SESSION 12

Blockchain - The Underlying Technology

Learning Objectives

- Discuss how blockchain is considered as a store of value
- Describe how data is stored on a blockchain
- Explain how to secure data on a blockchain
- Discuss the limitations of blockchain

SESSION 12

Introduction

The real world is full of assets such as stocks, real estate, gold, carbon credits, oil, etc. Most of these assets are difficult to transfer or trade physically, so most buyers and sellers trade on paper. However, paper and legal agreements can be hard to track and difficult to follow. A solution to this problem is to switch to a digital system similar to Bitcoin but attached to an asset. With the excessive overhead of standardized agreements, major startups and financial companies are now moving towards tokenization. Tokenization is defined as the conversion of physical assets into a digital token on a blockchain.

Suppose, Alexa has diamonds having a worth of 15 million dollars. Diamonds are difficult to trade as they require security and careful inspection to ensure that fake diamonds are not introduced. Bobby wants to invest in diamonds but does not want to deal with any issues related to their trading. Therefore, Alexa subdivides the stocks of her diamonds and sells fractional pieces of it. Now, Bobby can easily trade his fractional ownership to other people. This is an example of how blockchain tokens represent real-world assets.

In this session, you will learn how blockchain is considered as a store of abstract value. You will also learn how data is stored on a blockchain. After this, you will gain insights into how to secure data on a blockchain. Towards the end of this session, you will be made conversant with some of the limitations of blockchains.

Viewing Blockchain as a Store of Abstract Value

[LO - Discuss how blockchain is considered as a store of value]

From its development in 2008, blockchain has developed into a very flexible technology. Its implementation has moved far from cryptocurrencies and is not only limited to Bitcoin anymore. It has become so versatile and efficient a technology that it can serve multiple functions from streamlining services to enhancing security.

Nowadays, financial transactions are a very complex process. Now, digitization is being used to speed up the process of sorting information in private databases. Smart contracts using blockchains are being used to create complex and secure legal agreements. With

the transparency and security of distributed ledger, it is now possible to create a direct connection between the two parties by removing all the intermediaries.

Bitcoin and other cryptocurrencies have revolutionized the financial industries by tokenizing and decentralizing money. With more advancements in blockchain, it can now not only tokenize and decentralize money but also real and financial assets. Now, it is possible to liquidate literally anything. Tokenization allows investors to trade on real and financial assets without any complexity.

Tokenization helps in changing the concept of ownership. It allows us to convert anything from ideas to paintings to buildings into tokens and freely trade these assets on the blockchain. Blockchain provides a way to revolutionize paper markets by dramatically reducing costs and paperwork and circumventing the middlemen.

Now, let's understand tokenization. Tokenization is a method which is used to convert any real-world asset into a token that can be traded, stored or recorded in a blockchain system. It allows the user to convert the value stored in any object into a token which can be used on the blockchain. The object can be a physical object like a property or painting or even an intangible object like carbon credits.

Nowadays, everything owned by a user such as a car, a house, an investment portfolio or cash in the bank is tied to his/her name. Generally, assets owned by a user are either illiquid or difficult to trade. With the help of tokenization, the asset can be broken into pieces. After this, a stock can be created, or a single proof of ownership can be tied to an asset.

For example, suppose you own a home worth 1 million dollars. With the help of tokenization, you can break the ownership of the home into 100 tokens each having a worth of 10,000 dollars or 1000 tokens each having a worth of 1,000 dollars. It allows you to sell the partial ownership of your home without any third-party or intermediary.

Although blockchains can tokenize any asset, these assets can be broadly categorized into three categories:

- **Intangibles**: Suppose, company X wants to transfer the design of a mobile app to company Y. The two companies are located in two different geographical locations. Tokenization allows transferring the rights of this asset to company Y in a safe manner using smart contracts. The transfer will be immutable, verifiable and almost instantaneous.

  Blockchain allows the tokenization of intangible assets as they are difficult to evaluate. The intangibles include things like patents, trademarks, brand recognition, copyrights and goodwill. Blockchain makes intangibles more financially perceivable and provides a guarantee of their legitimacy.

- **Fungible goods or fungible assets**: Fungible goods are the goods, securities or instruments which are equivalent and can be interchanged. Fungible goods possess identical qualities which help in exchanging one fungible item for another identical item of equal value. Fungible assets are supported by the physical resource which makes them difficult to trade. For example, the transfer of 1,000 tons of steel. Tokenization simplifies the process and removes any intermediaries.

- **Non-fungible goods or non-fungible assets:** The previous example of selling partial ownership of your home is an example of tokenization of non-fungible goods. The best use case is art, real estate or CryptoKitties.

  When a property or a piece of art is tokenized, a digital signature is attached which is unique and cannot be changed. The token representing an asset can be split into many sub-tokens that have their own unique digital signatures. It means that shares of any real estate or work of art can be traded in the form of crypto assets.

Introducing Data Storage on Blockchain

[LO - Describe how data is stored on a blockchain]

Cryptocurrencies such as Bitcoin use blockchain to provide new forms of currency. They store transactions as digital packs of data within blocks. They can also be used to store other forms of data.

Some of the reasons why blockchain should be used to store data are:

- **Tamper resistance**: One of the major benefits that a blockchain provides is immutability. Blockchain uses cryptography that protects a record from tampering. This tamper-resistance nature helps in preventing fraud related to data.
- **Visibility**: When a public blockchain is used to store data, it becomes visible to the public. After storing a document or its hash on the blockchain, it will be stored on the blockchain permanently. Private blockchains can be used to provide only permanent visibility to a preselected group.
- **Decentralization**: Blockchain provides decentralized data storage features that distribute the data across a network of nodes. It helps in removing trust and the need for providing control over central authority.

However, it is necessary to understand that a blockchain should not be viewed as a store for large data sets or for data that is transient in nature. This is due to its decentralized nature which leads to enormous replication of this large dataset. For example, a 10MB file, if somehow stored on the blockchain, would be replicated by thousands, if not millions of users. This could end up permanently consuming gigabytes of data which is inherently small in nature. Hence, it is not advisable to look at the blockchain as a large data store. There are ways to store large data sets in a decentralized manner without the permanence feature inherent to the blockchain.

Blockchains use a transaction model to store the data. For example, “Alexa pays 50 dollars to Bobby” is a transaction. The transaction stores the addresses of the sender and receiver, and the amount of money transferred. This approach is easy to use and understand when transactions are related to money. However, the challenge arises when you want to store data using this concept. In order to store data on the blockchain using the transaction model, the data needs to be packaged into transactions.

Some blockchains provide the facility to append data to transactions within their protocols. However, if this facility is not available on blockchains, a small amount of data can be stored using addresses. In this method, the data is encoded into the receiving address instead of a payload field inside the transaction. The disadvantage of this technique is that the amount of data to be transmitted cannot be larger than the size of the blockchain address.

Another way of storing data on the blockchain is by storing only the hash of the data in the blockchain. The hash value of a very large data is comparatively smaller, and its transaction cost is also less. You can store the raw data on any relational database and link the hash of the blockchain transaction to the raw data. It helps in utilizing the advantages of traditional storage mechanisms and blockchain. However, by using traditional storage mechanisms, advantages of blockchain such as decentralization and transparency are lost.

The lost advantages can be achieved by storing the hash of the data and parts of data on the blockchain. On the basis of the parts of the data, transparency can be achieved as the data is accessible publicly and decentralization can be achieved as the subset of the data is stored in a decentralized manner.

Another method for storing data in a decentralized way with immutability feature is to use Interplanetary File System (IPFS). IPFS is a protocol which is used to serve information on the web. It is a versioned file system that stores and tracks versions similar to Git. It also defines the mechanism of movement of files across a network which makes it a distributed file system similar to BitTorrent. By using the versioned file system and distributed file system, it helps in creating a new web and improving the way existing Internet protocols are used.

IPFS focuses on creating a new permanent and distributed web. It uses a content-addressed system instead of HTTP's location-based system. For example, an IPFS request would be:

/ipfs/QmIihLIjeg5soif/directory/data.txt

As shown in the given example, instead of using location address, IPFS stores a representation of the content itself in the form of a cryptographic hash value. The hash value points to a root object and other objects that can be located in the path. Instead of requesting for a location, the user asks for a file.

IPFS uses a Distributed Hash Table (DHT) to store data. If you have a hash value of the data you want, you will ask the peer network who has the content located at that hash and directly download the content from the node itself. Suppose a user looking for some content on IPFS finds that some neighbors have access to the content. Then he/she can download small bits of the content from those neighbors. IPFS also uses a Merkle tree to track the content across the entire web.

Now, in the next section, let's understand the security issues with the data being stored on the blockchain.

Securing Data Storage on Blockchain

[LO - Explain how to secure data on a blockchain]

In blockchain, data is stored in the form of events known as transactions. In cryptocurrencies, transactions are used to store scripts which help in transferring assets. Transactions can also contain arbitrary information such as smart contracts. However, it is necessary to ensure that the data stored on the blockchain should not be bulky because the transaction fee is calculated based on the size of the data in the transaction.

The data stored on the blockchain cannot be modified. You should always keep in mind that the transactions take some time for processing in the blockchain network. It is suggested to wait for some block confirmations even if the transaction has been added in the block. In case, a specific data item needs modification frequently, then it will take a lot of time for processing. Most of the nodes may even reject transactions, in case the transactions refer to other unconfirmed transactions. Therefore, it is recommended to store and process such data off-chain.

Another problem with storing data online occurs when you try to store some personal or confidential data. When personal data is stored on a public blockchain, the data will be available to everyone and it is not possible to delete data on the blockchain. One solution can be encryption of data, but then you will have to manage encryption keys and their distribution.

Another threat to the security of data is quantum computing. Quantum computing deals with quantum theory where Qubits (quantum bits) are used in place of bits. Qubits manifest themselves in several states concurrently which implies that they are not mutually exclusive. The performance benefits due to quantum computing can be used to solve complex computing problems. However, it can also be used to break major cryptographic algorithms which are the backbone of blockchain. The immutability in the blockchain is achieved by the difficulty level provided by hashing puzzle. If quantum computing is used to break the one-way property of hashing algorithms, then the public ledger will be compromised very easily.

Quantum computing can pose a great threat to asymmetric cryptography where it can provide the means to compute the private keys from public keys. Sensing these threats, many technology firms have already begun their work to solve them. One such example is of the NEO blockchain that provides a quantum safe (NeoQS) cryptographic mechanism which uses lattice-based cryptographic mechanisms.

It is obvious that quantum computing will create security issues for blockchain technology. However, it is certain that blockchain technology will evolve to secure itself against quantum computing when the need arises in the near future.

Exploring Limitations of Basic Blockchains

[LO - Discuss the limitations of blockchain]

Despite a lot of benefits, blockchain technology also suffers from various challenges. Some of the limitations of blockchains are as follows:

- **Underperformed functionality**: Blockchains cannot handle a large number of transactions concurrently yet. For example, Bitcoin blockchain can only handle seven operations per second. Underperformance makes blockchain less appealing as compared to its existing alternatives. However, this will change in the coming years as significant research is promising more scalable, fast, efficient blockchain solutions.
- **Significant cost:** Blockchain needs high operational cost which becomes a major barrier in its adoption. Even developers do not have enough flexibility. Blockchain does not support free applications.
- **Platform Lock in:** Generally, users and developers are required to select a blockchain on which they will work. It is not easy to switch to other platforms available in the markets. There is no interoperability as of now, though this has become something which new protocols are trying to take care of.
- **Risks of early adoption and the possibility of disrupting existing infrastructure**: Even with all the benefits, the cost of adoption of blockchain technology is a significant risk. This risk is specifically true in cases where complex legacy systems and huge back-office processes are used.

SUMMARY

- Tokenization is a method which is used to convert any real-world asset into a token that can be traded, stored or recorded in a blockchain system.
- Although blockchains can tokenize any asset, these assets can be broadly categorized into three categories—intangibles, fungible goods and non-fungibles goods.
- The reasons why blockchain should be used to store data are its tamper resistant, transparent and decentralized nature.
- A way of storing data on the blockchain is by storing only the hash of the data in the blockchain.
- It is necessary to ensure that the data stored on the blockchain should not be bulky because the transaction fee is calculated based on the size of the data in the transaction.