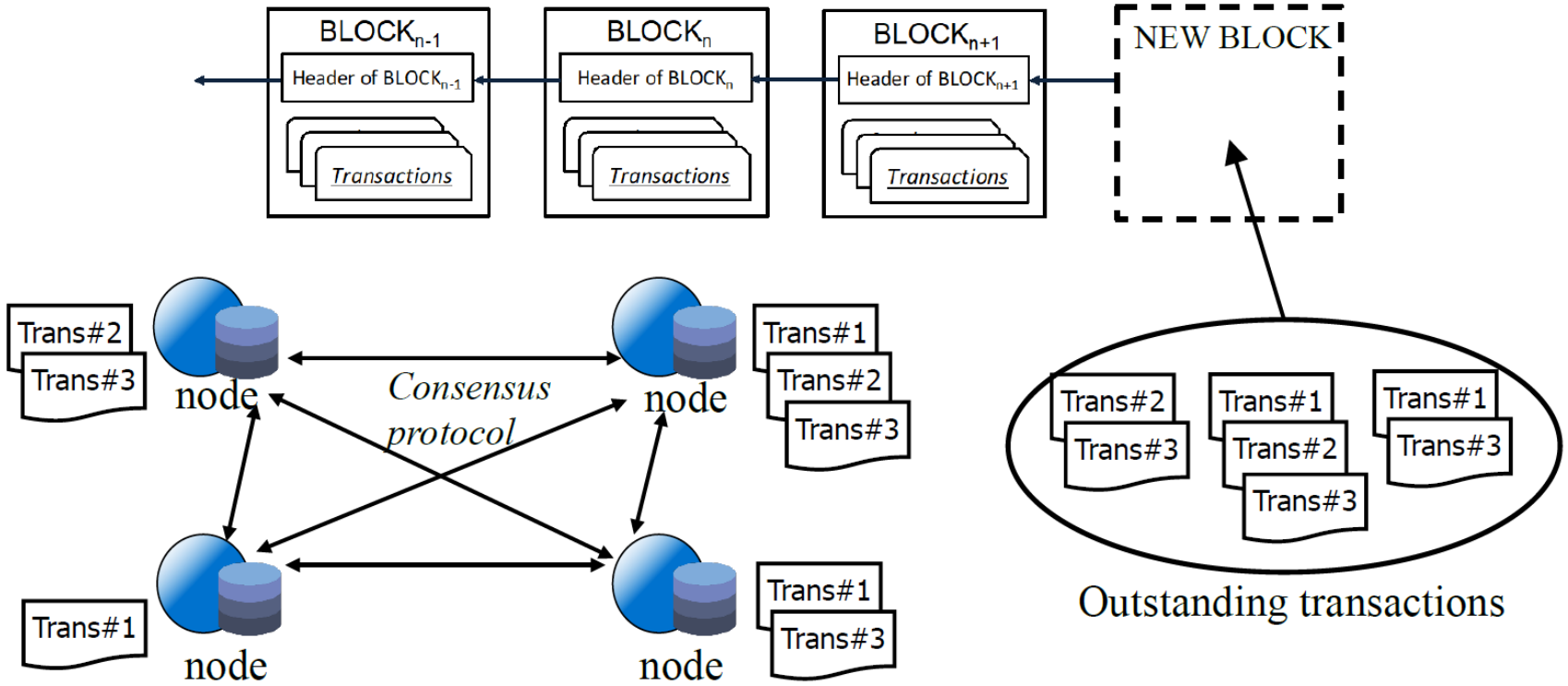
Demo: Block and Transaction in Blockchain

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



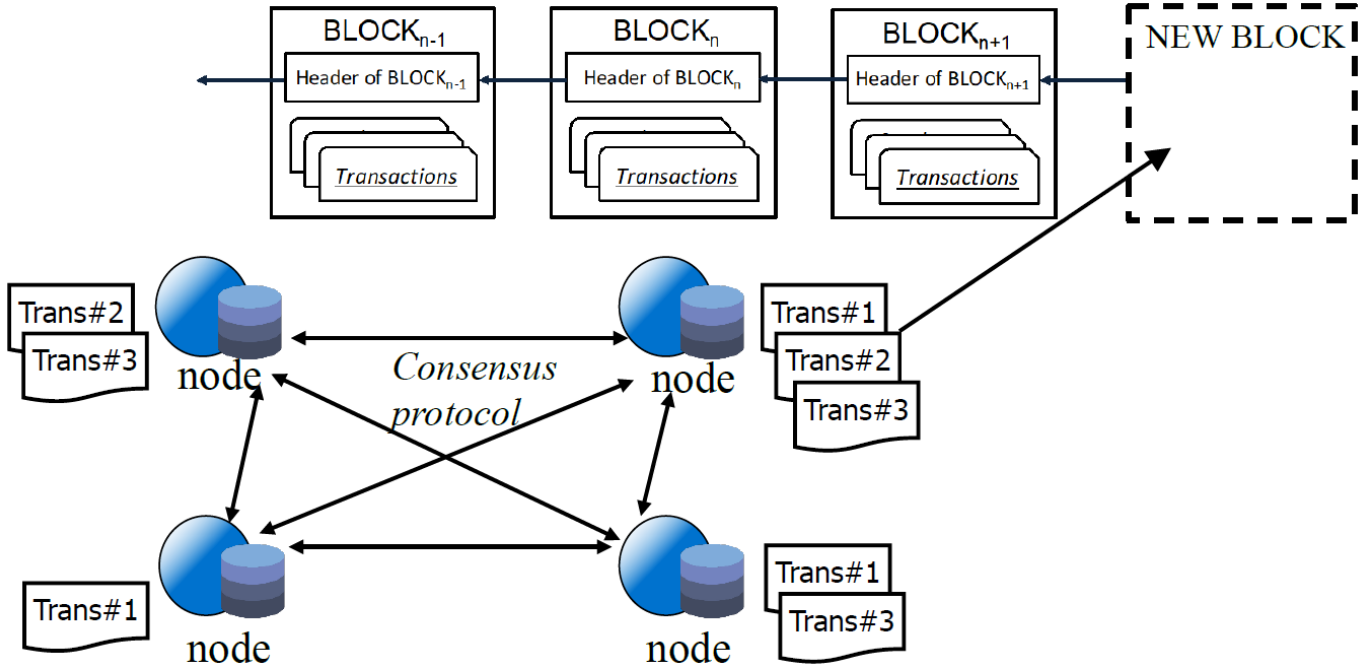
Distributed Consensus: Block Mining

- 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

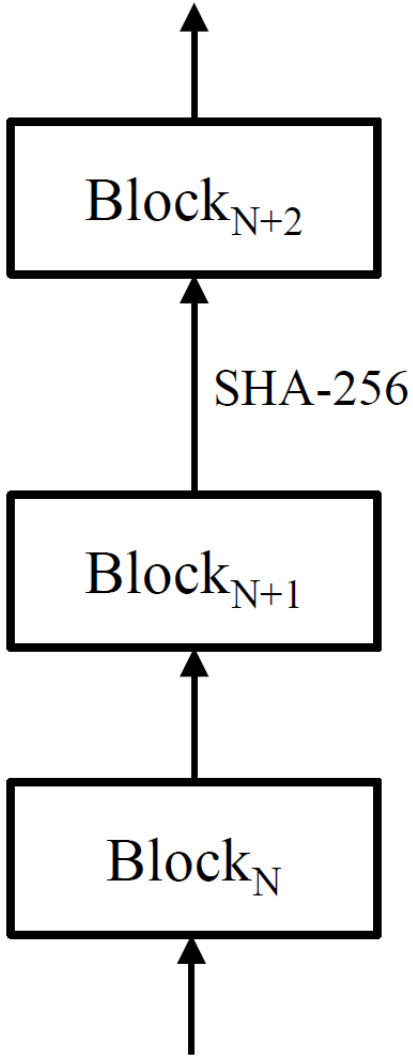


Mining a New Block: Verify Transactions and PoW

- 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



Block Mining: Proof-of-Work (PoW)



Mining difficulty

SHA-256 (block header) = 0x0000000000000c67aa..

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

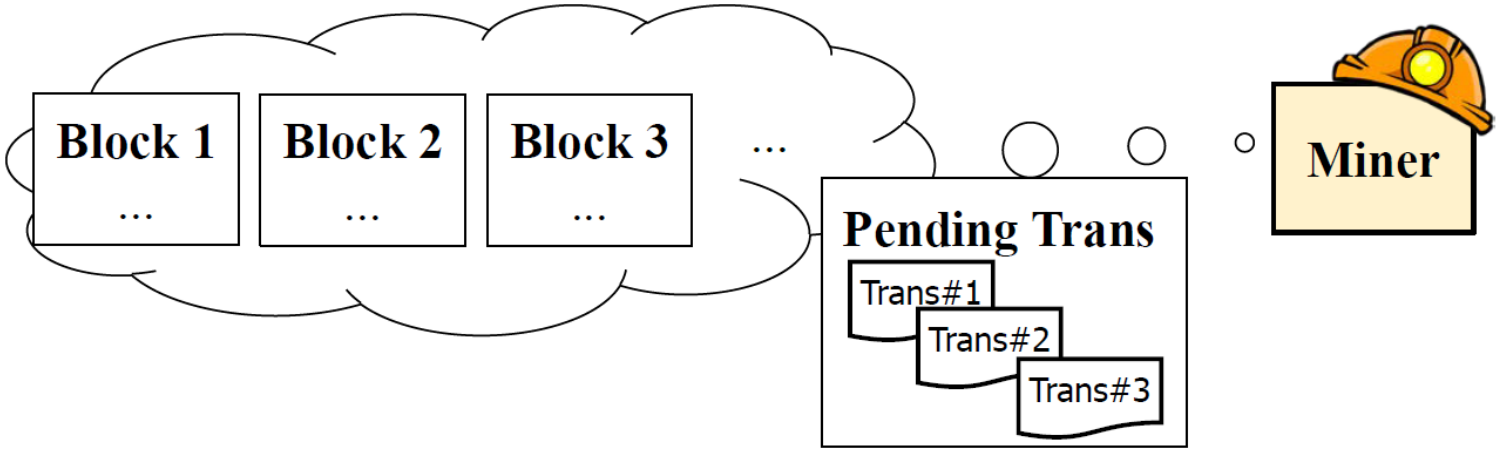
SHA-256 (block header) $\overset{?}{<}$ Z

e.g., hash of previous block header,
Merkle tree root hash, **nonce**

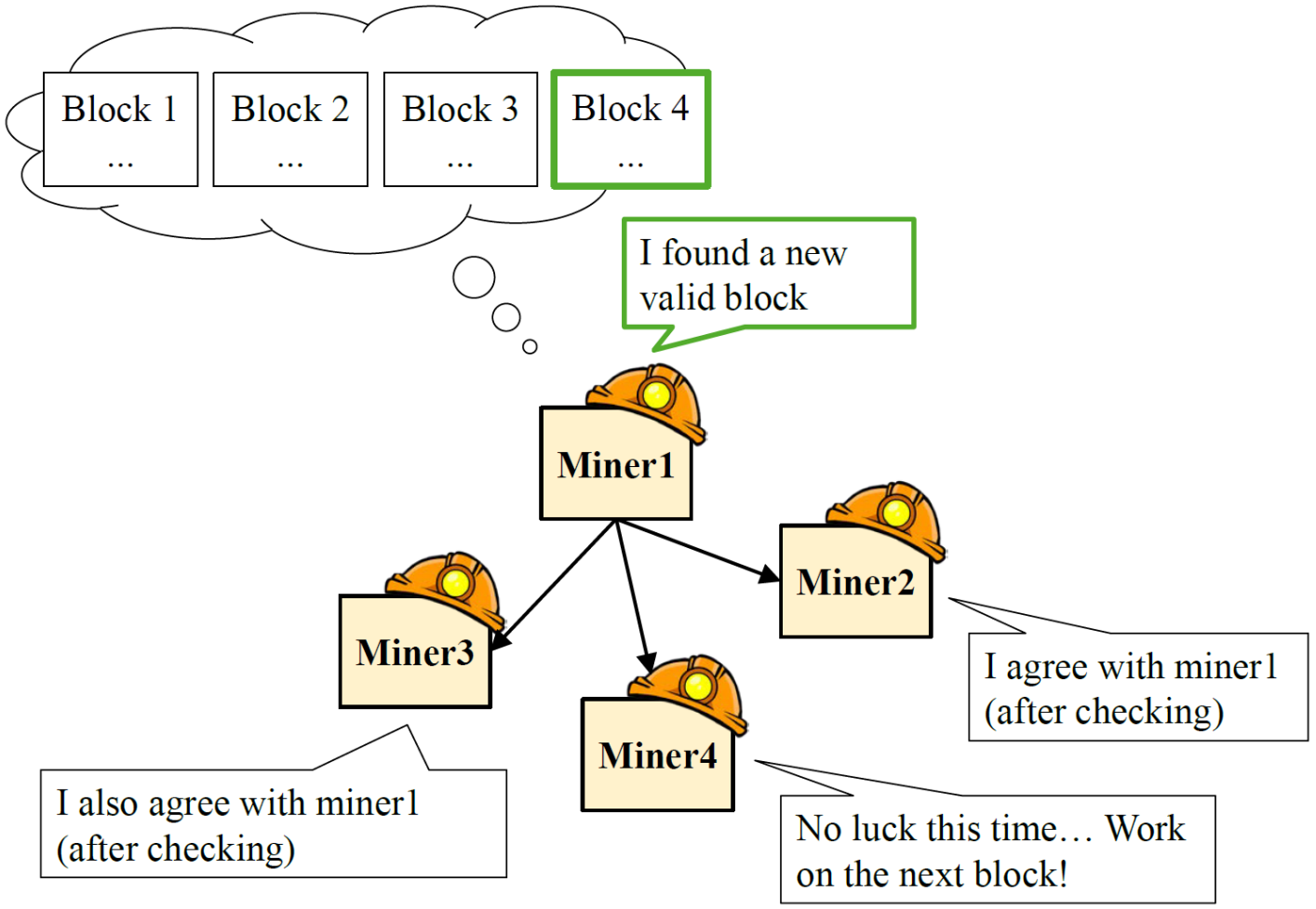
Example: Miners Generate A New Block

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

```
                                        Z = 0x000***...
Hash(Block 3 |   ...   | 0xb9824 )  = 0x000c3f...
```

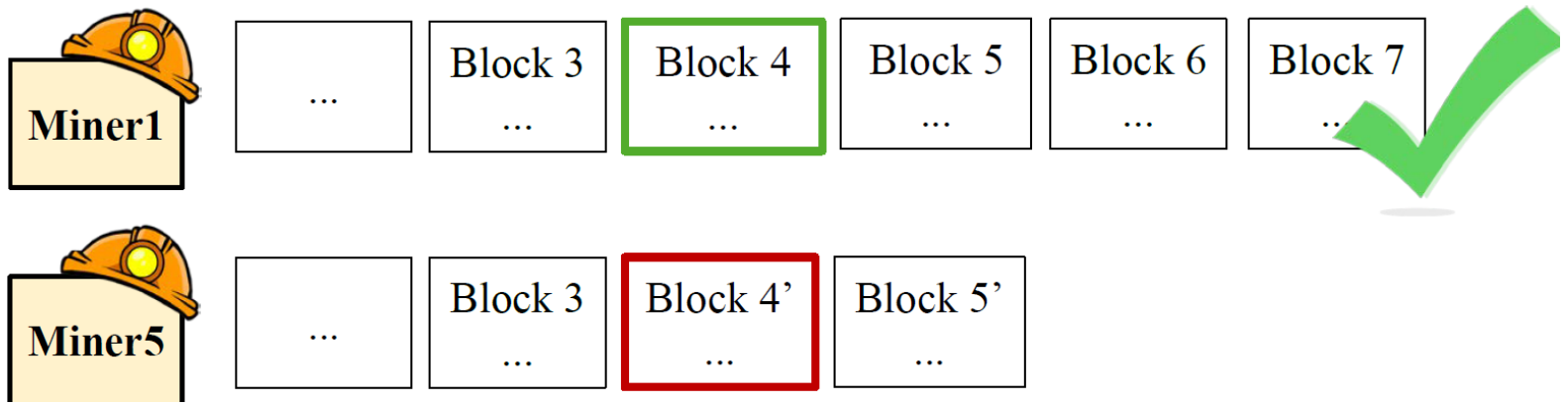


What if a miner loses the competition?



What if two miners succeed simultaneously?

- Distributed consensus: Longest chain
  - 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
  - Transactions of shorter blocks are put back to the pool



What happens if a miner finds a faked trans?

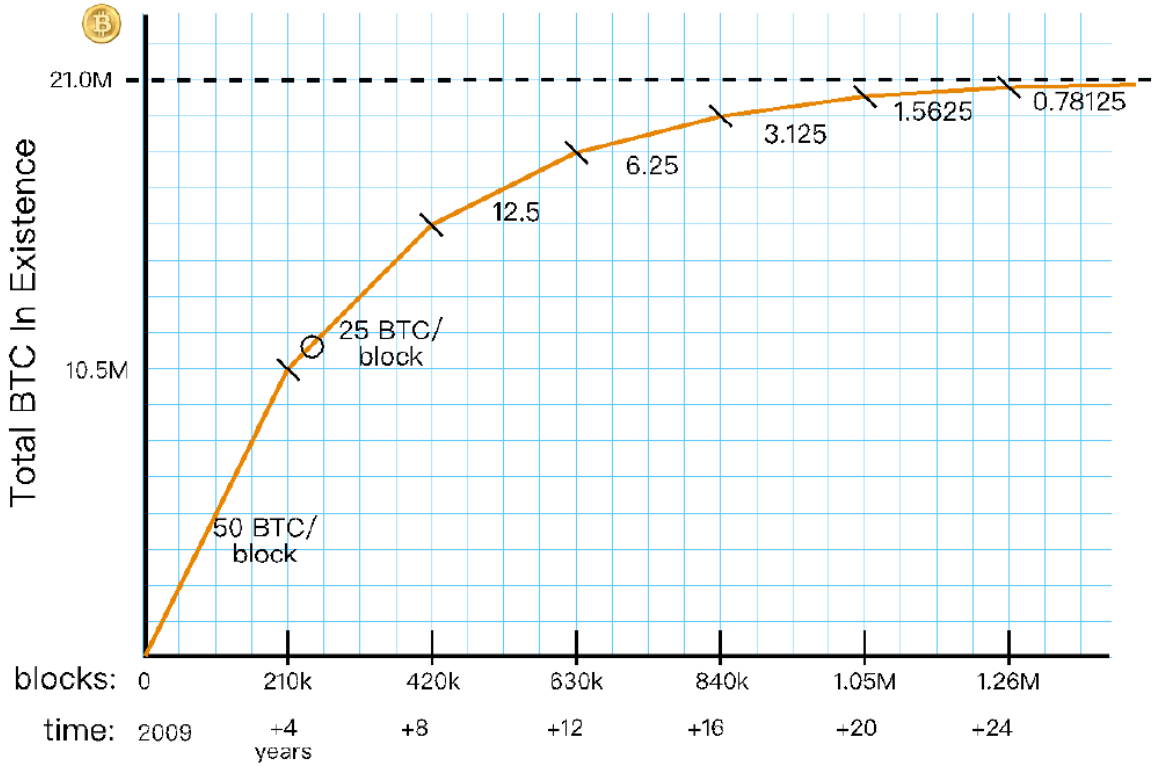
- It simply doesn’t follow the block for growing a new block
  - no reporting mechanism
  - note: no law-enforcement nor central-authority to catch the offenders in blockchain
- The owner of faked trans won’t be able to keep up with the pace to generate subsequent new blocks
  - the block containing 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

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 21M coins coming from?

Maximum Number of Coins (21M)

- Coins are only generated through block mining
- The block reward is cut in half every four years
- Originally, 50 BTC/block; but today, 6.25 BTC/block



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
- Block size 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)

Bitcoin's Dark Side

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

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

Other Potential Application of Blockchain

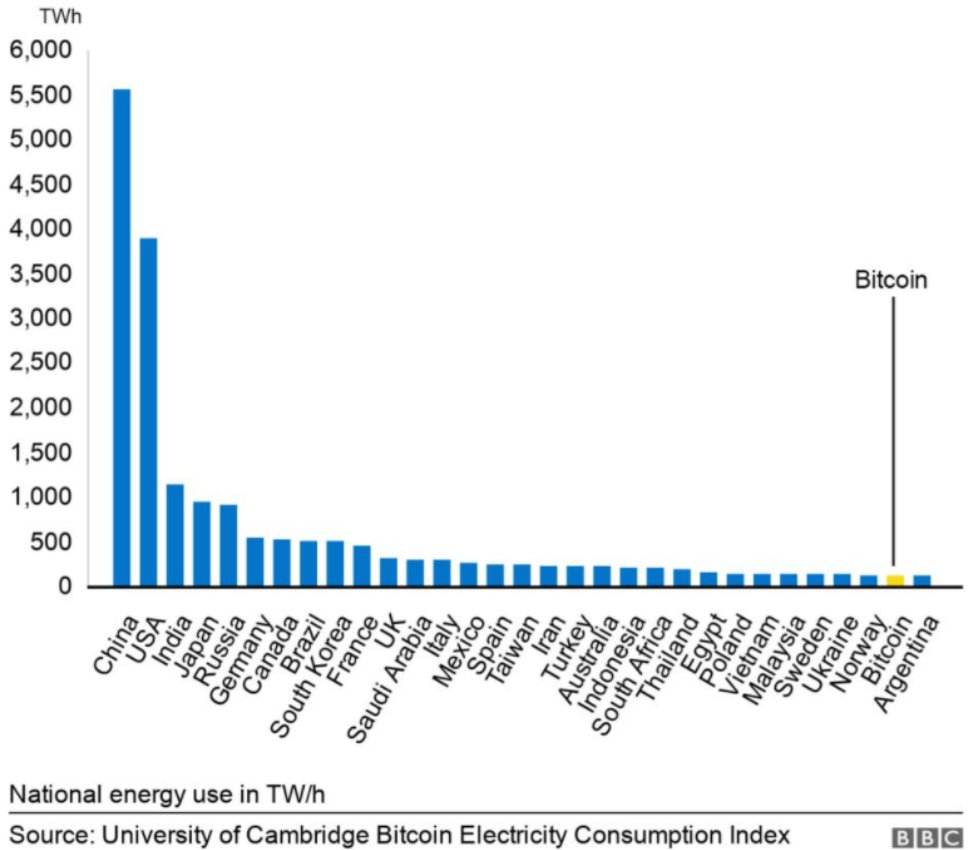
- Smart contract https://soliditylang.org/
  - The terms, rules and conditions of the contract are translated into code, published on the blockchain
  - If a condition is met, the corresponding code is executed and the payment is done
  - The contract and the progression are publicly available
  - IDE Remix
- Product Supply Chain
  - Use blockchain to verify the sources of your food
- Land and properties ownership
  - Store ownerships records on blockchain
- …

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

Discussion

- 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?



Proof of Stake

- Ethereum switched on its proof-of-stake (PoS) mechanism in 2022 .
- https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/
- Proof of Stake (PoS):
  - A cryptocurrency consensus mechanism for processing transactions and creating new blocks in a blockchain.
  - Users need to **stake** their coins in order to participate in the verification process. This mechanism does not need computational resources like PoW.
  - Validators have put something of value into the network that can be destroyed if they act dishonestly.

Proof of Stake

- How does it work?
  - In PoS, users have to be qualified to participate in the verification process. To participate as a validator, a user must deposit 32 ETH (at least) into the deposit contract.
  - Once you are qualified, validators receive new blocks from peers on the Ethereum network.
  - Time in proof-of-stake Ethereum is divided into slots (12 seconds) and epochs (32 slots). One validator is randomly selected to be a **block proposer** in every slot. This validator is responsible for creating a new block and sending it out to other nodes on the network.
  - In every slot, a committee of validators is randomly chosen, whose votes are used to determine the validity of the block being proposed.