Blockchain

How does Bitcoin work?

Definition

A blockchain is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree). By design, a blockchain is resistant to modification of its data. This is because once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks.

Source: https://en.wikipedia.org/wiki/Blockchain

Uses

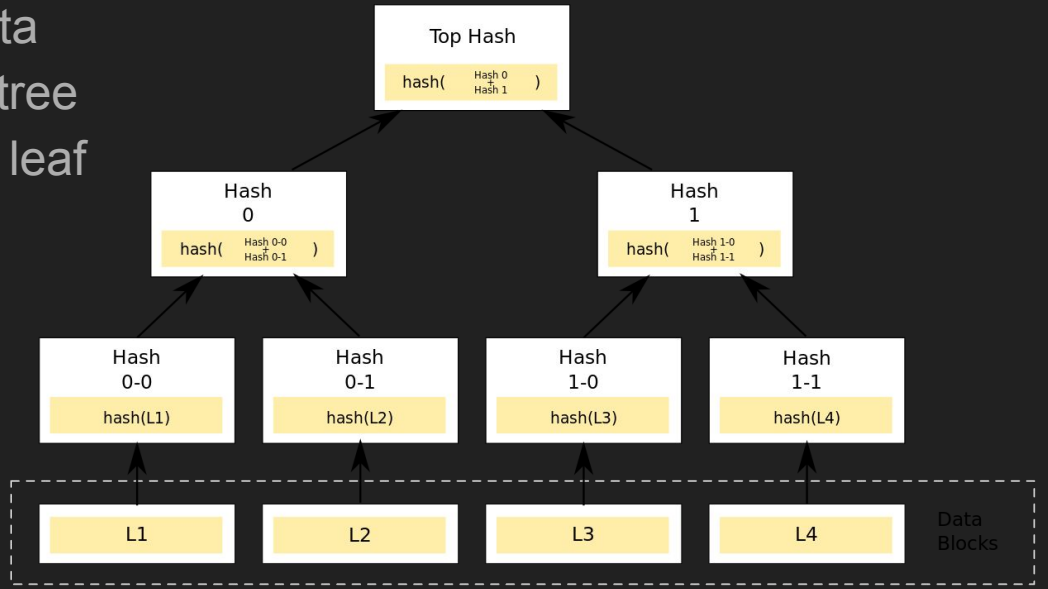
- Timestamping
- Currency
- Proof of freshness
- Systems that require keeping publicly agreed upon unalterable records
    - Information need not necessarily be public

Cryptographic Hash Functions

- Hash function takes arbitrary length input and outputs some fixed number of bytes (digest)
- Preimage resistance
- Second preimage resistance
- Collision resistance

Merkle Trees

- How to hash large amounts of independent data?
- Create hash of each piece of data
- Assign hash to leaves of binary tree
- Requires log(n) hashes to verify leaf



Digital Signatures

- Verify the authenticity of a message
- A private key is used to sign the message
- Signatures should be difficult to forge and unique for every message
- A key is used to verify the message
  - public for asymmetric
  - secret for symmetric
- Signatures have an upper bound on length, but messages can be any length

Bitcoin

- Uses a blockchain
- Blockchain is a very broad concept and can be implemented in many different ways
- Bitcoin is an early implementation that also functions as a currency
- The Bitcoin blockchain can be used for other purposes
  - Timestamping
  - Proof of freshness
  - Storing arbitrary data (can become costly)

Bitcoin

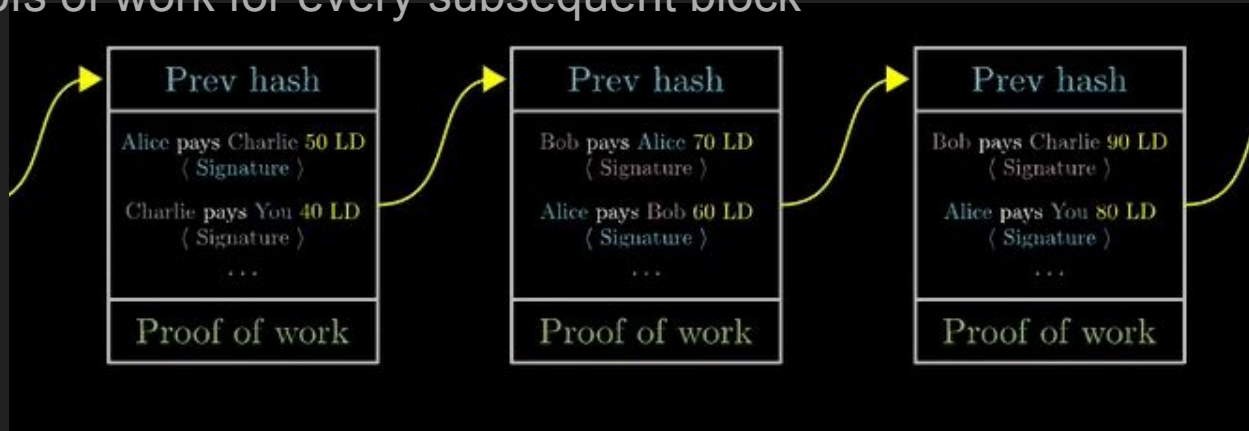
- Bitcoin is a decentralized ledger of transactions
- Anyone can submit a transaction
  - Transactions must be signed by the address sending money
  - Transactions cannot spend more money than an address owns
- Anyone can maintain a copy of this ledger
  - Copies are maintained on nodes
  - Nodes form members of the network and they can also distribute copies and mine new blocks
- Anyone can contribute to maintaining the ledger and adding new transactions
  - Nodes reject blocks that disobey the protocol
  - Miners find new blocks

Bitcoin

- All currency is held by addresses in the form of UTXOs (unspent transaction outputs)
- Addresses can create a transaction that consumes 1 UTXO and outputs multiple UTXOs (each sent to a particular address (including itself))
- Transactions are signed by the private key held by the owner of the address
- Anyone with this key is able to authorize transactions
- One exception: mining reward (coinbase transaction) is sent to an address and originates from no UTXO

Bitcoin

- Transactions are organized into blocks
- Each block has a header that includes details about the block including
  - Timestamp
  - Proof of work
  - Hash of previous block
- The hash of the previous block prevents blocks from being reordered without having to compute proofs of work for every subsequent block



Trusting the Chain

- Nodes will trust the longest chain
- The assumption is that the longest chain is trusted because an attacker would need an immense amount of resources to create the longest chain
- As long as coordinated attackers do not represent a majority of users (exactly how majority is defined can vary from blockchain to blockchain), they cannot alter records in the past
- This is fundamental because it prevents someone from making a transaction and then withdrawing it

Proof of Work

- Bitcoin uses a method called proof of work to ensure the integrity of the blockchain
- An attacker would need > 50% of computational resources of all miners in order to modify the block chain
- Miners are calculating values that prove they did “work” in order to add blocks
- As a reward they can receive the output of the coinbase transaction

Proof of Work

- Cryptographic hash functions cannot be reversed (assumption)
- Finding the preimage for a sha256 hash should require brute forcing the function
- This is expected to be infeasible for anyone
- Posing a requirement like “the first n bytes of the hash must be 0x00” allows a concept of “work” to be created
- This work has adjustable difficulty
- Miners are trying to find a nonce value for a block header such that the hash of the block fits some predefined format (by the specification)

Proof of Work

- Bitcoin blocks maintain an average block time (time it takes to add a new block) of 10 minutes
- When blocks take more time to find, the difficulty is lowered
- When blocks take less time to find, the difficulty is raised
- As more miners look for blocks, the total computational power devoted to finding blocks increases, and blocks become harder to find to keep the block time around 10 minutes
- Mining blocks is essentially a random process
- The only controllable factor in the mining process is the amount of computational resources one devotes

Privacy

- Bitcoin brings up privacy complications
- Anyone can create transactions without the approval or oversight of a governmental body (technically not necessarily legally)
- All transactions and addresses are public
- Coins that obfuscate this information (Monero, Zcash, etc.) can be used for keeping financial records confidential
- Nodes can connect over Tor

Time Stamps

- Bitcoin blocks keep track of time
- This time is enforced by the community
- A sense of time is fundamental to block creation
- It is not high precision, but it is unalterable
- Records stored in a certain block (or their hash) must have existed at or before the time the block was created
- Similarly, the hash of a block can be used as a proof of freshness

Additional Resources

- https://bitcoin.org/bitcoin.pdf
- https://youtu.be/bBC-nXj3Ng4
- https://en.bitcoin.it/wiki/Main_Page

Questions?