Timeline

THE BIG SHORT MOVIE

2008 - Global Financial Crisis.

2009 - Bitcoin whitepaper

https://bitcoin.org/bitcoin.pdf

2010 - The 10k BTC Pizza

https://www.youtube.com/watch?v=j28hkTJMuTA

2015 - Ethereum Launch

2018 - Solana Founded

2020 - Solana Mainnet Beta

2020 - COVID-19 & Infinite Money printing

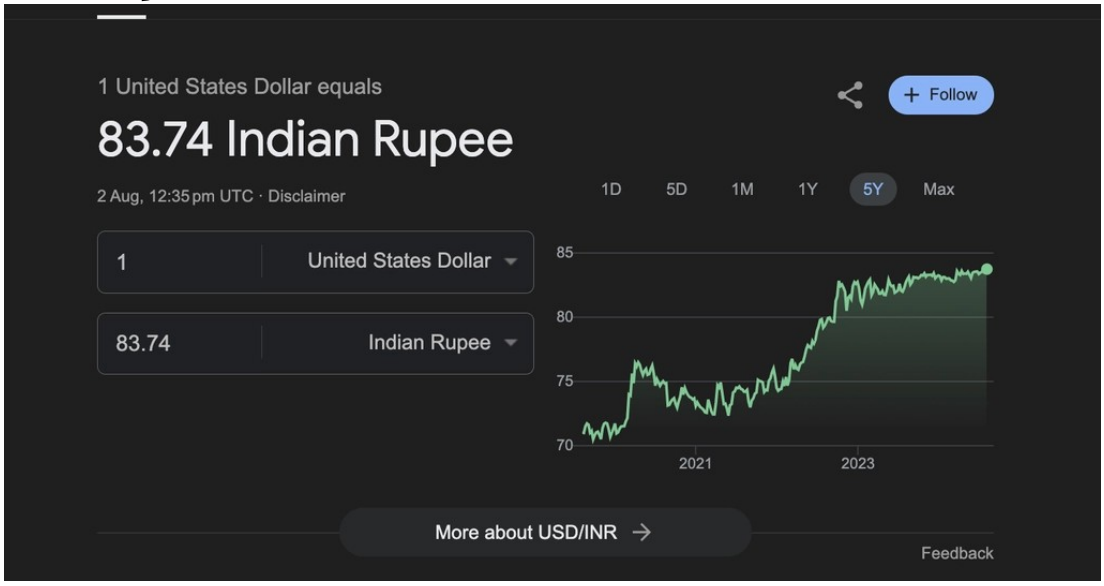
2021 - NFT, DeFi & Solana Breakout

2025 - Trump coin/Memecoin saga/Hyperliquid/Lighter

Problems with currencies

Inflation

Last year



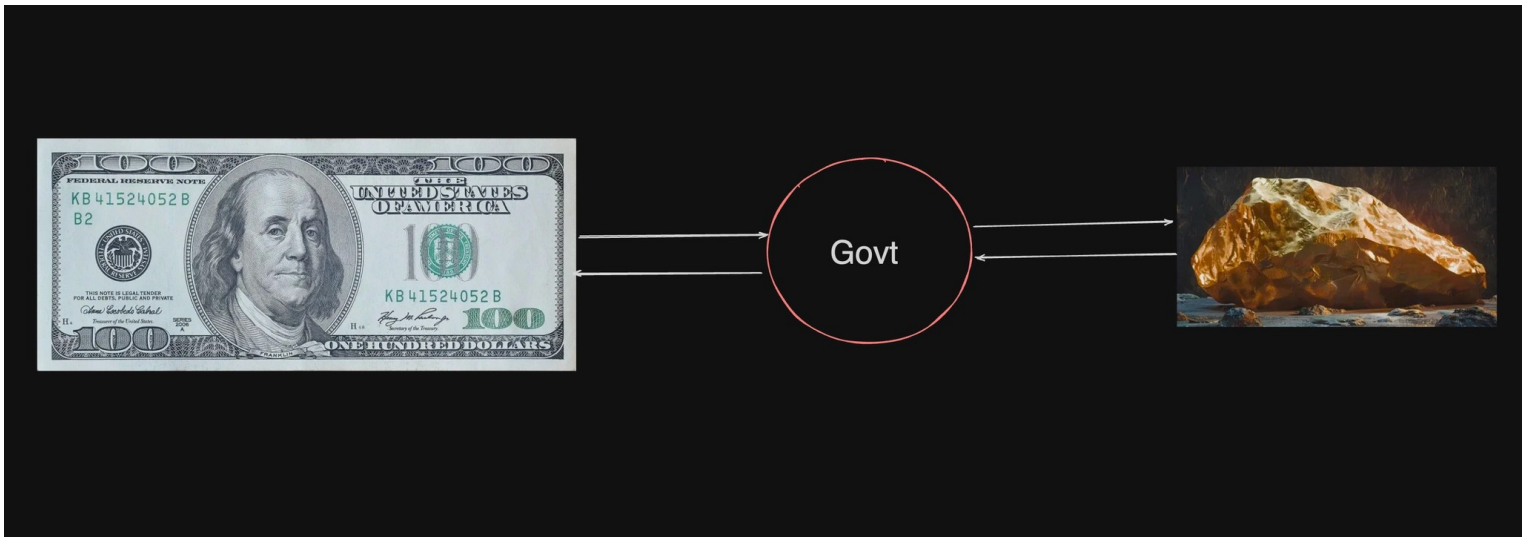
This year

Centralized

The govt/RBI gets to decide when to mint, where to use the newly minted supply, if there is a need for stimulus cheques.

Not backed by anything

There was a time when currencies were backed by gold. You could always take $X to the govt and they would return you 10 grams of gold. That no longer holds true.



Gold as a store of value

People consider **gold a store of value** because, across history and economics, it has several qualities that help it *preserve purchasing power over long periods of time*. The main reasons are:

---

1. Scarcity and Limited Supply

Gold is rare and costly to extract. Unlike paper money, it **can't be created at will** by governments or central banks. This scarcity helps prevent rapid devaluation.

---

2. Durability

Gold doesn't rust, corrode, or decay. A gold coin from 2,000 years ago is still essentially the same today, which makes it reliable for long-term value storage.

---

3. Universal Acceptance

Across cultures and civilizations, gold has been recognized as valuable. Even today, it’s traded globally and accepted almost everywhere, making it highly liquid.

---

4. Intrinsic Demand

Gold has value beyond investment:

- Jewelry
- Electronics
- Dentistry
- Industrial uses

This ongoing demand supports its price even when financial systems are unstable.

---

5. Inflation Hedge (Historically)

Over long periods, gold has tended to **retain purchasing power** when currencies lose value due to inflation or excessive money printing.

---

6. Independence from Governments

Gold isn’t tied to any single country’s economy or political system. When trust in governments, banks, or fiat currencies declines, people often turn to gold.

Bitcoin as a store of value/currency/digital gold

1. Gold is hard/invonvinient to carry
2. Very hard to tell the purity of gold w/o getting it checked.
3. Inefficient markets (India price is different from US price, gold shops have >3-5% making charges)

Wouldn't it be nice if something digital holds the same properties as gold?

Where price discovery was better than gold, purity could be judged digitally.

Where it would be easy to create global marketpalces rather than localized gold shops.

This is what was introduced in the BTC whitepaper

THEN EVERYTHING AFTER THIS IS IN THE SOLANA JARGON
ALL THE BASICS

How would you create a decentralized blockchain/currency?

1. Write a program (./bitcoin_miner.exe) that people can run on their machine to become miners of the network
2. Write code in the program that dictates how the currency is minted (new currency is created) and who gets the initial supply (developers, initial investors, airdrop)
3. Let anyone join the network/be a miner by running the program (bitcoin_miner.exe)

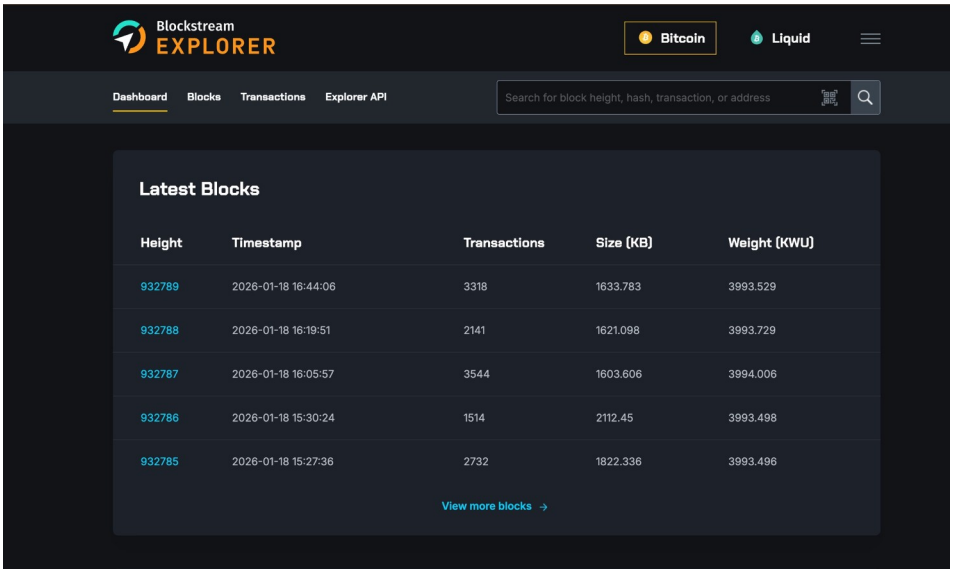
4. If people want to send BTC/receive BTC, they should create a public private keypair (no username password like banks)
5. To send BTC from your wallet (your public key) to a different wallet, sign a transaction/message and send the transaction to one/many miners (btc-miner-india.100xdevs.com)
6. Miners bundle multiple transactions (lets say all txns that came in the last 10s) in a block. The block is transmitted by the miner to everyone else in the network. This creates a permanent record/ledger of all the blocks since the starting (genesis).
7. A chain of these blocks is called the blockchain.

There are a lot of problems in this approach that we will discuss/fix in the upcoming slides.

Ref - https://www.canva.com/design/DAG-wwcLjb0/-PJvxmw65928wfsLQDPOrQ/edit?utm_content=DAG-wwcLjb0&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton

Latest blocks - https://blockstream.info/

Aims to create 1 block per 10 minutes by varying difficulty of proof of work



to become a miner you have to just clone the github.com/bitcoin/bitcoin repo and than just use that to mine the bitcoin and when you create

consesus algo in bitcoin is proff of work
in solana, eth its proff of stake

its like used to stop the people for randomly pushing the blocks in the chain and prventing from filling with many useless blocks

Problems with current approach

- **Can a miner move money from one random address to another?**

  No, only the user who holds the private key can sign the transaction. So even if a miner tries to mimic a transaction, other miners will reject the transaction signature.

- **Which miner should I send my transaction to?**

  When you hit "send" in your wallet, your transaction gets broadcast to whichever Bitcoin nodes your wallet is connected to. From there, it propagates across the entire network through a gossip protocol—each node that receives your transaction validates it and forwards it to the other nodes it's connected to. Within seconds, your transaction typically reaches most nodes on the network, including those run by miners.

- **What if a miner doesnt include my transaction?**

It can happen. There can be blacklists/less incentive for a miner to include ur txn. That is why the concept of tipping exists

- **Why would a person start a new miner? What do they get?**

  When you propose a block, you add a txn to the top that gives you the block reward. This is how new BTC is added to the system. You can also earn tips based on who wants their txn to be included the fastest.

  1. Block subsidy (the "block reward")

  This is newly created bitcoin that gets awarded to whoever mines a valid block. It started at 50 BTC per block in 2009 and halves roughly every four years (every 210,000 blocks). Currently it's 3.125 BTC per block after the April 2024 halving. This subsidy is how all new bitcoin enters circulation.

  2. Transaction fees

  Every transaction in the block includes a fee paid by the sender. The miner who finds the block collects all the fees from every transaction they included. When the mempool is congested, fees can add up to a meaningful amount—sometimes rivaling or even exceeding the block subsidy during periods of high demand.

- **Why wouldnt a miner always start to propose a block then? I would want to keep all the block reward for myself. I’ll just start a new miner and start proposing blocks every 1 minute.**

To be able to propose a block, you need to solve a cryptographically hard problem. If there are 100 miners right now all having 4 cpus, they are all solving the same problem. On average you will only be able to propose a block once in 100 blocks (simple probability).

This is why people say BTC/crypto is bad for the environment because thousands of machines all around the world are solving the same futile problem just to be the block leader

What if two people propose a block at the same time?

This happens occasionally and is totally normal—it's called a **chain split** or **temporary fork**.

What actually happens

Say miners A and B both find valid blocks at roughly the same height. Some nodes will hear about block A first, others will hear about block B first. Each node considers the first valid block it receives as the current tip of the chain and starts building on that. So now you briefly have

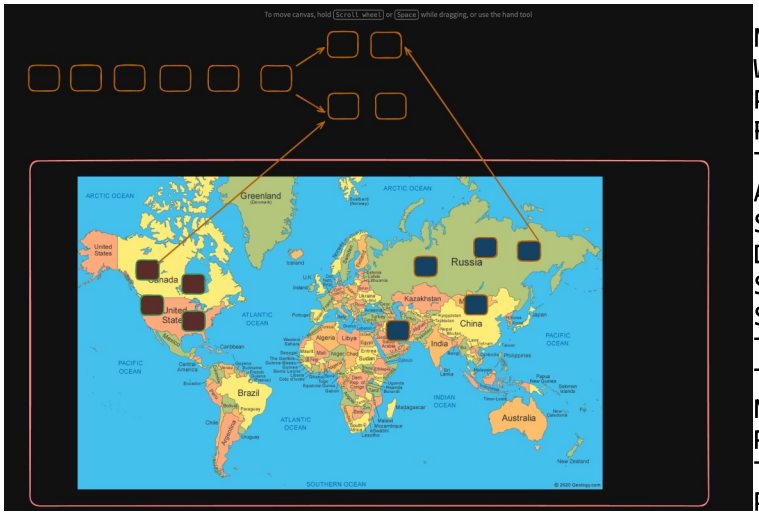
two competing versions of the blockchain, each with a portion of the network working on it.

How it resolves

The rule is simple: the longest chain wins (technically, the chain with the most cumulative proof-of-work). As soon as another block gets mined on top of either A or B, that chain becomes longer. Nodes following the shorter chain will immediately abandon it and switch to the longer one. The "orphaned" block gets discarded—its transactions return to the mempool to be included in a future block.

Implications

This is why people wait for "confirmations" before considering a transaction final. One confirmation means it's in a block, but that block could still get orphaned. Six confirmations has become the informal standard for high-value transactions—at that depth, a reorg is extraordinarily unlikely without a deliberate 51% attack.

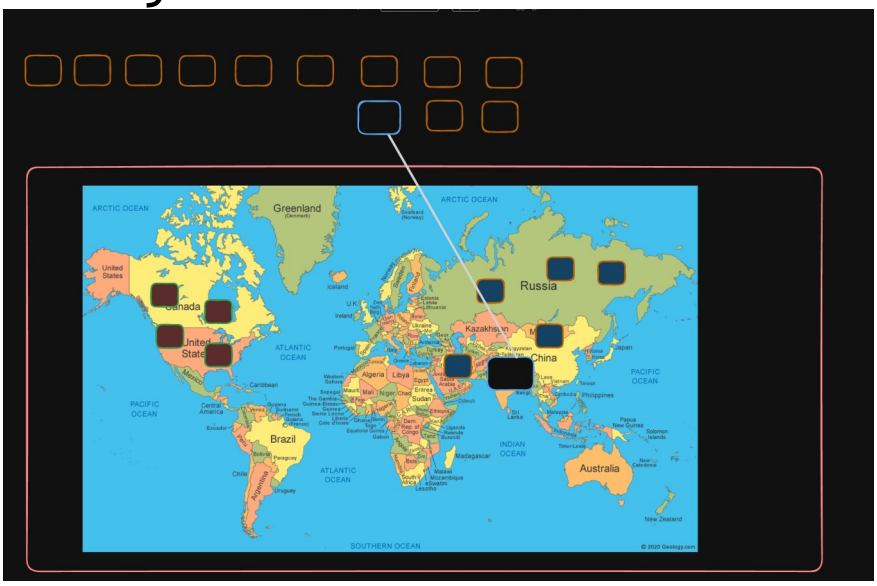


NOW IN THIS WHAT HAPPENED IS A FORK IS CREATED WHICH IS LIKE WHENEVER THERE ARE LIKE IMAGINE TWO PEOPLE IN DIFFERENT LOCATION SAYS THAT I HAVE FOUND THE NONCE AND NOW I AM THE BLOCK PROPER DUE TO THAT LIKE IN RUSSIA ONE NEW CHAIN HAS STARTED AND IN US ONE NEW CHAIN HAS STARTED WHERE THERE IS SOME ANOTHER BLOCK PROPSER AND IT CAN ALSO CONTAIN DIFFERENT NUMBER OF TRANSACTIONS
SO AFTER SOMETIME WHEN A CHAIN BECOME BIGGER THE SMALLER CHAIN DISCARD THERE BLOCKCHAIN TRANSACTIONS AND THEN KEEP THOSE TRANSACTIONS IN THE MEMPOOL AND THEN JOIN THE BIG TRANS CHAIN
NOW THE REJECTED TRANSAC IN THE BLOCK WHICH WAS REJECTED GET REMOVED , SO WHENEVER YOU DO A TRANSAC YOU SHOULD WAIT FOR LIKE 5 BLOCKS TO GET PASSED SO ENSURE THAT THE FORK IN WHICH WE WORKED WAS THE LONGEST ONE ONLY AND THE TRANS WAS NOT REJECTED

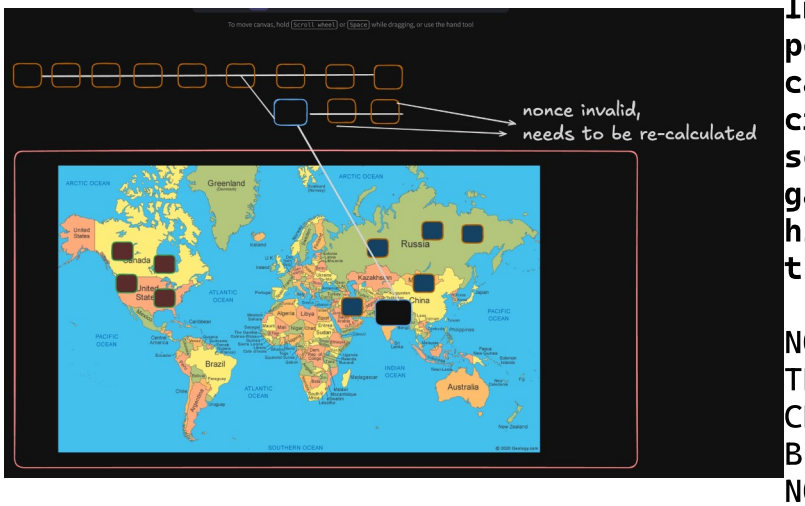
How to forks get resolved?

Eventually one fork will start to become longer, and broadcast this fork to the miners currently maintaining the other fork. The other miners will then accept the longer fork and discard their original fork. This happens automatically and rarely does a fork sustain for more than a few hours

- Can a transaction ever be reversed? Can you ever create a new fork that doesnt have a transaction that you want removed from the blockchain?



A blocks nonce is generated with the txn signature of the prev block attached. You will have to compete with everyone else creating the longest chain while you try your best to create a fork.

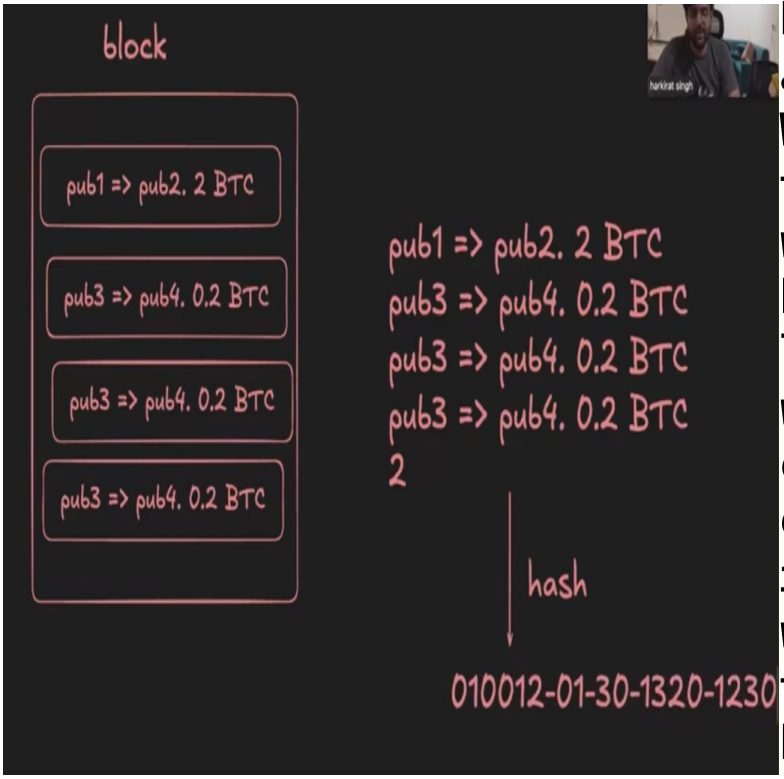


Imagine when a person did a deal with a person in exachange of a btc he got a camera and after that tran 2 blocks were created so no issue in that
so when the person left the person who gave 2 btc created a new block with not his transaction and told everyone to use this block is this possible?

NO BECAUSE WHILE MAKING A BLOCK WE NEED THE PREVIOUS HASH ALSO AND IF WE TRY TO CHANGE THE BLOCK IN BETWEEN ALL THE NEXT BLOCK WILL ALSO CHANGE AS ONE TRANS WAS NOT INCLUDED WHICH WILL CHANGE THE HASH SO FOR THAT YOU HAVE TO CALCULATE THE PROFF OF WORK FOR THE NEXT BLOCKS ALSO WHICH IS NOT POSSIBLE SO THIS IS THE ISSUE IN THIS APPROACH

THAT IS WHY THE PREVIOUS BLOCK HASH IS INCLUDED IN EVERY BLOCK MINING

WHAT PUZZLE THE MINER HAS TO SOLVE TO GET THE INCENTIVE OF THE BITCOIN BLOCK?



Previous block has also added+
With all the transaction they have to find a number which when hashed find a hash which starts with like 20 0’s the number which we are finding is called as nonce and who ever finds this get a reward and there block will be proposed
they will be called as block propser