Overview

• Bitcoin overview
• Distributed ledger
• Consensus
• Blockchain generalised
• Limitations

Bitcoin

• Satoshi Nakamoto
  • Oct 2008: Bitcoin: A Peer-to-Peer Electronic Cash System
  • 2009 open source software
• Peer-to-peer digital cryptocurrency (e-cash)
  • anonymous, irreversible transactions
  • goals: privacy, scalability (throughput), decentralisation
    • previous e-cash systems: centralised
    • challenges: protocol updates, robustness of overlay network, incentives

Bitcoin Example

Alice → Bob → Carol
• We need:
  • Identity
    • use public keys
  • Transaction
    • public key Alice sends $X$ coins to public key Bob
  • Ledger of Transactions
    • global list, contains history of all transactions
    • transactions validated before adding
    • ledger is immutable
Threats

- Integrity
  - Spend money you don’t have
    - create bitcoins
    - add a transaction for someone else
- Availability
  - Prevent a user from entering any transactions in ledger
- Confidentiality
  - Break anonymity, identify links between different identities

Blockchain

- Transactions signed -> can’t forge
- Hash pointers -> immutability
- Represents Ledger -> validate transaction before adding it

Distributed Ledger
Threats: Distributed Ledger

- Integrity
- Double spend
  - Bob’s ledger contains Alice -> Bob
  - others contain Alice -> Alice’
- Honest nodes vs dishonest nodes

Proof of Work

- How does everyone agree on the ‘random’ node?
- Do a bunch of work, whoever finishes first gets to go
- Work: hash puzzle. Find nonce such that
  - \( H(\text{nonce} + \text{prev hash} + \text{mrkl_root}) < \text{target} \)
  - target set so that on avg a nonce found every 10 minutes
- Unlikely that >1 node will find a nonce at same time

Consensus

- New transactions broadcast to all nodes
- Random node:
  - collects transactions it received into block
  - broadcasts its block
- Other nodes:
  - validate transactions in block
  - add block to their copy of the blockchain

Transaction Details

- meta data
  - hash id of transaction
  - # inputs, # outputs
- inputs: array of input records
  - input TxID & index
  - ScriptSig: sig (Tx hash signed with Tx creator privkey), pubkey (of Tx creator)
- outputs: array of output records
  - value
  - ScriptPubKey: contains dest pubkey hash
Checking Transaction

• Check T2:
  • T1:HPB = H(T2:PB) => PBs match
  • PB(sigB) = H(T2) => T2 creator has SB

Incentive: Mining Bitcoins

• Create new bitcoins every time a block added to chain
• halve number of bitcoins every 4 years
• limited total number of bitcoins
• Transaction fee for every transaction processed

Network Details

• P2P network
• Joining network
  • seed node
  • get peer info
• Flooding

Mining Details

• Every block has coinbase transaction
  • 15 BTC
  • all transaction fees (inputs - outputs) for block
• coinbase field: arbitrary data
• output: to miner

• Receive transaction:
  • validate inputs
  • check if input already spent
  • check if transaction already seen
  • check if valid scripts (whitelist)
Defence Against Threats

- Steal bitcoin: Bob creates transaction Alice -> Bob
  - signature and keys
- Forge bitcoin: Bob creates a transaction Null -> Bob
  - invalid transaction
- DoS identity: refuse to add any of Bob’s transactions to chain
  - honest nodes will add transaction, need majority of honest nodes

Defense Against Threats

- Double spend: Alice creates a transaction Alice -> Bob, then replaces it with Alice -> Alice’
  - wait until several blocks added so transaction is ‘safe’
  - unlikely that malicious node can add enough fraudulent blocks.
    - needs to create fraudulent chain longer than good chain
    - has to re-mine X fraudulent blocks faster than good nodes can mine single new blocks
  - unless >= 51% of nodes

altcoins

- Ethereum
  - blockchain-based platform
- Ethereum VM, Smartcontracts
- Zcash
- *coin
- Differences:
  - proof of stake
  - zero-knowledge proofs

Generalising Blockchain

- Blockchain is a distributed database
- What can you do with a public distributed database?
  - DNS, identity management, track physical assets, authorisation
  - Smart Contracts
Limitations

- Low throughput
  - bitcoin: 7 transactions/sec
  - credit card: 2000 transactions/sec
- Latency
  - bitcoin: 10 min to process a block
  - credit card: seconds

Reading List

- Bitcoin: A Peer-to-Peer Electronic Cash System. Satoshi Nakamoto
- Lots of articles, blogs, forums, videos, software
- https://blockchain.info: view the blockchain