WHAT IS BLOCKCHAIN?

1. What are blocks?

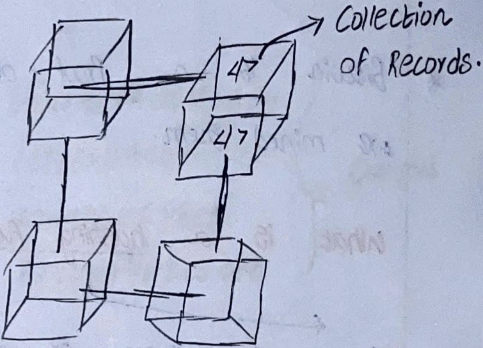
When it comes to blockchain, the blocks are what makes it up.

→ Simply put, blocks are just a collection of data.

In terms of Bitcoin, this data is transactions from one account to another account.

In terms of Ethereum, it's transactions AND Smart Contracts

Blocks are usually not that big, and how fast they are created is determined by the blockchain.



Bitcoin's 'block-time' is 10 minutes.

Ethereum's 'block-time' is 10 seconds.

2. What is the chain's part?

Every block starts with a very important piece of data.

A summary of the last block.

List of Transactions
X pays Y → 50$ A pay B →

After the summary, they include their data, and then they summarize the summary + new data.

[image to be added of 3 blocks, using math]

In this picture, I'm using numbers as the "summaries", because the summaries are actually really messy mixes of numbers and letters. They use math to 'summarize' the data. Here's what a usual summary looks like: "0xe8e341827a0643469086 3b14a6b29ba597c77ab4906"

This way every block has a summary of each block before it.

In Bitcoin, a record of transactions is called **LEDGER**.

record of value exchanging hands.

Blocks do have limits, so we have to keep adding more blocks.

For example, Bitcoin has average around **1500** transactions in block.

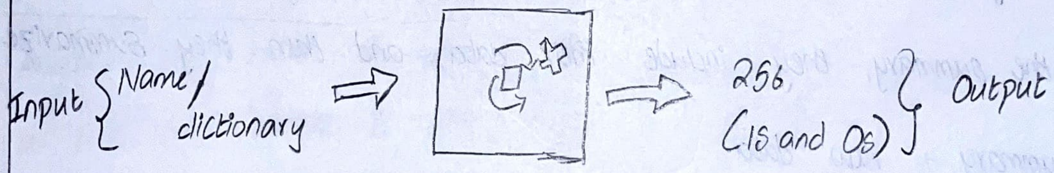
* So, when the blocks are full, we add them to the network

This happens when we mine them.

* Bitcoin is a Proof-of-work model, we have to prove that we mined them.

What is a hashing function?

It is a system or you can put something into it and it will output a hash.



This process involves ton of math.

Bitcoin uses SHA-256 hashing function.

Secure Hashing Algorithm ← SHA - 256 → 0 and 1 that it has in whatever it puts out.

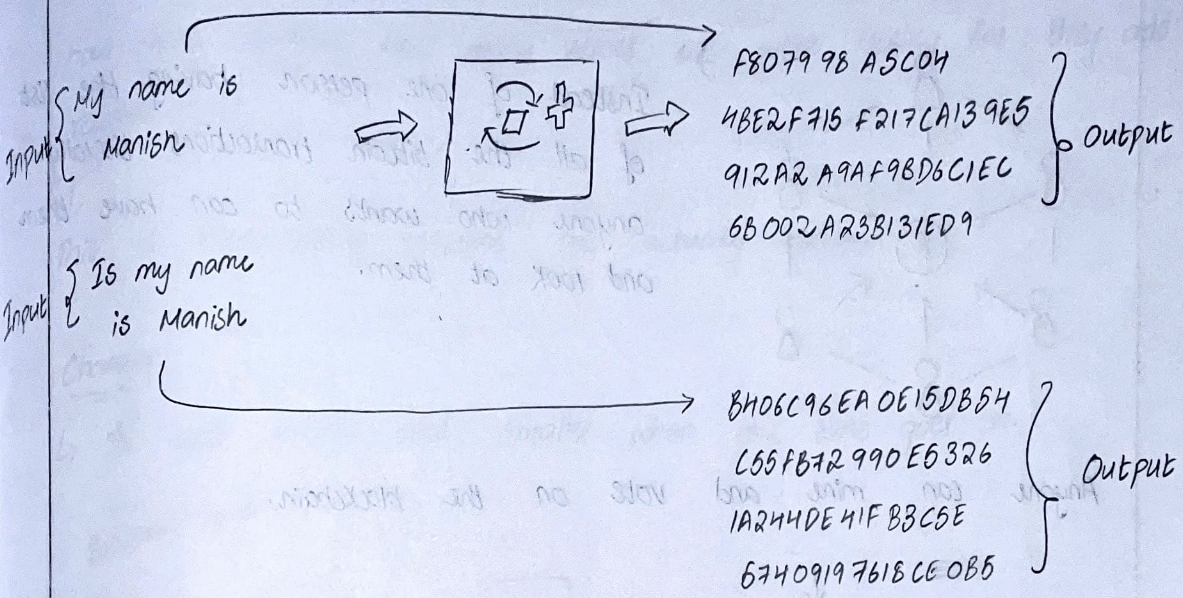
With hashing functions, you need to know three things

With Hashing functions, you need to know three main things:

1. You can't find the input of a hash, you have to guess and check.

2. Changing the input just a tiny bit, changes the output a lot.

↳



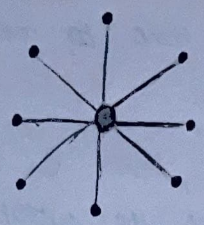
3. Calculating the hash takes some time.

It might only takes (10) millisec to calculate one piece of string of text. But if you a book to check variations it starts to rack up time, and computing power.

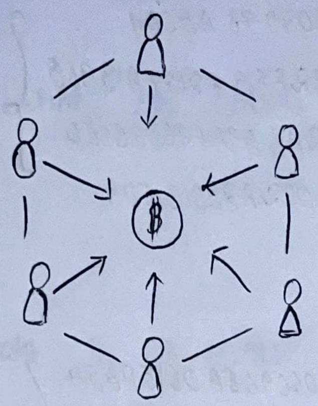
So, In Bitcoin whenever you mine it ~~you~~ will add random numbers to whatever the block is so that we get special ending.

Essentially, Bitcoin is looking for lot more zeroes, and computers all around the world in their mining farms are mining away to find the right number. → When they do we say that block is solved and verified.

Decentralized:



Centralized means one person controls it. For example, our grades in high school, only our teacher had access to our grades.



Instead of one person having the list of all the bitcoin transactions. Literally, anyone who wants to can have them and look at them.

Anyone can mine and vote on the blockchain.

↓

This means they can say Bill really did pay John $50

↓ (or)

They can make fake transactions and John paid Bill all of his money.

So, how do you make sure that someone makes fake transaction and spent all of my money.

↓

This problem can be solved by using asymmetric encryption with cryptocurrency wallets.

Also, in every blockchain you get a reward For participating and putting in good votes.

↓

For example, For mining in Bitoin you get paid in Bitcoin.

→ **The chain**

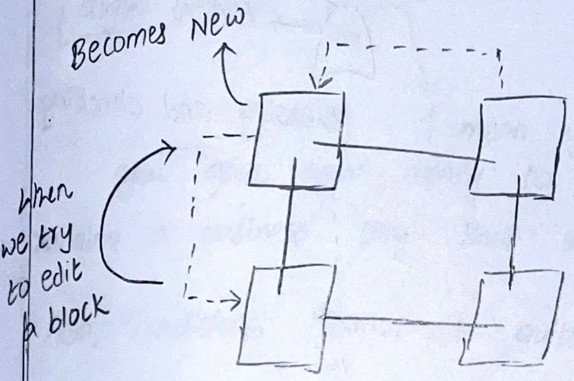
Whoever, solves the block and Finds the magical hash that has how many numbers how many zeroes we were looking For, they add rewards.

↓

This is how many bitcoins are actualy created.

Changes

↳ It gets smaller and smaller when the time goes on.



(They add the hash of the last block to it)

Each block refers to the last one. So, the password of the last block gets added to next block.

Whatever gets added to the Blockchain, it's written down in history forever. As it can't be changed.

↓

This is good For - transactions

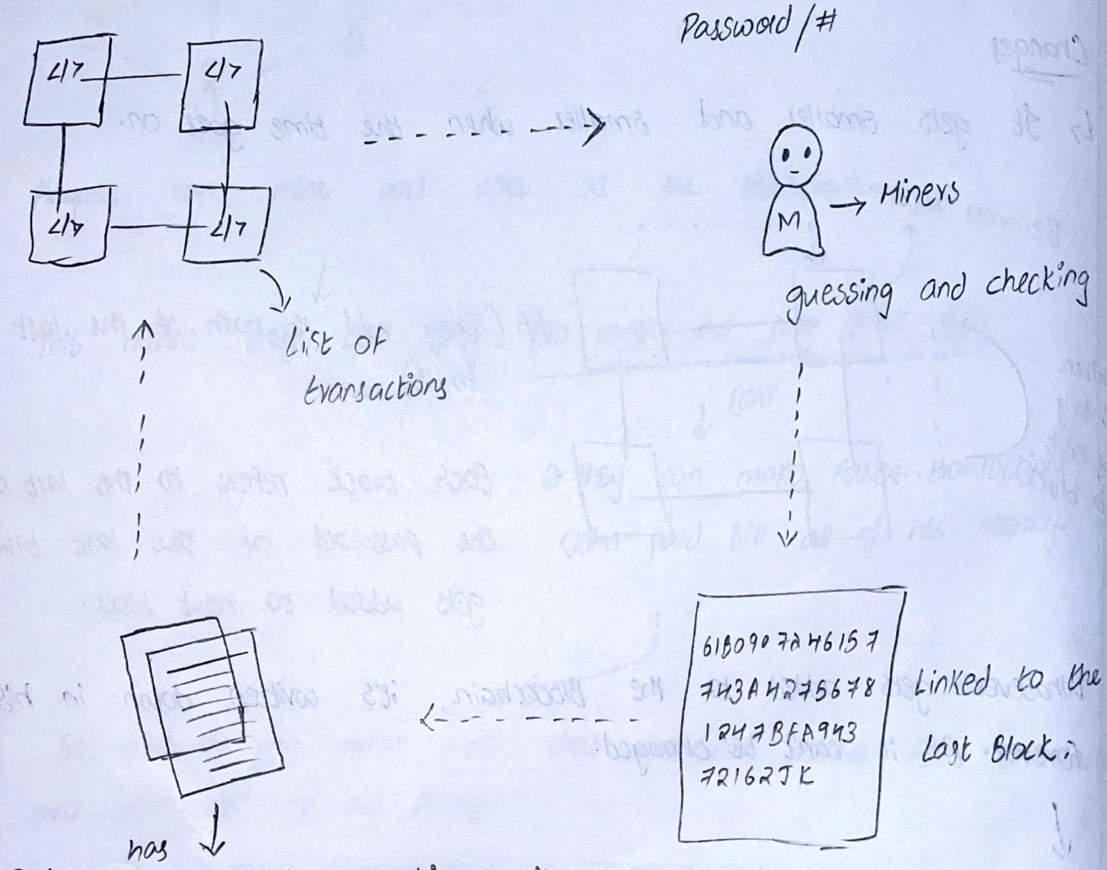
bad For - CopyRight Mateial / Embarrasing things.

In conclusion,

We have blocks that consists of data, and in case of crypto it's usually a list of transactions.

Next, we have a block. We have to ~~have~~ find a password to the block (#) that solves the block and miners do this by guessing & checking.

After they find the solution of the block, they make sure that the linked to the last block. So, each block have history of transactions, because it refers to previous block.



Each block has History of transactions on it.

So, each block is connected with the last block that makes it a chain.