SESSION 13

Programmable Blockchains – Smart Contracts

Learning Objectives

- Discuss programmable blockchain in detail
- Describe smart contracts

SESSION 13

Introduction

Blockchain has offered a wide range of support to many industries. With the advancement in digital technology, blockchain experts and developers are trying to customize the technology according to the needs of an organization. The blockchain can be programmed to realize its full potential. Ethereum is an example of a programmable blockchain that utilizes smart contracts.

The smart contracts are self-executing programs that help in enforcing an agreement between the parties. They extend the utility of a blockchain from storing the transactions to implementing terms of multi-party agreements. They help you enter multi-party agreements involving anything of value, be it money, property dealings or any other entity, without the need for an intermediary third party.

In this session, you will learn about the programmable blockchain in detail along with its advantages and disadvantages. In addition, you will be made conversant with the concept of smart contract, its types and working.

Introduction to Programmable Blockchain

15 min

[LO - Discuss programmable blockchain in detail]

A blockchain includes different transactions that are stored in a sequential manner. Due to the immutable nature of the blockchain, it is impossible to change the data stored in the blockchain. The blockchain cannot be altered, once created. The transactions that are confirmed by nodes in a network cannot be erased or changed by anyone. Hence, it is considered most suitable for financial transactions.

Why is a programmable blockchain important?

The blockchains that can be programmed are more useful and have more potential than the non-programmable blockchains. Some of the examples of programmable blockchains are Ethereum and Cardano. The non-programmable blockchain examples include Bitcoin, Litecoin and Dash. Ethereum is the most popular programmable blockchain.

A programmable blockchain accomplishes various tasks by executing logic programs via the implementation of smart contracts. Programming helps in realizing the full capabilities of blockchain.

What is Ethereum?

Ethereum is a public distributed blockchain network. Ethereum is a programmable blockchain that executes the saved logic only when certain specific conditions are met.

Let's take an example to understand the concept of programming logic.

On 14th June, 100 dollars are to be transferred from A's account to B's account. The condition for transferring the money is: transfer the money if and only if B's account has a minimum balance of 500 dollars, else discard the transaction.

The logic or codes for these types of conditions can be written, stored and executed on Ethereum or any other programmable blockchain. With Ethereum, in addition to the transfer of money through its currency, Ether, you can also implement smart contracts and make DApps.

Ethereum needs miners for maintaining and securing the network in return for the reward of Ethereum token, known as an Ether. Ether can be used to send tokens from one address to another and pay for Ethereum gas.

Ethereum gas is used to run the Ethereum network and any transaction made on the EVM (Ethereum Virtual Machine) needs gas. The amount of gas required to perform the transaction or execute the smart contract is decided by the size of the contract or transaction. The gas system prevents the network from wasting resources on lengthy transactions. If a smart contract does not provide enough gas to perform the transaction, the miners will not be able to successfully execute the contract.

Ethereum blockchain is integrated with smart contract technology that removes the need for third-party intermediaries and escrow services.

Ethereum blockchain is not only a platform for performing financial transactions, but can also be used for executing smart contracts. This is performed on EVM mainly using the programming language Solidity (among other options such as Vyper etc.). Ether is used to execute smart contracts; hence Ethereum is also known as programmable money.

Benefits of Programmable Blockchains

The programmable blockchain enhances the functionality of the blockchain. Apart from adding functionality, other advantages offered by the programmable blockchain are listed as follows:

- **Zero Downtime**

  It is not a centralized technology stored on a single server and data is stored on thousands of nodes. It is not possible that all the nodes crash at the same time.

- **Censorship Resistant**

  As the data is stored on the different nodes across the network through a consensus mechanism; hence changing the data is not possible without controlling all the nodes in a network.

- **Versatile**

  The smart contracts integrated with the programmable blockchains offer a versatile platform to create, store and execute logic.

- **Fundraising**

  The programmable blockchain helps the developers to create decentralized applications and launch ICO (Initial Coins Offering).

- **Immutability**

  The data stored in a programmable blockchain cannot be changed by a third party.

- **Secure**

  It does not have a central point of failure; hence it is more secure from malicious and fraudulent activities.

- **Faster Transaction Speeds**

  The transaction of cryptocurrency on programmable blockchains is much faster as compared to non-programmable blockchains. For instance, the Bitcoin transfer takes a minimum of 10 minutes while Ether can be transferred in a fraction of seconds and the average block time is around 14 seconds.

- **DAO Development**

  Programmable blockchains allow the building of Decentralized Autonomous Organization (DAO), which are fully autonomous and decentralized with no single leader/owner.

Problems with Programmable Blockchains

The programmable blockchain offers numerous benefits but still, it has several limitations. Some of the problems and issues related to programmable blockchain are listed as follows:

- **Unfamiliar Programming Language**

  A programmable blockchain uses its own programming language, that is sometimes unfamiliar to developers that may lead to the generation of incorrect code. This might subsequently lead to problems such as the DAO hack.

- **Scalability Issues**

  Programmable blockchains such as Ethereum are facing scalability issues as they grow more popular. The arrival of games such as CryptoKitties has slowed down the Ethereum network in the past. This has given rise to apprehensions over its viability in the mainstream user base for large-scale transactions.

- **Propagation of Incorrect Data**

  The programmable blockchain is dependent on smart contracts. If, in case, the smart contracts receive incorrect information and blockchain executes it, then the data saved on the blockchain will be incorrect. It can lead to the broadcast of incorrect information to all the nodes in a network. This is, however, more of a problem of faulty data rather than an inherent problem with programmable blockchains themselves.

Overcoming issues of "Smart" Blockchains

The programmable blockchain is often referred to as a smart blockchain. There are different issues that arise during the implementation of smart blockchain. Some of the issues and the ways to tackle them are listed as follows:

- **Limited EVM Operations**

  Prior to the creation of Ethereum, the blockchain applications had a limited set of operations for security reasons. This issue was resolved by EVM which is a Turing complete software that is executed on the Ethereum network. It helps all the participants to execute their programs without the need for writing specialized blockchain protocols for each specific use-case. Instead of creating an entire blockchain for each particular application, it allows the development of numerous applications on a single platform.

- **Gas System**

  Gas is a unit for measuring the computational power to perform certain operations. The execution of code in Ethereum needs to be paid in Ether, which is measured by the amount of gas consumed. Ethereum is dependent on the hash rate for the consensus mechanism in a network. More miners mean more hash rate, which makes the system more secure and reliable. The miners are rewarded when they mine the block and get rewards in the form of gas. The gas system also facilitates the miners to charge a fee for validating smart contracts by using their computational power.

- **Gas Limit**

  The gas limit is the maximum amount of gas that a sender is willing to pay for a specific transaction. If during the execution of a transaction an operation runs out of gas, then the transaction is reverted to its original state. However, the miners are still paid for their computational power used for the mining operation and it is added to the blockchain irrespective of its execution. It is recommended to set the gas limit higher than the actual amount required for a transaction.

  The programmable blockchains facilitate the monetary transactions as well as allow the addition of arbitrary logic and conditions to those transactions. The conditions can be added by complicated scripting accomplished with the help of smart contracts.

Exploring Smart Contracts

[LO - Describe smart contracts]

A smart contract is a computer code that executes on the blockchain. The smart contract includes a set of pre-defined rules which, if met, leads to the automatic enforcement of the agreement. It helps in facilitating, verifying and enforcing the agreement. It includes a set of instructions that are written in a programming language, which works on the basis of the IFTTT (IF-THIS-THEN-THAT) logic.

An automatic vending machine is the most basic form of a smart contract. The transaction rules are pre-programmed into the machine. You are required to select a product of your choice available in machine and insert the money. Now, the machine acting on its smart contract program checks whether the money inserted is enough. If it finds the amount of money inserted to be enough, it ejects the product. In case, it finds the money less than required, it will not eject the product and revert the money. There is no requirement of a human vendor as an intermediary which reduces transaction costs and offers round-the-clock availability of service.

The sophisticated ways in which smart contract is being implemented today, it is all thanks to the blockchain technology. Some of the characteristics of smart contracts are:

- They are self-verifying in nature.
- They are tamper-resistant, just like the blockchain platform.
- They provide a greater degree of security.
- They eliminate the dependence on intermediaries.
- They offer lower transaction costs.

Example of Smart Contract

A traditional legal contract is a written document that includes terms and conditions of a service agreement. This type of legal contract is written in a human language that may be open to a variety of interpretations by different parties. Therefore, it requires an intermediary third party to act as a watchdog to ensure that the terms and conditions are kept by both parties. Its execution needs validation from an intermediary and then only involved parties can proceed towards the next steps as per the written contract.

Figure 1 displays a traditional contract:

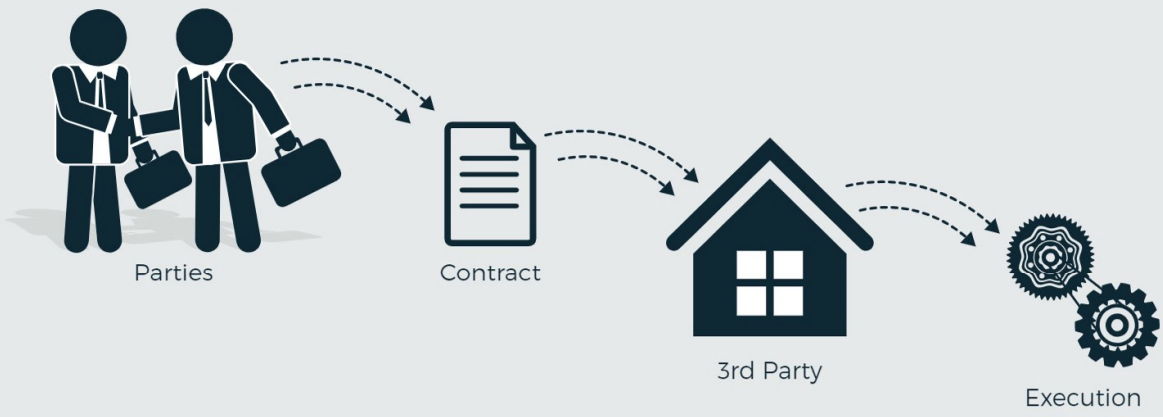

Figure 1: **Traditional Contract**

The features of a traditional contract are as follows:

- It is time consuming as it involves a lot of time for checking, validating and moving to the next step.
- It is resource consuming as it requires human intervention for its execution.
- It is expensive as it requires third-party, in case a dispute arises.

A smart contract is uploaded into the blockchain and helps in checking the validity of the transactions. This enables the automatic enforcement of the required steps as given in the contract.

Figure 2 displays the smart contracts:

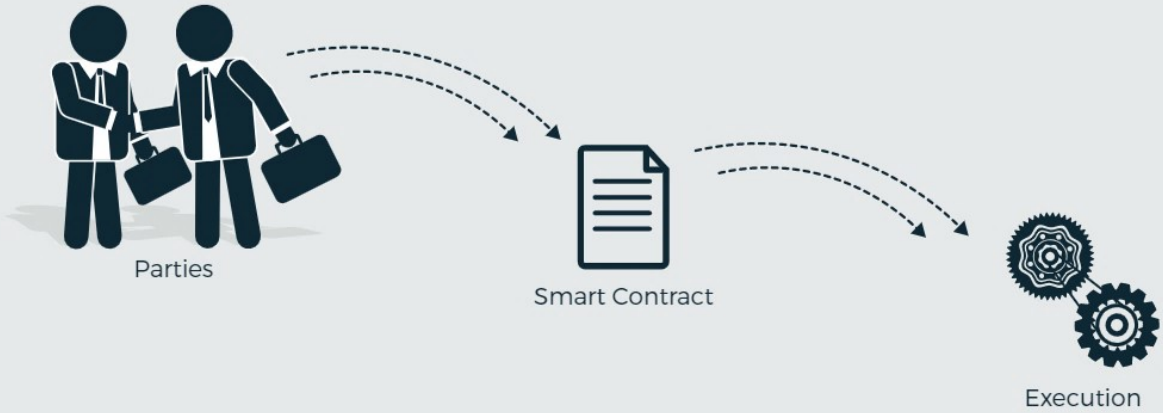

Figure 2: **Smart Contracts**

The main difference between a smart contract and traditional contract is that the former eliminates the need for third-party intermediaries and the cryptographic code helps in enforcing it.

Some of the use cases of smart contracts are:

- It ensures the authenticity of a copyrighted product in online shopping by making sure that the product bought by customer is authentic not an imitation. It is easily achieved, as the information stored on the blockchain is immutable; hence it is easy to prove that a purchased product belongs to a specific line of products.
- The insurance sector uses a blockchain application that helps in implementing the smart contract. AXA, a French multinational insurance company, has launched its first flight delay insurance product, Fizzy, with the help of smart contracts.

Types of Smart Contracts

Blockchain and smart contracts have impacted many industries such as banking, insurance, telecommunication and energy sector. A smart contract can be implemented from simple to complex scenarios.

Figure 3 displays the different types of smart contracts:

Figure 3: **Types of Smart Contracts**

You will understand the different types of smart contracts with the help of different use cases.

- **Digital Value Exchange**

  This type of smart contract deals with the transfer of cryptocurrency from one e-wallet to another. For instance, sending of cryptocurrency such as Bitcoin from one family member to another.

- **Smart Right and Obligation**

  Smart contracts that are enforced legally as they announce the rights, duties, obligations that have to be agreed by all the parties. A customer purchasing a digital content stream represents an example of a smart right and obligation type smart contract.

- **Basic Smart Contract**

  The smart contract that is executed only when conditions are met. A landlord remotely locking a tenant who fails to pay the rent is an example of a basic smart contract.

- **Multiparty Smart Contract**

  The multiparty smart contracts act as a legal binding agreement between the involved parties in a contract. A seller lending money to a buyer for purchasing a house is an example of a multiparty smart contract.

- **Distributed Autonomous Business Unit**

  An organization issuing its own bonds and the buyers monitoring the payments with the help of a shared ledger are examples of distributed autonomous business units.

- **Distributed Autonomous Organization**

  These smart contracts help in performing tasks such as making peer-to-peer deliveries and purchasing electricity from the cheapest provider at any time automatically. The automated trucks can easily make peer-to-peer deliveries and pay the local toll road tax.

- **Distributed Autonomous Government**

  These types of smart contracts help users in creating their own self-enforcing government services.

- **Distributed Autonomous Society**

  In these types of contracts, the users can form groups in their preferred locations to help in establishing trade agreements with other groups of users.

Design of Smart Contracts

In a blockchain, the smart contracts are written as a script using a programming language. The user can implement the logic or conditions of the contract to execute the transaction if the conditions are met.

The contract is written, and the script is deployed on the blockchain. The code is executed by the network and the output of the contract should always be the same. The contract is executed based on the different conditions and the user can opt for the smart contracts based on its requirements.

The design of smart contracts can be shown by using Figure 4:

Figure 4: **Design of Smart Contracts**

- **Request**

  A user identifies conditions and requests a contract.

- **Drafting**

  A simple digital contract is created based on the specified set of conditions.

- **Negotiation**

  The parties involved in smart contracts have to agree on the terms that are drafted in a contract.

- **Approval**

  The internal controls make sure that the execution of the contract results in the best outcome.

- **Execution**

  The contract is implemented on a blockchain such that the assets are exchanged securely. The contract is unlocked to perform transactions only when the conditions are met.

The organizations across the globe are now deploying smart contracts to manage the existing relationships or manage new relations with customers, partners, businesses, dealers, and suppliers etc. The blockchain and smart contracts have offered various advantages to the organizations irrespective of the contract size and volume.

SUMMARY

- A programmable blockchain accomplishes various tasks by executing logic programs via the implementation of smart contracts.
- Programming helps in realizing the full capabilities of blockchain.
- Ethereum blockchains store and execute newly coded programming logic.
- Gas is a unit for measuring the computational power to perform certain operations.
- The gas limit is the maximum amount of gas that a sender is willing to pay for a specific transaction.
- The smart contract includes a set of pre-defined rules which, if met, leads to the automatic enforcement of the agreement.
- Smart contracts are a set of instructions that are written in a programming language, which works on the basis of the IFTTT (IF-THIS-THEN-THAT) logic.