decentralized systems & blockchain networks

decentralized systems: introduction

decentralized – definition

- architectural

  物理分布式运行，能tolerate fault

- political

  系统权力和控制分布，decentralized没有单点控制

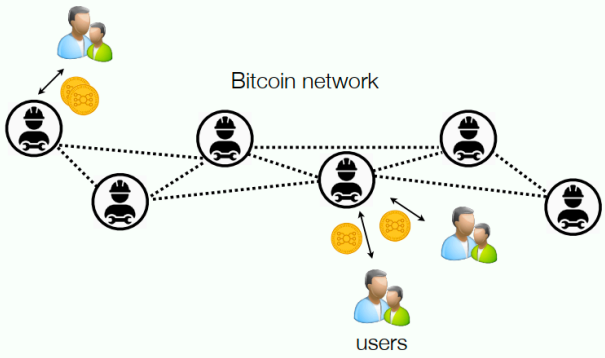
- logical

  a simple heuristic: 切开后两部分仍能独立运行

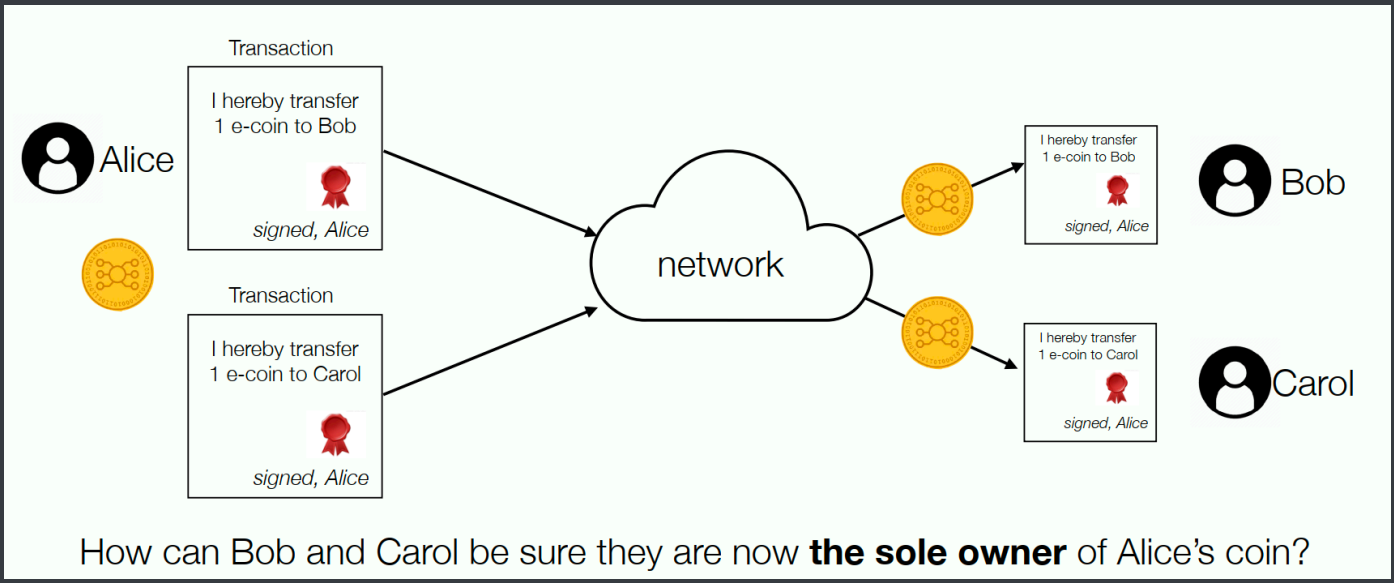
example with Bitcoin

Bitcoin is a decentralised payment network

- Not controlled by any single company or institution
- Introduces its own digital currency unit known as a bitcoin (Bitcoin = the network/protocol, bitcoin = the currency)
- Payment transactions are communicated over a **peer-to-peer** network
- Each **node** in the network **verifies** the validity of each transaction
- Valid transactions become part of a global, replicated, **public ledger**
- The network creates its own **money supply** according to a fixed algorithm
- Users are **pseudonymous**

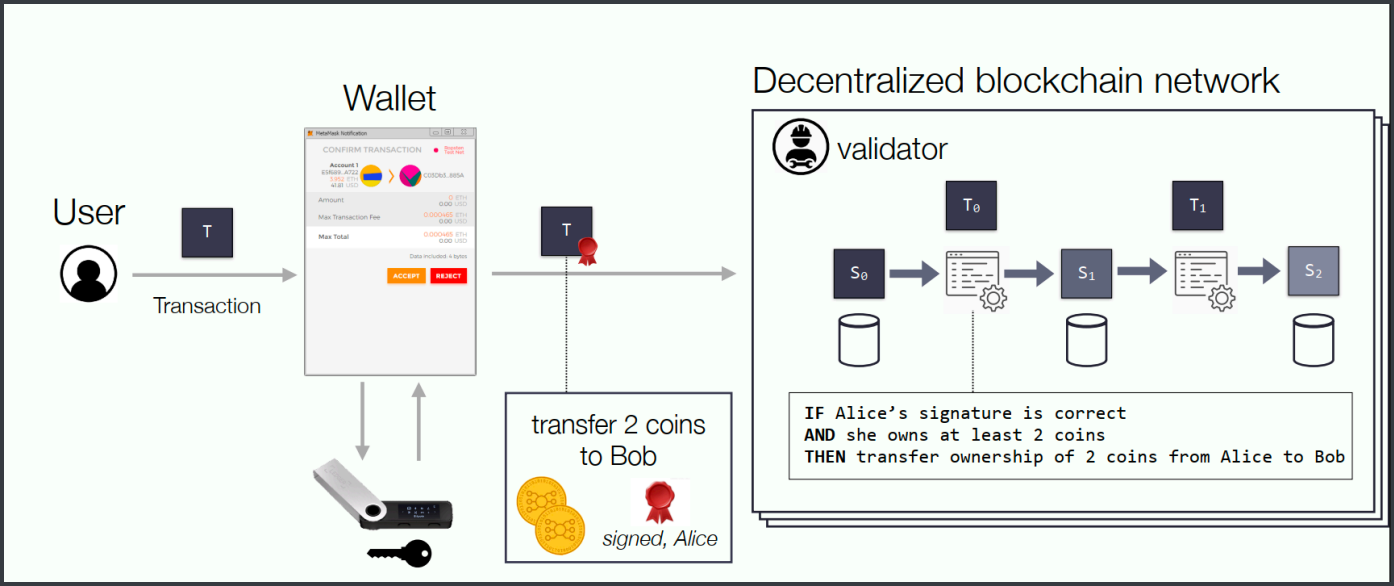


(pseudonymous 与anonymous相比，可被提供更多信息还原原身份)



rather than a single-party clearing house, use

blockchain: a replicated database, append-only, to store transactions



blockchain networks are **replicated state machines**!

"the life of a blockchain transaction"

- step 1: clients submit signed transactions
- step 2: validators validate and gossip transactions

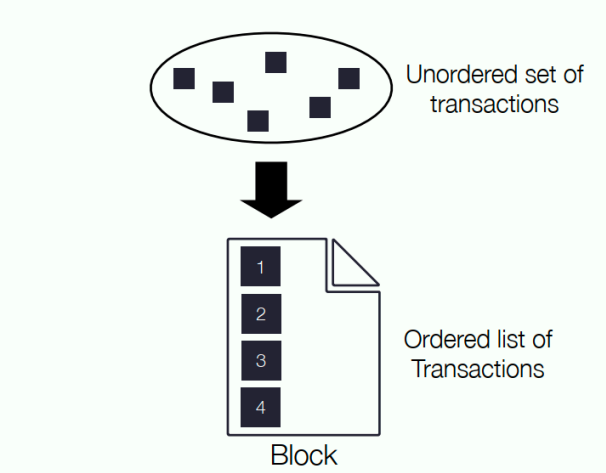
  validator keeps an unordered set ("mempool") of incoming transactions

  collects, validates, broadcasts transactions using **gossip** to other peers

- step 3: a validator produces a block of transactions

  some validators, some transactions,

  ("miners" / "staking validators")



- step 4: validators gossip block and append to blockchain

  gossip, the block is broadcast to all validators

  each validator checks again if valid

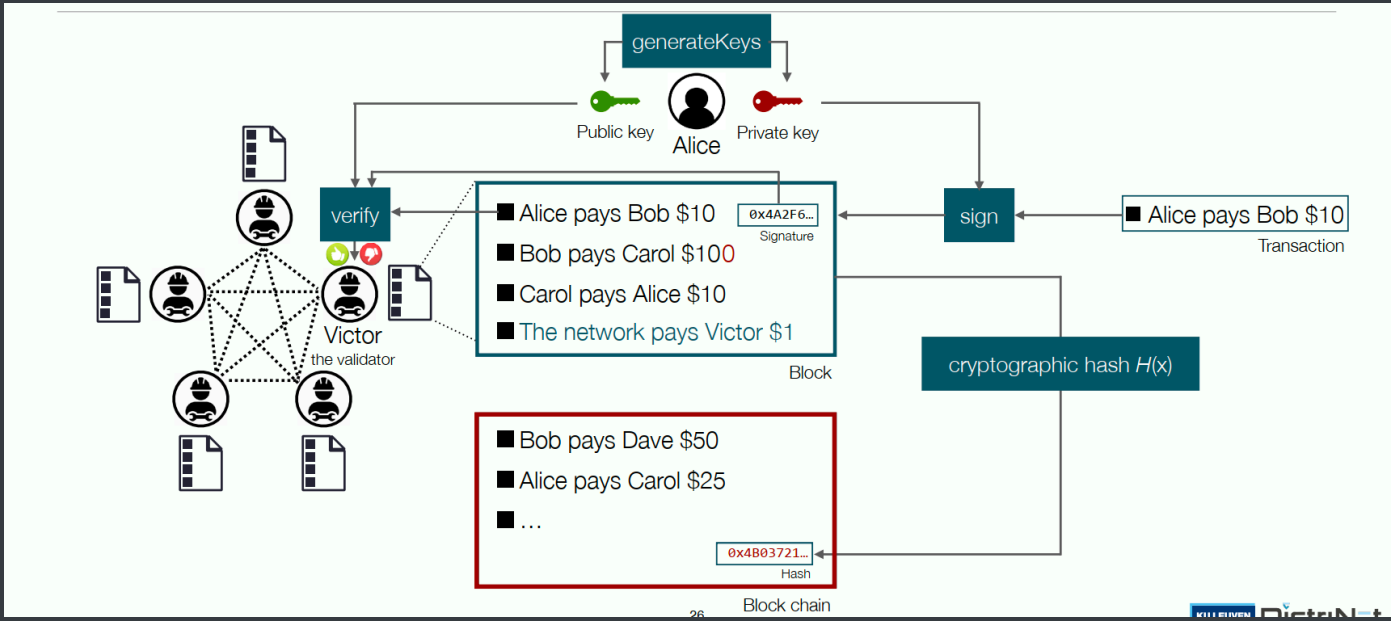
  append -> local transaction log (the blockchain)

tokens, transaction fees, mining rewards

tokens pay for transaction fee, and to **reward validators** for contributing hardware resources

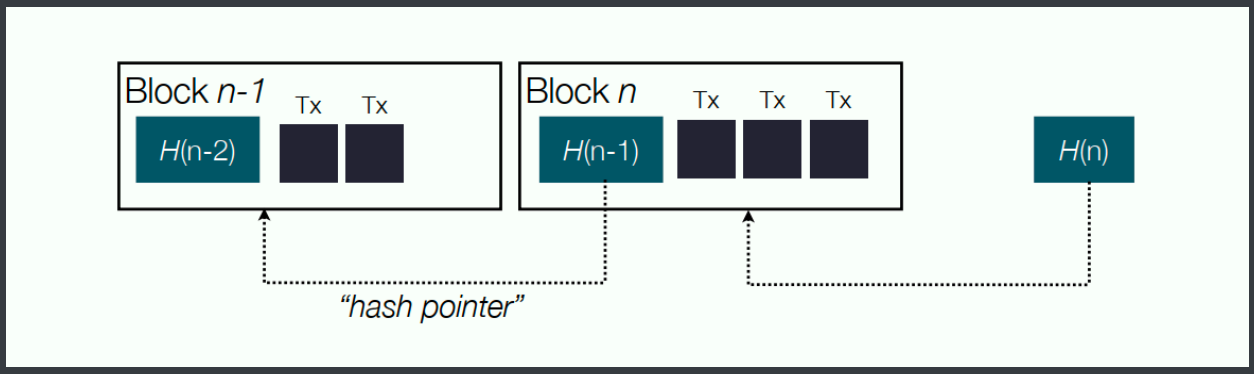
validators can earn additional tokens by producing valid blocks -> incentive mechanism to keep validators honest

cryptographic building blocks of a blockchain



签名ECDSA，哈希SHA-256

- hash pointers



unique identifier (to lookup with) && a digest (only append, no edit)

"tamper-evident"

consensus in blockchain networks

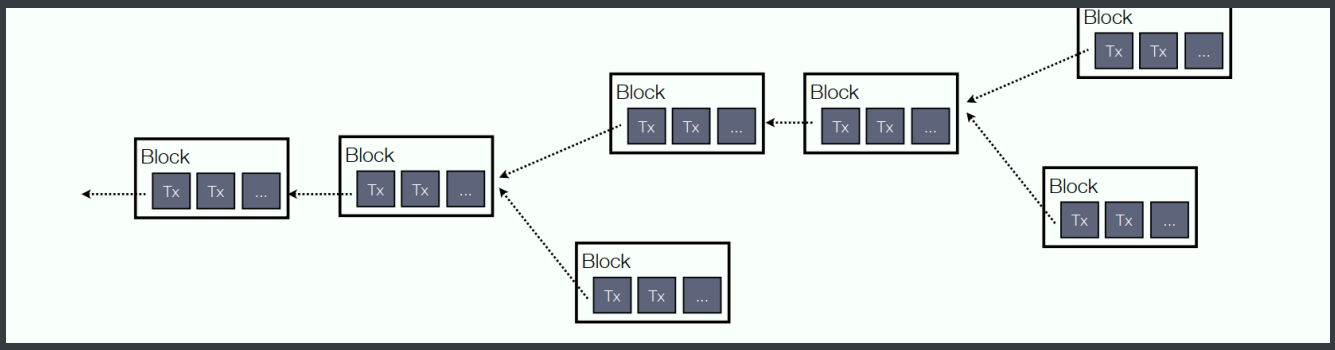
- who can be a validator

  type1: permissionless - group membership is open

  type2: permissioned - group membership is closed

- problem: diverging histories

  if anyone can easily produce a valid block and add it directly -> quick growing *tree* of blocks



- possible solution: organize a vote?

  vote randomly a single validator node to propose the next block

  but voting rights ("identity") is cheap to create, **sybil attack**

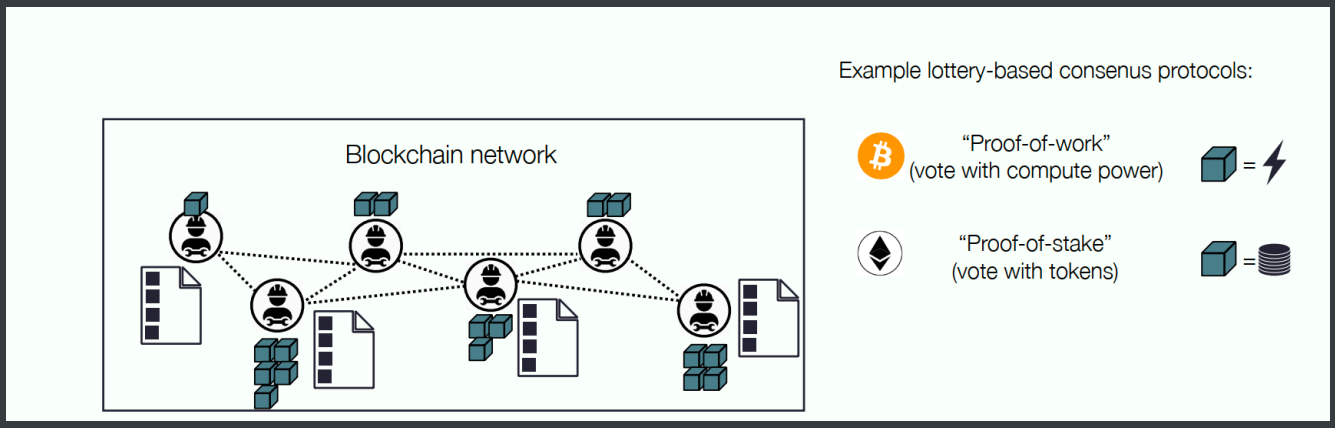
- organize a lottery

  fair - everyone can buy a ticket

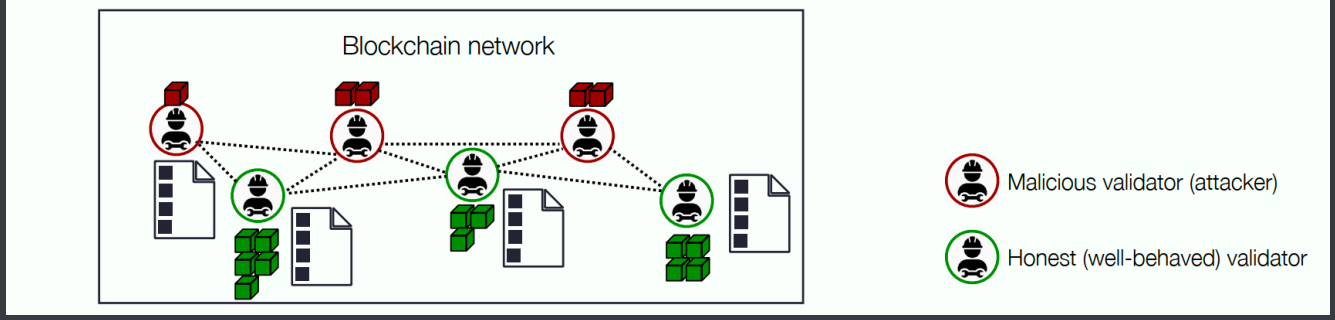
  proportional - the more tickets bought, the higher winning chance

  verifiable - everyone can verify whether the winning ticket is valid

  "proof-of-X": 证明自己有某种稀缺资源，不同系统用的资源不同



- The integrity of the blockchain is guaranteed as long as a **majority** of the network, **weighted** by their resource ownership, is controlled by well-behaved validators



"51% attack": if an attacker controls >50% of the scarce resources, they effectively control the production of new blocks

cannot fake signed transactions (steal tokens), can **censor** transactions & **approve double-spend** of their own tokens

- for permissioned blockchain: can avoid sybil attacks

  no need to "lottery", can use standard CFT / BFT consensus algorithms

	Permissionless	Permissioned
Network peers	Are fully **anonymous** and **untrusted**	May or may not be anonymous. May have some level of **trust** based on external (business) incentives.
Consensus achieved via	**Lottery-based** algorithms, based on proof of owning some scarce resource (e.g. Proof-of-Work, Proof-of-Stake)	**Voting-based** algorithms, such as Byzantine Fault-tolerant (BFT) consensus algorithms (e.g. PBFT)
Peer membership	**Open** (anyone can join, no need to ask "permission" to join)	**Closed** (an administrator manages membership, or pre-existing members vote to update the membership list)
Energy-efficiency	Very **low** for Proof-of-Work **High** for Proof-of-Stake	**High** (similar to a standard replicated databases)
Transaction rate	**Low** (3-4 tx/sec for Bitcoin, 15-20 tx/sec for Ethereum). Generally: the larger the consensus group, the lower the TPS	**High** (10,000 or more TPS) (TPS = transactions per second)
Transaction finality	**Slow**. E.g. in Bitcoin transactions are considered "final" after 6 blocks, and each block takes ~10 minutes to produce)	**Fast**. Block **production times** on the order of a few **seconds**, 1 block confirmation is often sufficient.
Security (51% attacks)	Scales to **large networks** of *O*(1000s) nodes making it very **expensive** for an attacker to disrupt a majority of peers.	Deployed with *O*(10-100) nodes making it **more feasible** (but still difficult) for an attacker to disrupt a majority of peers.