SESSION 14

Programmable Blockchains - Tokens & Oracles

Learning Objectives

- Explain tokens and their types
- Discuss oracles and their types

SESSION 14

Introduction

Bitcoin and other cryptocurrencies have revolutionized the financial sector by tokenizing and decentralizing money. With more advancements in blockchain, it can now not only tokenize and decentralize money but also other tangible and intangible assets. Now, applications of blockchain are not only limited to digital cryptocurrencies alone. Ethereum is used as a platform to create various DApps and digital tokens. With the help of Ethereum, developers can create tokens for any asset. A token is a representation of an asset or utility on a blockchain.

Another important concept in the blockchain is Oracles. Smart contracts on a blockchain are used to minimize counterparty risk and provide transparency. They can be programmed to make a payment on the basis of any conditions. Sometimes, they need data from the real world, then they take help from oracles. An oracle is an agent that collects data from the real world and provides the information to the smart contracts.

In this session, you will learn about tokens and their types. You will also gain an understanding of the underlying mechanism by which a token gains value. Next, you will be made conversant with the concept of oracles and their types. Towards the end of the session, you will learn about the security issues with oracles.

Introduction to Tokens

[LO - Explain tokens and their types]

A token can be defined as a representation of something in a specific ecosystem. It is not limited to a specific role and can perform various roles in its native ecosystem. Tokens are different from cryptocurrencies. Cryptocurrency such as Bitcoin, Bitcoin Cash, Ethereum etc. can exist outside their native platform and perform their function. However, tokens such as OmiseGO, Golem can only exist on a particular platform which makes them lose their value outside their native environment.

Vitalik Buterin, the co-founder of Ethereum blockchain, defines blockchain tokens as the representation of “a wide range of scarce assets, such as currencies, securities, properties, loyalty points, and gift certificates, among others.”

A token can be defined as an asset or utility that lies on the top of a blockchain. It can represent any asset which is fungible and tradeable. It is distributed among the investors during a public sale known as initial coin offering (ICO). ICO is a type of crowdfunding tool used by decentralized application (DApp) developers to gather the required funding for a project. Anyone can invest in a project by purchasing the tokens of that DApp.

Unlike a cryptocurrency, a token is not native to a blockchain and is created on top of a blockchain. A token is governed by a smart contract. For example, on Ethereum, tokens are governed by smart contracts that follow a common standard known as ERC20.

Blockchain tokens can represent various assets other than currencies. Some tokens are used in crowdfunding campaigns and some are used as ownership stakes. With the ability to create tokens, now developers can tokenize projects and sell blockchain tokens to fund projects. This has given rise to a new way of fundraising, which is known as ICO.

Figure 1 shows various aspects of blockchain tokens:

Figure 1: **Various Aspects of Blockchain Tokens**

Types of Tokens

According to the U.S. Securities and Exchange Commission (SEC) and Swiss Financial Market Supervisory Authority (FINMA), the tokens can be classified into two main categories:

- **Security tokens**: They are also known as asset token in FINMA. This category represents ownership of a real-world asset. They are similar to equities, bonds or derivatives. They use a blockchain system to determine the ownership rights of an individual. Blockchain Capital is a security token of a venture capital firm investing in blockchain technology companies. Slice is a real estate security token which offers fractional ownership in US Commercial real estate to its investors.
- **Utility tokens**: Utility tokens are the tokens which are used for a specific purpose. They provide future access to an organization's products and services. They are a type of discount coupon or premium access to the products and services of a project. For example, Filecoin raised 257 million dollars by selling tokens that will provide decentralized cloud storage to its users. Golem and Basic Attention Token (BAT) are examples of utility tokens.

How does a Token Gain Value?

In order to gain a value, token performs functions on the basis of three principles—role, features and purpose. Each role has its own features and purpose. A token can perform the following roles:

- **Right**: When a token holder possesses a token, he/she gets some rights within the ecosystem.
- **Value Exchange**: The tokens create an ecosystem where they help the buyers and sellers trade value. It allows people to earn rewards in case they have performed some tasks.
- **Toll**: Tokens act as a toll gateway that allows a user to access certain functionalities of a particular system.
- **Function**: Tokens allow the holders to enhance the user experience inside a particular ecosystem.
- **Currency**: Tokens are used as a store of value to perform transactions inside and outside the given ecosystem.
- **Earnings**: Tokens are used in the equitable distribution of profits and other financial benefits among investors.

Now, in order to gain value, a token needs to fulfill one of these roles/properties. Fulfillment of the maximum possible number of roles implies that the token might achieve a higher valuation.

Introduction to Oracles

[LO - Discuss oracles and their types]

A blockchain oracle is defined as a third-party information source which is used to provide data to blockchains in order to create smart contracts. A smart contract can be simply defined as a piece of code running on the top of a blockchain. It "collects" the data from an oracle and starts the flow execution on the basis of received information. Oracles provide the flexibility to use third-party data seamlessly.

Blockchain oracles sound something similar to oracles found in the stories of ancient Greek mythology. In these stories, when people did not have enough information to make decisions, they used to ask oracles for information beyond their understanding.

In the same way, blockchains such as Bitcoin and Ethereum cannot handle real-world or off-chain data. They do not have a direct way to check the validity of the conditions on which a smart contract is based. Oracles provide the relevant data from external sources to trigger the execution of smart contracts when the predefined conditions of the contract are fulfilled.

Let's take an example, Alexa and Bobby start a wager on what will be the score of a cricket team. Alexa said that the score will be 350 runs or more and Bobby said the score will be 349 runs or less. They design a smart contract that will pay to winner depending on the score. Therefore, in order to pay the winner, the smart contract queries an oracle and uses the gained information to decide the path of execution.

An oracle is a one-way digital agent that finds and verifies real-world data and submits this information securely to the smart contract. It is not a data source but a layer that provides an interface between data-sources and the blockchain.

Types of Oracle

Oracles are used by smart contracts to communicate outside of a decentralized blockchain network. Oracles can be categorized on the basis of two main factors: type and direction. An oracle can be either hardware or software. An oracle can either bring data inside a blockchain or inform an entity outside a blockchain.

Some of the types of oracles are as follows:

- **Hardware oracles**: Hardware oracles are the sensors deployed in the real world integrated with tangible or physical objects. For example, in supply chain management, when an object with an RFID tag arrives at a specific warehouse, this data can be sent to a smart contract.

  The ability to report readings without compromising data security is the most significant challenge for hardware oracles. Oracalize recommends a two-step solution to deal with such risks. It does so by providing cryptographic evidence of the sensor's readings and anti-tampering mechanisms, thereby rendering the device unusable in case a breach happens.

- **Software oracles**: Software oracles include online sources of information which are publicly accessible. They provide information such as temperature readings, public transport information and the current price of various financial assets. Their connection with the Internet provides the most up-to-date information to smart contracts.
- **Inbound oracles**: Inbound oracles are only responsible for providing information from the external world to smart contracts. For example, an automatic buy order when the value of a stock goes down to a predefined level.
- **Outbound oracles**: Outbound oracles use internal blockchain data in order to trigger an external event.
- **Consensus-based oracles**: These oracles query multiple sources and on the basis of the consensus they decide the outcome.

Security Issues with Oracles

Oracles have a lot of control over smart contracts as the data provided by them is crucial to the execution of smart contracts. Therefore, data collected from a third-party resource has a lot of influence on the execution of a smart contract which affects its trustless nature.

Oracles are not capable of providing trustless verification of the ownership of an asset. For example, it is not possible to prove that a piece of land has actually been physically transferred to its new owner, even if the new owner has a token representing the ownership of that land on the blockchain.

SUMMARY

- A token is a representation of an asset or utility on a blockchain.
- A token can represent any asset which is fungible and tradeable.
- The tokens can be classified into two main categories—security and utility.
- A token can perform roles such as right, value exchange, toll, function, currency and earnings.
- An oracle is an agent that collects data from the real world and provides the information to the smart contracts.
- Oracles can be categorized on the basis of two main factors: type and direction.
- Oracles have a lot of control over smart contracts as the data provided by them is crucial to the execution of smart contracts.