MID-TERM REPORT: BLOCKCHAIN TECHNOLOGY

Nandanmanjunath I 22B0920

Abstract

The topic I selected is blockchain technology and how this technology can be used in Bitcoin. I learnt these topics through the CS765 lecture video and have completed listening to 7 lecture videos till now.
Till now I understood what bitcoin is ,how is it better ,what is blockchain ,what are its basic components and how does it work and why is it used.

Contents

1 WHAT IS BITCOIN

BITCOIN is a type of currency, a digital currency which came after 2009 which was invented Satoshi Nakomoto. Satoshi Nakamoto didn't like the idea of central government having control over monetary because of bad decisions made by government in the past which lead to inflation,Bubbles e.t.c.
Bitcoin currency system is decentralized that is all the members have control over the currency.

2 WHAT IS BLOCK CHAIN AND WHY IS IT USED

I will explain through example and its properties also

Case 1: Suppose a company need to verify your degree certificates. The best way is through offline verification when interview is taken offline and certificate is also checked offline for validity. What if verification should be done online// One way is going through the official website and verifying based on his name being in the list of graduates in a particular batch and department.
But is this legitimate?
One can easily bribe the person who maintains the website to add his name to the list. This is one of the problems that blockchain can solve. In blockchain, once information is entered into a block, it can't be removed or modified. Storing information in blockchain, it is difficult(Almost impossible to tamper the data), and it builds trust on data
Case 2: Suppose a person needs to buy property from another person. This

can be done by exchanging the property documents and money.
In this case, the information should be known whether the person who is selling really owns the property. This can be checked by seeing when this property was bought by this person and checking in later years whether he sold his property or not.
The problem with normal currency is that both transactions cannot occur simultaneously. It is possible that after handing over the property, the other person might refuse to pay and vice-versa.
But by using blockchain technology, both transactions can occur spontaneously(Atomic transaction) **Case 3:** Suppose a person has to send money to another person. Suppose this is an international transaction. In this case, many banks will be involved, and it is transferred through multiple banks to reach the other person finally. In this case, a lot of transaction fee is taken, and also so much time is taken.
But by using Blockchain, transactions can occur very fast, and it will eliminate all of the middlemen.
HOW?
All banks maintain some block-chain(A local copy of their own)and share a single block-chain containing multiple blocks. When a user creates a transaction, this transaction is broadcasted and all banks can view this transaction.Then all banks agree on the block where the transaction is placed. This process is called *Consensus* and after consensus this block cannot be changed permanently and new transactions will be placed in next block.

3 CURRENCY SYSTEM

Here I will be explaining about the olden days currency system and what were its problems and how they updated making better versions. Before starting I will once list all the basic requirements a currency should have

- **Acceptability** Should be accepted by everyone.
- **Durability** Should be lasted longer.
- **Divisibility** Should be easily divisible
- **Fungility** One unit of substance can be exchanged with any other 1 unit of substance.
- **Portability** Can be easily carried.

3.1 Barter System

This was the earliest method. The barter system is when people trade goods or services directly without using money. The problems with bartering were that you needed to find someone who wanted what you had and had what you wanted, there was no agreed-upon value for things, it was hard to divide or move certain items.

3.2 Coins

It built trust for money. They were made with gold and other precious metals.This became the basis unit of transfer. But in Roman Empire when government needed money they started to dialate the percentage of gold in coins to make more coins which lead to inflation and it was one of the reason why the empire collapsed.

3.3 Notes

Newton observed that wear and tear occured to the coins (clipping) and the value of the coins were decreasing. So they decided to print notes(paper) and each note was equivalent to particular quantity of gold and all this gold is stored some where in reserve and instead of directly exchanging gold notes were exchanged.
But in WW1 after germany lost it hd to pay a lot of money to others. So government started printing more money than the gold they had and which lead to inflation(sky-rocketing of prices) and prices went upto 10^{12} times.

After WW2 Bretton Woods agreement took place. Us government had a large reserve of gold and they made an agreement than 35$ is one ounce of gold and they will be circulating 2.5 times the resrve they had.This system will fail if all people come together at once to withdraw gold in exchange of money.

Later during Vietnam War US government need more money and they started printing more money and this created tension to neighbouring countries as the reserve of gold in US is being completely utilised. Many countries decided to return back all the US dollars they had in exchange of Gold.
Currently all countries are using FIAT currency i.e. any ammount of currency can be created by government.
MMT(Modern monetary theory) includes FIAT and setting interest rates by central bank.

Let us come to the basic Question again. **Why currency has value** It has value because it satisfies all the 5 above mentioned properties. But the current currency has many problems. What about alternatives. Bitcoin is one of the alternative. The benifits are very fast transactions can occur and it is a decentralized currency system.

4 Basic Terms to be known

4.1 Inflation

Inflation is when prices of goods and services generally go up over time, causing the value of money to decrease. It's measured by tracking changes in price

indexes. Factors like increased costs and changes in supply and demand contribute to inflation. Moderate inflation can be beneficial for economic growth, but high inflation can harm the economy and people's standard of living.

4.2 Bubbles

It is a situation where the prices of certain assets, such as stocks, real estate, or cryptocurrencies, become significantly inflated, detached from their underlying intrinsic value. This price surge is often driven by speculative buying and market optimism, rather than the fundamental value of the asset. As the bubble grows, more investors join in, expecting prices to continue rising and hoping to make a profit. However, bubbles are unsustainable, and eventually, the prices reach a point where they can no longer be justified, leading to a sharp decline or crash in prices, often resulting in significant financial losses for investors.

4.3 Proof of work

Proof of Work (PoW) is a consensus mechanism used in blockchain networks, such as Bitcoin, to validate and secure transactions. It involves miners competing to solve complex mathematical problems to add new blocks of transactions to the blockchain. The process requires significant computational power and energy consumption.
To participate in PoW, miners must invest computational resources and solve a mathematical puzzle by repeatedly guessing a solution until they find one that satisfies the required criteria. The solution, known as the "proof," is then shared with the network and verified by other nodes. Once verified, the miner's block is added to the blockchain, and they receive a reward in the form of newly minted cryptocurrency(Bitcoin).

4.4 Demand-Supply

Demand refers to the quantity of a product or service that consumers are willing to purchase at various price levels, assuming other factors such as income and preferences remain constant. It is influenced by factors such as price, consumer preferences, income levels, availability of substitutes, and overall economic conditions. Generally, as prices decrease, the quantity demanded tends to increase, while higher prices lead to a decrease in demand.

Supply, on the other hand, represents the quantity of a good or service that producers or suppliers are willing and able to offer for sale at various price levels. It is influenced by factors such as production costs, technological advancements, resource availability, and market conditions. As prices rise, producers have an incentive to supply more of the product, leading to an increase in supply.

The interaction between demand and supply sets the equilibrium price and quantity in a market. When demand exceeds supply, there is a shortage, and prices tend to rise. Conversely, when supply exceeds demand, there is a surplus,

and prices tend to fall. The equilibrium occurs when the quantity demanded equals the quantity supplied, resulting in a stable market price.

5 What are required for functioning of Bitcoin

The basic things for bitcoin to work are

- **DEMAND/SUPPLY**
- **Double spend** no one can use the same money more than one time.
- **Anonymity**All are connected to some network where they interact and each one knows how many bitcoins others have(decentralisation) but they don't know who in real life has those bitcoins. each person is identified by his public private key.
- Hash functions, P2P(peer to peer network), Public private key, Proof-of-work. I will explain all these in detail.

6 Peer to peer network

I will explain different type of networks with example.

Case 1: consider a case where all the people in a network are connected to a central server. Suppose a person A in this network has a songA and a person B wants that song.In this network first SongA must be sent to server and then to person B. But in this network many companies faed losses as A was directly selling the song to B.

Case 2: A Distributed Hash Table (DHT) is a way for computers in a network to find and share information with each other without relying on a central server. It works by dividing data into smaller parts and assigning unique labels to them. Each computer in the network keeps track of certain parts of the data based on their labels. When a computer needs to find or store data, it asks the other computers that are responsible for those specific parts. This helps distribute the workload and makes the network more reliable and efficient.
Suppose if there are N nodes in a P2P network then it takes log(N) steps time order to find a particular file from the network. It initially ask its neighbours and if it is not able to find it asks its next nearest tables and so on until it finds the file in an network.

Bitcoins peer-to-peer network
When a user initiates a Bitcoin transaction, it is broadcasted to all the nodes in the network. The nodes then validate and verify the transaction using consensus mechanisms like Proof of Work (PoW) .Once the transaction is confirmed by the network, it is added to a block, forming a part of the blockchain.

In a P2P network, each node has a copy of the blockchain, which contains a record of all Bitcoin transactions. This ensures transparency and prevents a single point of failure. If a node goes offline, the network remains functional as other nodes continue to operate.

The P2P nature of Bitcoin also extends to other aspects, such as the mining process. Miners, who are nodes with powerful computers, compete to solve complex mathematical problems to validate transactions and add new blocks to the blockchain. This decentralized mining process helps secure the network and maintain the integrity of the blockchain.

7 Structure of a blockchain

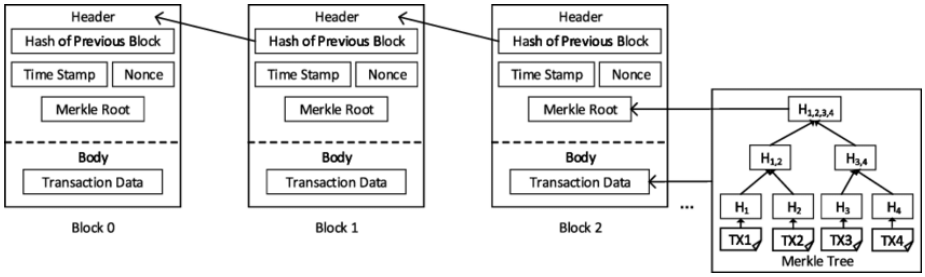

Figure 1: Structure of block chain

A blockchain is composed of multiple blocks. Each block typically contains a list of transactions or data, along with a unique identifier called a hash. The hash is generated based on the contents of the block and serves as a digital fingerprint, ensuring the integrity and immutability of the block. Each block in the chain contains a reference, known as a hash pointer, to the previous block in the chain. This creates a sequential link between the blocks, forming a chain-like structure. I will explain all these parts.

8 Hash Function

It is a function which on giving an input gives an output of fixed size. There are many types of hash functions but they should satisfy certain conditions in order to be used.

8.1 Properties of hash function

- Input is of any size
- Output is of fixed size
- Output is effieciently computed

8.2 Additional Properties

8.2.1 Collision resistance

A function (H) is collision resistant if it is computationally infeasible to find two inputs x_1 and x_2 which are unequal such that H(x_1)=H(x_2) Computationally infeasible means it takes so much time and resources to find two such inputs.

8.2.2 Hiding

A hash function H is said to be hiding if when a secret value r is chosen from a probability distribution that has high min-entropy, then, given H(r||x), it is infeasible to find x. Here r||x stands for r concatenated with x. This can be used such that r is a key and x is a message and this can be used to encrypt the message.
high min-entropy: means that the distribution is very spread out, so that no particular value is chosen with more than negligible probability. min-entropy is defined as max of $-\log_2 P(r_i)$ where $P(r_i)$ represents probability of getting r_i from a probability distribution

8.2.3 Puzzle Friendliness

A hash function H is said to be puzzle friendly if for every possible n-bit output value y, if k is chosen from a distribution with high min-entropy, then it is infeasible to find x such that H(k||x) = y, in time significantly less than 2^n
If a hash function is puzzle friendly, then there is no solving strategy for this type of puzzle that is much better than trying random values of x
Proof-of-work
NONCE is a term that stands for "number used once." It is a random or arbitrary value that is used only once in a specific cryptographic operation, such as the mining process in a blockchain.
The Hash function will run until the output of the hash function willbe less than some value known as threshold value.The hash function can be changed by changing input by adding nonce to it and the hash function will run until the condition is satisfied

9 Working of Hash Function and Merkel Tree

Let the input given to hash function be M bits.

It divides the input into groups of 512 bits. Each group of 512 bits is passed into a compressor function which has two inputs, initialisation vector and the 512 bit message and the output is 256 bit message. This output is again send into the compressor function with the 512 bit message be next part of the message and initialization vector be output obtained before. This compressor function will run until the complete message is sent through the compressor function.

What if the size of the message is not a multiple of 512. Then it will add 1 followed by zeroes till end and in next 512 bit group it will represent the message size.
Due to this way of sending message the input for all the possible different messages will be different and no two messages will have same output.

9.1 Merkel Tree

Suppose the message contains transaction information in it. Suppose we place all the transactions in the message side by side and hash function is applied to this message. What if some information is wrong in it and we have to add or edit or remove some transaction. If we place all the information side-by-side we have to apply hash function again to this new message even if there is a small change and it is time consuming.
Merkel Tree is a type of data structure and by using this it reduces the time to find output of a hash function if some data is changed
In a Merkel tree, data is organized in a hierarchical manner, where each level

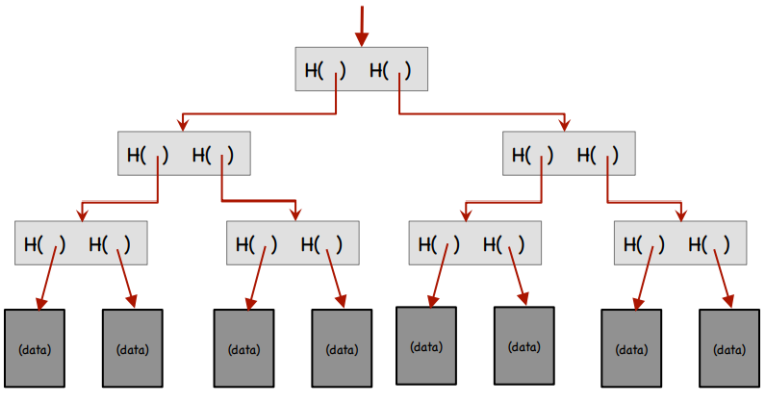

Figure 2: Merkel tree

consists of nodes that are formed by hashing the data from the level below. The bottom level of the tree contains the actual data blocks, such as individual transactions or pieces of data.
If there is a change in a data it take O(logN) to compute data instead of O(N)
The key advantage of a Merkle tree is its ability to efficiently verify the integrity of specific data within the tree. By comparing the hash of a specific data block with the corresponding hashes in the tree, it is possible to verify if the data block is unchanged or has been tampered with. This is accomplished by traversing the tree from the leaf nodes to the root, combining and hashing pairs of nodes along the path.

10 Block-Header

It shows what information is stored in a block

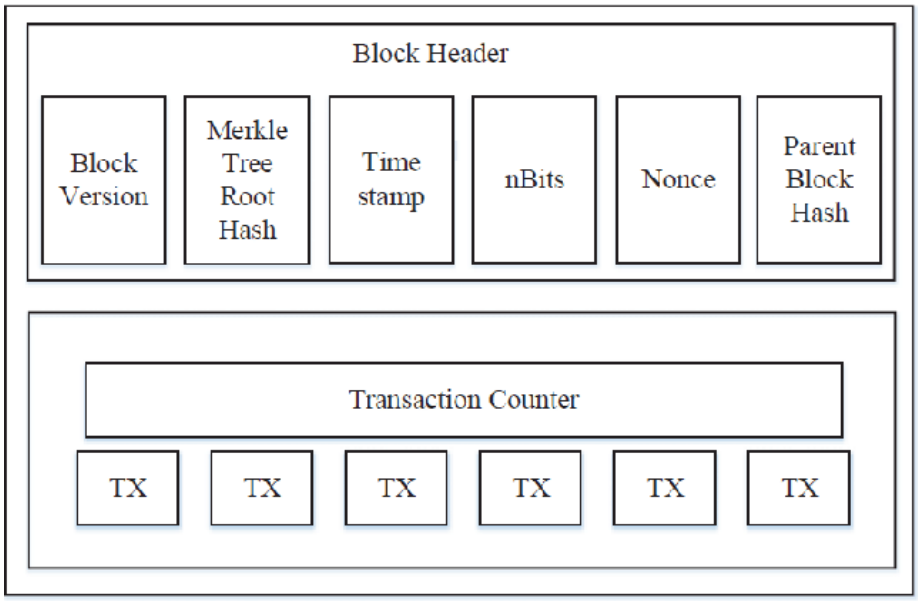

Figure 3: Block-Header

10.1 Bits

It represents the threshold value. It contains 4 bytes b_1 b_2 b_3 b_4 and threshold is given by $b_2 b_3 b_4 * 256^{b_1 - 3}$

10.2 Parent Block Hash

Output of the Hash function from the previous block.

10.3 Timestamp

Represents time taken to find a nonce value such that the output of hash function is less than threshold value.

Light Clients store only the value of block header.

11 Digital signature

A signature should be such that it is easy to create and verify but hard to forge Digital Signature Scheme consists of 3 algorithms:

- (sk,pk) := generateKeys(keysize) generates a key pair
- sk is secret key, used to sign messages
- pk is public verification key, given to anybody
- sig := sign(sk, msg) outputs signature for msg with key sk.
- verify(pk,msg,sig) returns true if signature is valid and false otherwise.

ECDSA (Elliptic Curve Digital Signature Algorithm) is a type of algorithm which generates public privare keys.

12 Bitcoin Transaction structure

Every block in the Bitcoin blockchain contains transactions made by the users. Every transaction records the transfer of Bitcoin from one entity/person to another. We can use these records to trace every Bitcoin to its point of creation. Inputs are the coins the user owns and wants to transfer to another person/entity. Every input has essential subfields to locate and unlock that coin in the Bitcoin blockchain. These fields are as follows:

Previous transaction ID: This is the ID of the transaction in which that Bitcoin was created as output and assigned to the current owner.

Previous transaction index: Every Bitcoin transaction can have multiple outputs (an array of outputs), and every output is identified by a unique index (index of the array). This index, along with the previous transaction ID, can be used to locate the transaction where that Bitcoin was created and to identify its real owner

Outputs are the newly generated Bitcoins locked to the hash of the public key of the payee.
Based on the input value number of Bitcoins a person has can be determined and the output bitcoins is less than or equal to input.
Multiple outputs can be generated from inputs.
Suppose a transaction of 3 bitcoins is done from A to B and A has 3.5 bitcoins. then sum of inputs will be 3.5 and output contains 3 bitcoins transferred to B and the remaining balance added back to public key of A itself.

Transaction Propagation: When a user initiates a transaction, it is broadcasted to the network of nodes. The transaction contains the sender's address, the recipient's address, and the transaction amount.

Transaction Verification: Miners, who are responsible for validating and adding transactions to the blockchain, receive the transaction and verify its

validity. They check if the sender has sufficient funds to cover the transaction and if the transaction adheres to the protocol rules.

Inclusion in the Mempool: Valid transactions are stored in the mempool, a temporary storage area for pending transactions. The mempool acts as a waiting area where transactions await confirmation.

Confirmation and Block Addition: Miners select transactions from the mempool to include in the next block they aim to add to the blockchain. They bundle several transactions together, perform proof-of-work calculations, and create a block.

Consensus and Block Validation: Miners propagate their newly created block to the network. Other nodes validate the block by ensuring that the transactions within it are valid and have not been previously spent. They also check if the proof-of-work calculations are correct.

Chain Extension: If a miner successfully validates and adds a block to the blockchain, it becomes a part of the longest chain. If all the transactions are valid then only the block will become valid and corresponding chain will become valid. If a chain contains an invalid block complete block chain becomes invalid. The other nodes in the network accept the longest chain as the valid version of the blockchain.

If an attacker attempts to double spend by creating conflicting transactions, the network will only accept one of them based on the longest chain principle. The rejected transaction will be considered invalid, preventing *double spending*.

12.1 Transaction Fee

it is the difference of sum of inputs and sum of outputs. To who is it payed. It is payed to the minor who creates a new block. creating a new block needs to solve the problem that is finding nonce to satisfy the threshold condition and this requires commputers and electricity is required.

13 Plan-of-work for upcoming Weeks

I am lagging behind the schedule. I will cover the remaining 20 lectures in the next 3 weeks and read the resources given in the last few Weeks. from now
Week1: 8 lectures
Week2: 8 lectures
Week3: 4 lectures and additional resources
Last week: Additional Resources.

Till now I was not able to do much work because of exams and started all my work after exams.I hope I will be able to complete the tasks mentioned above. Till now I got a basic idea of Block-chain and how it works and what are its benefits. Hope I will learn more about it in upcoming lectures.