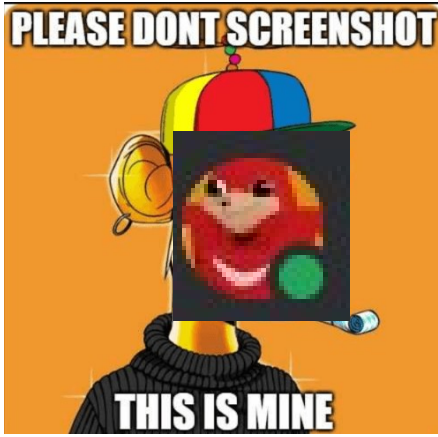
Blockchain



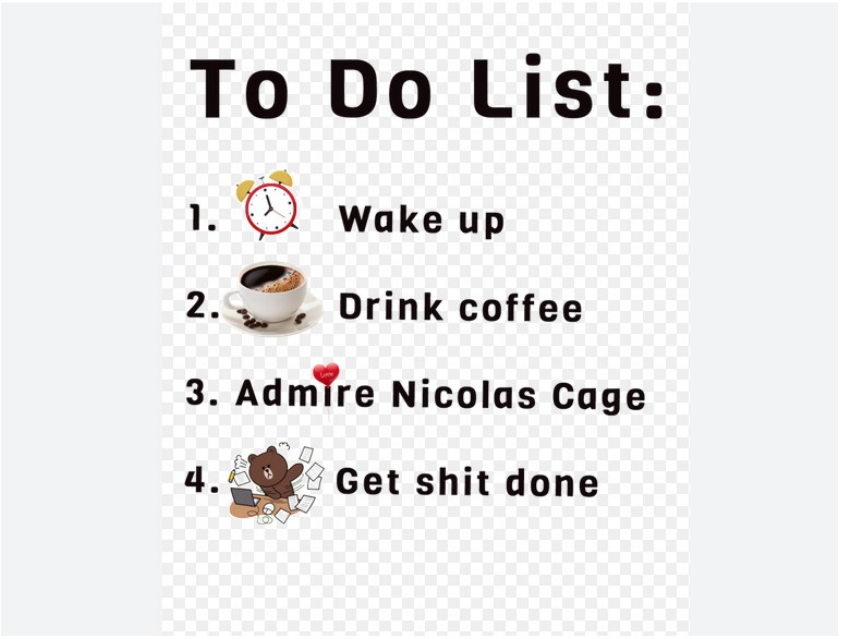
I do not approv e :(

China declares all crypto-currency transactions illegal

24 September 2021

Why?

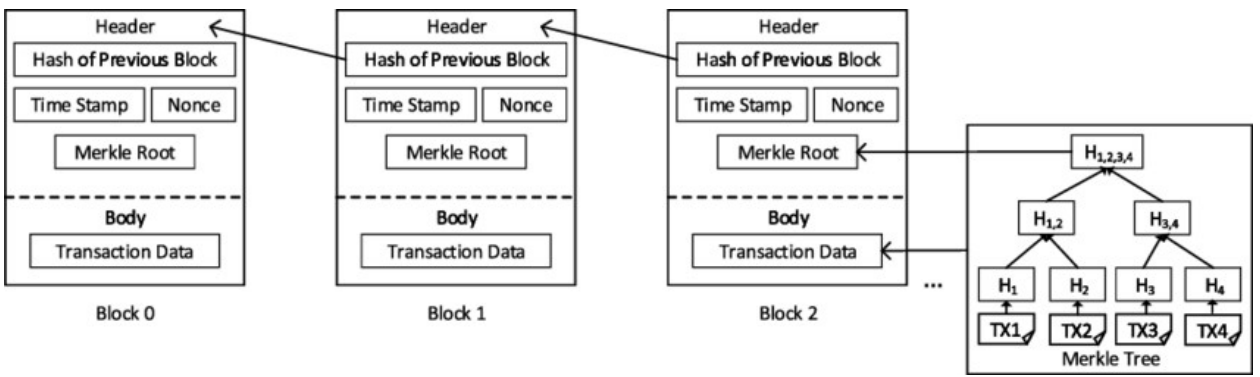
- Decentralized - not owned by a specific company/entity
- Distributed - located on many computers/nodes
- Permissionless - anyone can run their own node
- Public - anyone can view actions on the blockchain
- Permanent - blocks cannot be removed from the blockchain



I have no idea what this has to do with crypto

Blocks

- The distributed database is made of a series of *blocks*
- Blocks can be appended only
- Each contain a hash of the previous
  - Previous blocks in the chain can’t be edited



*The Merkle root is just a fancy hash of the block contents in a tree structure

https://www.shiksha.com/online-courses/articles/structure-of-a-block-in-blockchain/

Consensus mechanisms

- Determine which new blocks are added to the blockchain
- Very strict rules on which blocks are *confirmed*
- Aim to maximize the number of people competing to *mine* a block, thus making attacks more difficult
  - Successful miner receives a set financial reward, plus transaction fees
- Chance of mining a block is stochastic
- Might involve setting aside currency (*proof of stake*, e.g. Ethereum) or using a large amount of computing power (*proof of work*, e.g. Bitcoin)

Bitcoin

- All other systems of payment except cash payments require some kind of third party (banks, credit cards, PayPal, etc.). Bitcoin aims to get around this.
- Distributed ledger
- Divisible to 10^{-8} ฿
- Each block contains many transactions
- New block approximately every 10 minutes
- Pseudonymous - Bitcoins are transferred to *addresses*
  - Addresses are created from a public key
  - Spending bitcoin requires signing the transaction using the private key
- Uses a proof-of-work consensus mechanism

Bitcoin’s consensus mechanism

The block reward started at 50 Bitcoin in 2009, and gets cut in half roughly every 4 years. Miners also receive transaction fees from the transactions contained in the block.

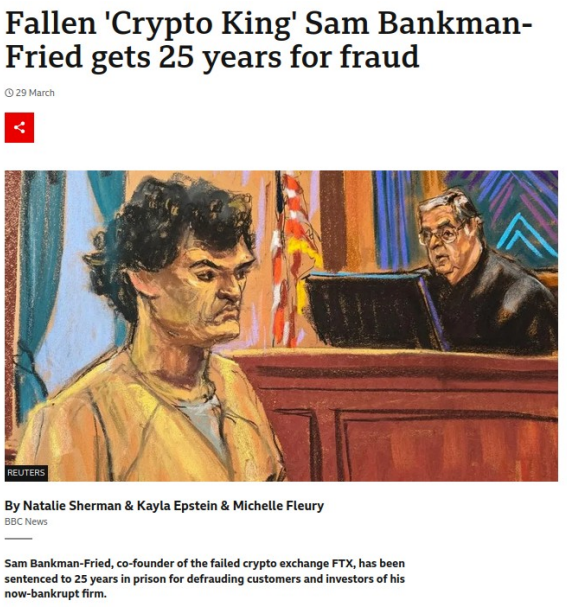
- A miner collects transactions
- Adds a special transaction which awards the *block reward* to themself
- Computes the Merkel root of the transactions in the new block
- Needs to find a *nonce* value such that SHA256(Merkel root, nonce) is less than the *target hash value*
- The target hash value is adjusted such that the average time to mine a block remains at 10 minutes
- If the target hash value is lower, the *difficulty* of mining a block is higher

Why does Proof of Work work?

- It prevents transactions from being censored
  - The transaction fees system incentivizes the miner to collect as many transactions as possible
  - Since the chance of mining a block is stochastic dependent on the amount of computing power invested, you would have to acquire the majority of computing power to have a chance at getting a censored block confirmed
- It prevents double spending
  - Sometimes you can have competing blocks submitted to the chain.
  - This creates a *fork*.
  - The longest chain is considered the legitimate one.
  - Theoretically, a user could submit a transaction in exchange for resources, then mine 2 competing blocks to create an alternative chain. Again, this would require the majority of computing power.

Problems with Bitcoin

- It is **obscenely** power-intensive
  - Bitcoin's proof-of-work system used an estimated 0.2% to 0.9% of global demand for electricity in 2023 (https://www.eia.gov/todayinenergy/detail.php?id=61364)
- It is slow
  - New blocks are added every 10 minutes
  - For large transactions it is common to wait for several blocks to be confirmed
- It has become more centralized
  - Managing public and private keys can be a hassle, so it's common to use web wallets/centralized cryptocurrency exchanges
  - Centralized mining has made Bitcoin more vulnerable to *51% attacks…*



Fallen 'Crypto King' Sam Bankman-Fried gets 25 years for fraud

29 March

REUTERS

By Natalie Sherman & Kayla Epstein & Michelle Fleury

BBC News

Sam Bankman-Fried, co-founder of the failed crypto exchange FTX, has been sentenced to 25 years in prison for defrauding customers and investors of his now-bankrupt firm.

“51%” attacks

- If someone gains control over the majority of the hashrate they could theoretically double-spend coins or censor transactions
- This has actually happened due to the emergent behaviour of *pooling*:
  - Since it is very unlikely to successfully mine a Bitcoin, it is common to *pool* mining power
  - If any member in the pool mines a block, the reward is divided between all members
- Ghash.io reached a 51% network hashrate in 2014 before voluntarily capping its power at 39.99%
- Proof-of-stake blockchains are also vulnerable to this attack
  - An attack would require staking more than half of the total currency staked

Blockchain summary

- Blockchains rely heavily on financial incentives to maintain a trustless system
- It works best when there are a large amount of users (as attacks become more difficult)

Messaging apps

- Need to consider what level of trust be built into our system
- How can we prevent old messages being inserted?
- How important is having everyone seeing messages in the same order?
- Probably need to run on an existing blockchain, e.g. Ethereum
  - A tutorial to do just that (partially written by AI because of course) https://medium.com/coinmonks/building-a-blockchain-based-messaging-application-on-ethereum-a-complete-guide-3ce5a7253260
  - Main advantage over a traditional client-server is immutability