SESSION 6

Bitcoin Design

Learning Objectives

- How bitcoin is designed

SESSION 6

Introduction

Earlier, commerce on the Internet depended only on the financial institutions that served as third parties to process payments. However, this system suffered from disadvantages such as transaction costs, limited transaction sizes, the requirement of trust, etc. To resolve this problem, Bitcoin came in the picture. The Bitcoin system is based on decentralization and a trustless environment. Bitcoin uses complex computations to compensate for the trust element employed in centralized systems.

In this session, you will learn how hashing, distributed ledger, digital signature and other concepts are combined together to form Bitcoin. After this, with the help of an example involving four users, you will be made conversant with the evolution of a public ledger towards the blockchain.

Why Bitcoin Was Designed the Way It Was - Part 1

[LO - How bitcoin is designed]

As discussed in previous sessions, Bitcoin is a digital asset and a payment system that allows users to perform transactions without the involvement of any third-party. It is a form of digital currency that is used and distributed in an electronic form. It was introduced in a whiter paper written by Satoshi Nakamoto. In this paper, Bitcoin was described as a "purely peer-to-peer version of electronic cash."

Bitcoin is widely considered as the first modern cryptocurrency. It is a digital currency that does not need any bank or a third-party intermediary to verify its transactions and does not have any authority to manage the accounts. Moreover, every transaction in Bitcoin is extremely transparent. Every transaction is stored in a massively distributed public ledger called the blockchain.

Before the arrival of Bitcoin, currency systems that were used developed from the barter systems. One thing that made these barter systems stable was the trust element. Even, nowadays, people rely on a centralized, trusted third party to process their payments. However, issues such as transaction cost and time taken to settle transactions started occurring. These problems were solved by Bitcoin. Bitcoin is the first cryptocurrency that uses cryptography methods to eliminate the need for trusting intermediary third parties.

Let's take an example. Suppose there are four users, Alexa, Bobby, Charles and David. In order to keep a note of the expenditure between them, they create a common ledger, in which they record all the payments that are made, as shown in Table 1:

Table 1: Example of a Ledger

Ledger	
Transaction Details	**Amount**
Alexa pays Bobby	$50
Charles pays Alexa	$40
David pays Alexa	$40
Bobby pays David	$50

This ledger is stored publicly, and everyone can access this ledger like a website. In this ledger, anyone can add transactions and at the end of the month, the transactions are settled with the real money. The problem with the public ledgers like this is that anyone can add a transaction or make a change in any transaction. Suppose, Charles made a change in a transaction in the ledger stating that Bobby pays Alexa without any approval from Bobby, as shown in Table 2:

Table 2: Tampered Ledger

Ledger	
Transaction Details	**Amount**
Alexa pays Bobby	$50
~~Charles~~ Bobby pays Alexa	$40
David pays Alexa	$40
Bobby pays David	$50

Now, the problem is how to trust these transactions and ensure that they are true and updated correctly. This problem is solved by digital signatures.

Just like handwritten signatures, digital signatures help in preventing any forgeries. As you have already studied in Session 4 that a digital signature uses a public and private key pair and signs the document to provide authenticity to a digital document. A user signs a document by using his/her secret key and in return, the signature can be verified by the corresponding public key. When a user signs a message using his/her digital signature, he/she also hashes the message to protect the integrity of the message.

Let's understand the mechanism by which Bobby actually signs the message. He creates a unique fingerprint of the document being signed, called a hash. He then encrypts this hash with his own private key and bundles it along with the document and his public key. Anyone interested in verifying the authenticity of the document, i.e. ensuring that it

is indeed Bobby who signed the document, takes Bobby's public key and decrypts the encrypted hash. If this decrypted hash matches the hash generated from the document by the verifier, it is guaranteed that Bobby had signed the document in the first place.

Let's go back to the public ledger. Now, let's update this ledger with the corresponding digital signatures of the users, as shown in Table 3:

Table 3: Ledger with Signatures

Ledger		
Transaction Details	**Amount**	**Digital Signature**
Alexa pays Bobby	$50	Alexa (01100001.....)
Charles pays Alexa	$40	Charles (01100011.....)
David pays Alexa	$40	David (01100100.....)
Bobby pays David	$50	Bobby (01100010.....)

However, signing their transactions is a good option but what happens if a user copies the signed message as many times as he/she wants. Therefore, it is necessary to have a unique ID (also known as a "nonce") to be attached to every transaction. Whenever a user signs the transaction, he/she should also sign the unique ID associated with that transaction.

Suppose, Bobby copies Alexa's transaction multiple times in the ledger. If there is a nonce associated with Alexa's transaction, every transaction will have a different digital signature signed by Alexa, as shown in Table 4:

Table 4: Ledger with Unique ID

Ledger			
Unique ID (nonce)	**Transaction Details**	**Amount**	**Digital Signature**
0	Alexa pays Bobby	$50	Alexa (01100001.....)
1	Alexa pays Bobby	$50	Alexa (1001100011.....)
2	Alexa pays Bobby	$50	Alexa (11100100.....)
3	Alexa pays Bobby	$50	Alexa (011110010.....)

Digital signatures help in removing a huge aspect of trust in the original ledger system. However, if this method is still being used, there is still some trust required as users need to trust other users that they will follow up and settle the ledger using cash at the end of the month.

Suppose a user is in debt of hundreds of dollars and does not agree for the settlement. The solution to this problem can be simply not allowing anyone to spend more than they have put in the first place. For example, in the previous case, each user deposits some amount of money. If a user tries to spend more than he/she has deposited, then that transaction will automatically get rejected.

For example, Table 5 shows a ledger in which each user deposits 100 dollars.

Table 5: Ledger with a Deposit

Ledger			
Unique ID	**Transaction Details**	**Amount**	**Digital Signature**
0	Alexa deposits	$100	
1	Bobby deposits	$100	
2	Charles deposits	$100	
3	David deposits	$100	
0	Alexa pays Bobby	$50	Alexa (01100001.....)
1	Charles pays Bobby	$50	Charles (1001100011.....)
2	David pays Alexa	$50	David (10010100011.....)
3	Charles pays David	$50	Charles (11100100.....)
~~4~~	~~Charles pays Alexa~~	~~$25~~	~~Charles (011110010.....)~~

Now, when Charles tries to spend more than he has deposited, his transaction will get rejected automatically. In order to verify a transaction, it becomes necessary to know the complete history of transactions which can be exhausting.

Why Bitcoin Was Designed the Way It Was - Part 2

[LO - How bitcoin is designed]

Suppose if everyone started using public ledger without even spending cash in real life. They can send or receive money on this ledger without even converting it to real money. Let's suppose that the money on this ledger will be known as LedgerCoins. Users can exchange real money with LedgerCoins. Suppose, Bobby pays Charles 100 dollars in the real world to add and signs a transaction on the ledger saying Charles pays Bobby 100 LedgerCoins.

This concept has given rise to the concept of distributed ledger which forms the backbone of Bitcoin or any other cryptocurrency. It means that cryptocurrency is a ledger and the history of transactions is the currency. However, one of the biggest differences between this public ledger, which is being discussed, and the distributed ledger is that the public ledger is centralized, and the distributed ledger is decentralized.

The public ledger exists in a public place such as a website where anyone can add new lines. This website or a public place would need an authority who will host and manage the website. This means that users are required to trust the authority. In order to create a trustless environment, distributed ledgers are implemented. A distributed ledger is a database that exists among multiple participants of a network. It means that every user

will have their own copy of the ledger. Whenever a user wants to add a new transaction, he/she will broadcast it and also record in their own ledgers, as shown in Figure 1:

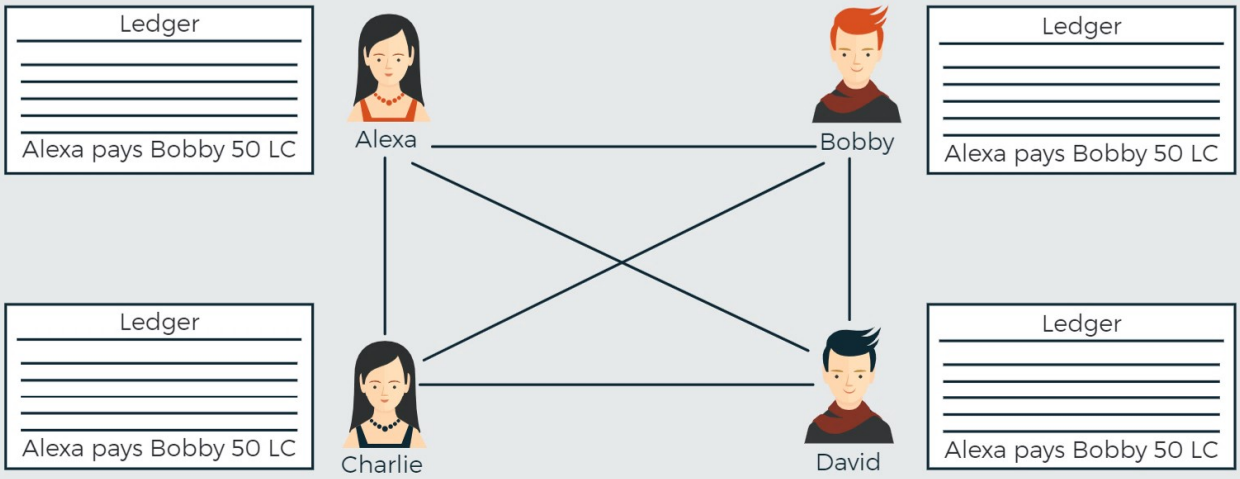

Figure 1: **Distributed Ledgers**

However, one main problem with distributed ledgers is how anyone can be sure that everyone is receiving the broadcast of transactions and recording those transactions in the same manner. Suppose the original transactions and their order are as follows:

Alexa pays Bobby 50 LC

Charles pays Alexa 40 LC

David pays Alexa 40 LC

Bobby pays David 50 LC

However, the users did not record the transaction in the same manner and in some scenarios, they do not even record the transaction, as shown in Figure 2:

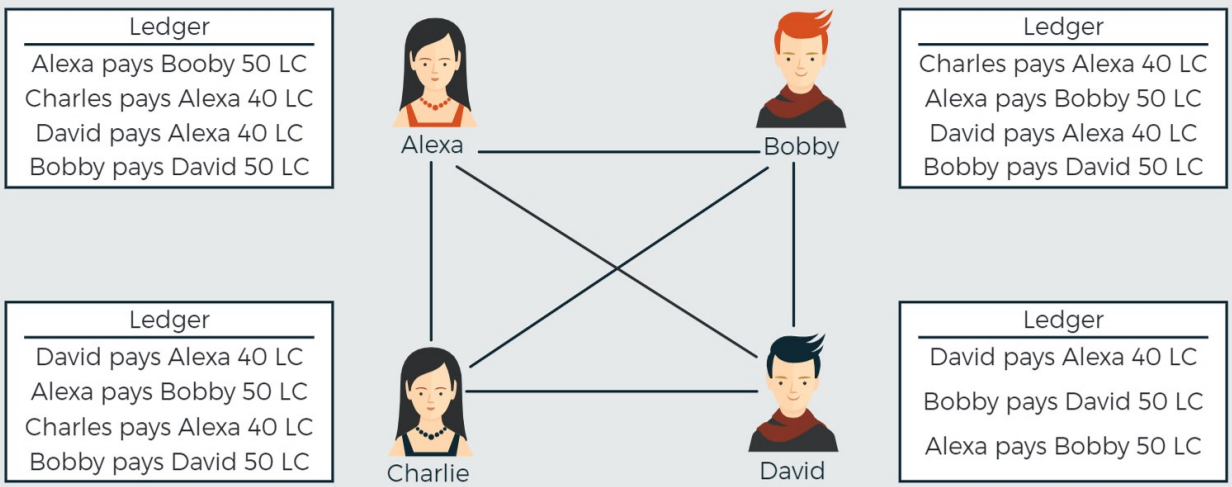

Figure 2: **Problem with Ledgers**

As shown in Figure 2, every user recorded the transactions in their ledgers in a different manner and one of them did not even record one of the transactions. Now, the problem arises as to which version of the ledgers should we trust.

The solution to this problem of distributed ledgers has been addressed in the original Bitcoin paper. The solution provided in the paper says that whichever ledger has the most computational work performed will be the most trusted ledger. This brings to the usage of hashing in cryptocurrencies. You have already learned about hashing in Session 4.

Hashing is a technique that transforms data or a string of characters into a short and fixed length value which represents the original data. This value is called hash or message digest or hash key, which is unique. It is infeasible to find a message on the basis of a given digest. In the Bitcoin blockchain, SHA-256 is mainly used that provides a hash value of 32 bytes.

Now, let's focus on making a connection between distributed ledgers and hashing functions. Suppose a user shows you a list of transactions and says that he/she has calculated a special number which, when added to the transactions, will calculate a hash value starting with four zeros, as shown in Figure 3:

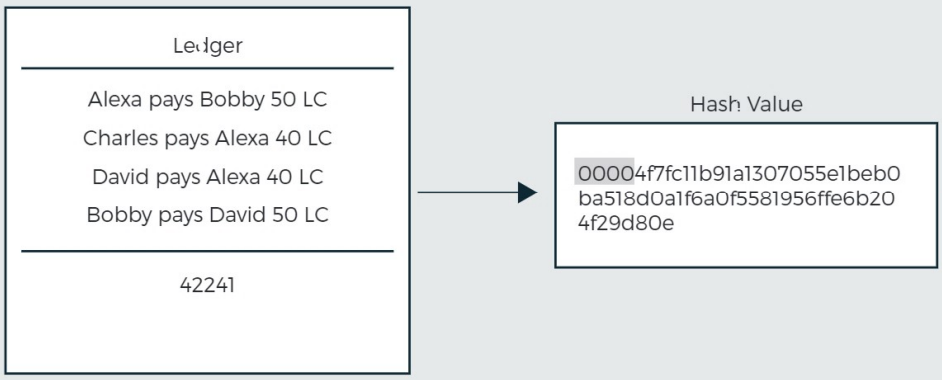

Figure 3: **Hash Value of a Ledger**

Let's find how many attempts it would have taken the user to find that number. It would have required him/her to make a lot of guesses to find that number. The probability of finding a hash that starts with four zeros is about one in a billion. It is impossible to find a specific message from billions of messages based on their hash values. He/she must verify many messages before finding the message with a specified hash value.

However, it is relatively easy to verify if the computation is correct. This is known as proof of work. It means that if anyone even makes the slightest change, then the hash value will be changed, and that person will need to go through another billion guesses to find that number or new proof of work.

Now, let's go back to the distributed ledger condition, where every user is broadcasting transactions and storing them. The problem is to find which user has a correct ledger. The solution to this problem is provided by the ledger which has performed the maximum amount of work.

Let's understand its working. Let's organize a ledger into some blocks where each block will have a list of transactions together. The blocks will also contain proof of work as a special number so that the hash of the whole block starts with a bunch of zeros, as shown in Figure 4:

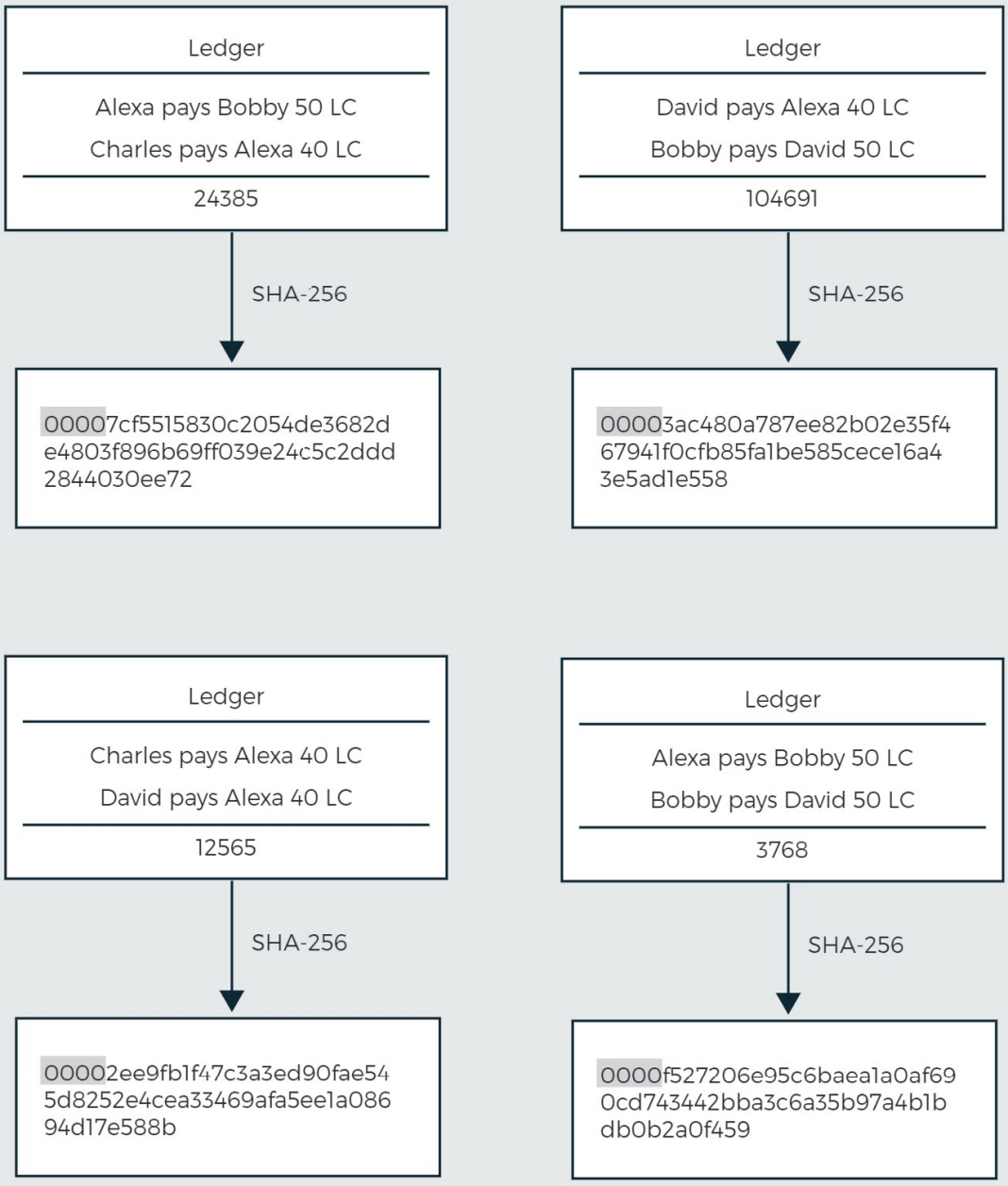

Figure 4: **Ledger Blocks**

As shown in Figure 4, each ledger block has a number which provides proof of work. This number ensures that the hash value of each block will only be started with four zeros.

As you have already learned, a transaction is considered valid if it is signed by the sender. Similarly, a block is only considered valid if it has been validated by using a proof of work. Now, in order to ensure that there is a standard order between these blocks, each block should contain the hash value of the previous block in its header, as shown in Figure 5:

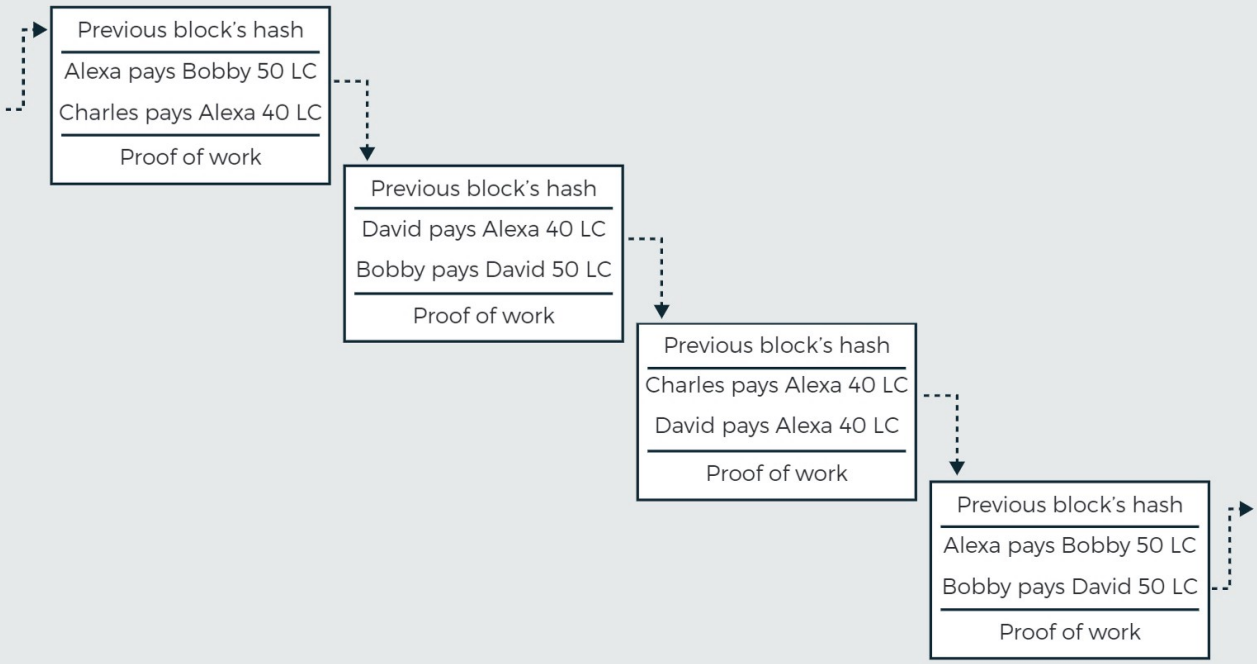

Figure 5: **A Chain of Blocks**

In case any change is made in a previous block or blocks are swapped; it will affect all the succeeding blocks. Now, in order to make all the blocks valid again, you would need to find a new number for each of these blocks that makes their hashes start with four zeros. This is an ever-increasing task as the number of blocks being mined by others will keep increasing, and this makes it very difficult to "rewrite" the blockchain. This chain of blocks secured in this manner is known as a blockchain.

When transactions are being broadcast, anyone can listen to them, collect them into a block and then perform proof of work for that block. That person is known as a miner. After performing the proof of work for that block, miners broadcast the block. As a reward to perform all the work, they add a special transaction on the top of the block. This is known as a block reward. This complete process of creating and validating a block is known as mining.

Now, going back to the example, every user can start listening to blocks being broadcast by miners instead of transactions and updating their blockchains. In case, users come across two distinct block chains with conflicting transaction histories, then they should prefer a blockchain that has performed the maximum amount of work. No central authority and everyone maintaining their own blockchain helps in reaching a decentralized consensus.

All the concepts discussed till now conclude the working of all the cryptocurrencies.

SUMMARY

- Bitcoin is a digital currency that does not need any banks to verify its transactions.
- The problem with public ledger is the amount of trust needed to manage the ledger.
- Digital signatures ensure that the transactions are true and updated correctly.
- A problem with digital signatures is that they can be copied infinitely. This problem was solved by a unique ID.
- Earlier ledgers were managed by a central authority which required the users to trust an intermediary. This problem was solved by decentralization.
- In a distributed ledger, users broadcast their transactions and update their ledgers by listening to other ledgers.
- Hashing solved the problem of deciding the most trusted ledger among ledgers having various versions.
- A transaction is considered valid if it is signed by the sender. Similarly, a block is only considered valid if it has been validated by using a proof of work.
- Each block of transactions has the hash value of the previous block so that any change made in the previous block will affect all the succeeding blocks.