Quick dive into Smart Contracts in Blockchain Technology

Author: Kashyap Shah

What is Smart Contract?

"Smart contracts" are a critical component of many platforms and applications being built using blockchain or distributed ledger technology. "Smart Contract" term is used to describe computer code that automatically executes agreement and is stored on a distributed, decentralized blockchain network. Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism. They can also automate a workflow, triggering the next action when conditions are met. The objectives of smart contracts are the reduction of need in trusted intermediates, arbitrations, and enforcement costs, fraud losses, as well as the reduction of malicious and accidental exceptions.

Smart contract - History and Creation

The smart contracts were first proposed by **Nick Szabo** in **1994**. Back then, there was little interest or activity in smart contracts because there was no digital platform or distributed ledger technology that could support them.

In 2008, the bitcoin cryptocurrency was developed on a blockchain network with a distributed ledger that tracks monetary transactions. This technology enabled the development of smart contract code that is used to enter the terms of the contract into the blockchain.

Many platforms now allow the use of smart contracts, such as Ethereum, Hyperledger, Tezos, and Corda. Today, with the growing adoption of bitcoin and different blockchain technologies, smart contracts are growing in popularity.

How do Smart Contracts Work?

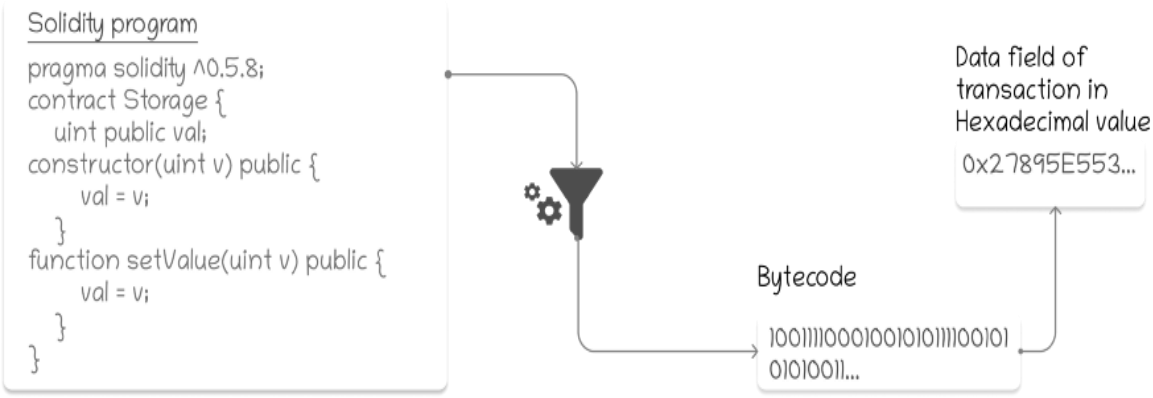
The process of creating a smart contract starts with business teams working with developers to describe their requirements for the desired behavior of the smart contract in response to various events or circumstances. Simple events could be conditions such as payment authorized, shipment received, or a utility meter reading threshold. More sophisticated logic might encode more complex events such as calculating the value of a derivative financial instrument and processing trade of the derivative or automatically releasing an insurance payment in the event of a person's death or a natural disaster.

The developers then work in a smart contract-writing platform to develop the logic and test it to ensure that it works as intended. After the application is written, it is handed off to another team for a security review. This could be an internal expert or a firm that specializes in vetting smart contract security. Once the contract has been approved, it is deployed on an existing blockchain or other distributed ledger infrastructure.

Once the smart contract is deployed, it is configured to listen to even updates from an "oracle," which is essentially a cryptographically secured streaming data source. The smart contract executes once it receives the appropriate mix of events from one or more oracles.

Programming & Deploying of Smart Contract

So how does one go about programming these smart contracts? Everything has programming language. Like websites built using HTML, CSS and Javascript, Ethereum Smart Contracts are built using Solidity. Ethereum uses Solidity to write programs (its syntax is almost identical to Javascript). They are then compiled into bytecode (one and zeroes computers can understand). This bytecode is sent as a hexadecimal value (zero representation form) in the transaction data field. This process of sending bytecode to sales is called intelligent contract transfer. Ethereum blockchain understands that the system is being distributed and provides an address to this smart contract. Anyone can send money to this Smart Agreement or withdraw money from this Smart Contract using this address.



State of Smart Contracts

There are Distributed Apps with Smart Contracts installed on them. These apps provide ways to work with a smart contract, to reflect the current state of a smart contract, and especially to execute certain logic. Other popular DApps are, Uniswap, MakerDAO, CryptoKitties. Each of these applications aims to enter a specific contract into smart contracts. This contract is always maintained regardless of external circumstances.

What exactly does this mean? Each smart contractor can capture data. This data is stored in a variable that can be numbers, strings, addresses, and so on. Types of variables more complex than maps of string addresses or whole values or addresses. These are just a few examples. After digging the block, that block holds the current status of all smart contracts in the Ethereum blockchain. Current status is the current value of all variables, the amount of Ether stored on Smart Contract addresses, and other common addresses.

Apart from the flexibility, Smart Contracts also have functions. They do it when certain conditions are satisfied. One can perform a function in Smart Contract by sending a transaction with the required parameters to the transaction data field. For example, if I want to enter a competition with an entry fee of 0.01 Ether. I would work with the Smart Manager Agreement (mostly done via DApp) and send 0.01 Ether to their address. Then the Home Smart Smart Contract will give my address to pass. Later, when I want to enter a contest, I will have to verify my address and, once approved, I can successfully join.

So, with a variety of Solidity, functions, and multiple APIs, one can create a variety of features in the Ethereum blockchain. You may have heard the name NFT (Non Fungible Token). This is nothing but wise agreements that make some sense in them. Each NFT is a Smart Contract with flexibility that keeps the NFT owner's address. It also has some functions that help transfer NFT ownership to another person. They have some fixes that help prevent attackers from gaining undue NFT control. The technical name of the NFT Smart agreement is ERC721. We will go into saying this in a future article! In the meantime, all you need to know is that ERC721 defines a set of tasks that need to be done to make the Wise Agreement into NFT.

Applications of Smart Contracts

- Trade and finance: Automated approvals have become a key element of smart contracts, helping to streamline operations as permits take less work and thus time.
- Procurement management: Supply chains can be best managed with blockchain-based smart contracts. First of all, Internet of Things devices can be used throughout the series to record every step and thus keep track of each item and its location at a given time. Even in large warehouses, these smart contracts can help managers see real-time and time-consuming stock levels to keep products in line with supply chains, and help them improve delivery times. In addition, smart contracts can be used to initiate automatic restructuring and to pay for orders already received.
- Product development: Similarly, smart contracts can be used to keep a ledger recording the stages of product production. The two parties will sign the contract subject to certain conditions and the production stages of the product will be recorded in a smart contract. So in cases where the parties agreed to split the payments, the payments would be made upon reaching the agreed-upon procedures and all this would be done without compromising on the security of sensitive information (consider the rationale for large and small companies).

- Peer-to-peer transactions: Smart contracts can be used for peer-to-peer transactions (consider any business transaction between two parties). And it is this use that has paved the way for the development of the Ethereum blockchain and other such companies. Users from different sectors can use these platforms to create collaboration agreements. These contracts remain valid until the terms of the agreement are met. Once this has happened, the remaining part of the agreement is fulfilled. This part of the agreement usually transfers funds (and cryptocurrensets) but can also refer to securing the services of development groups.
- Insurance: In addition to sponsoring an initial insurance policy, smart contracts can help develop insurance companies by processing claims - either by conducting error checks or determining the amount of payments according to certain categories (those in a person or organization) policy, all over time, with greater accuracy and lower costs.

Over time, smart contracts can be used with the Internet for Motor Vehicle Enforcement to simplify payment insurance policies and speed up post-accident claims. Processing information such as driver's licenses, driving records, accident reports, and policy details can also be done in a short period of time.

- Real Estate: Smart contracts can be used to record property ownership and lease, eliminating the need for real estate agents and sellers. Even loan transactions can be done quickly and efficiently with such contracts. There will be greater clarity between the two parties as the change of ownership will be shown only after the approval of the unique key code on behalf of the original owner, thus making the whole process more secure and reducing criminal incidents.

In fact, such contracts can be used to record ownership and lease of other items as well - consider jewelry, telephones, watches, etc. and real estate.

- Healthcare: Today, millions of patient medical records are stored in computer systems. If this information is converted into smart contracts, you will enjoy the benefits offered by blockchain technology: consider all data that is securely encrypted and stored and accessible only by those who have a private key. In addition, smart contracts can be used to issue orders, keep receipts, general stock management, keep test results, and so on.
- Medical research: Using smart contracts, highly sensitive data such as patient records can be safely transferred between research departments / institutions. Similarly, medical research companies can use smart contracts to store test results and new drug formulas.
- Voting: Voting fraud can be successfully implemented through smart contracts; can be used to verify voter identity and record their vote. Given the fact that the blocks within the blockchain cannot be changed once they have been recorded, the manipulation of this record would not be possible.
- Solving macroeconomic problems: Smart contracts can be used to deal with macroeconomic problems, especially those related to distribution. Complex issues

such as limited ownership - for example, many farmers with a single tractor to reduce costs per farmer or equitable distribution of power throughout the world - can be addressed with smart contracts.

Aside from the many benefits of using smart contracts, it is important to note here that smart contracts are not the same as smart contracts. The latter refers to an agreement that legally binds the indigenous language with certain terms specified and used in machine-readable code.

Also, a smart contract does not have to be a legally binding agreement. Some legal experts even claim that smart contracts are not legal contracts, instead calling them default payment methods and ways to transfer tokens or cryptocurrensets. Also, some experts have emphasized that the critical or diminishing status of systemic languages can affect the legal validity of smart contracts.

That means the efforts are at a level where they are officially registered. In 2017, through the Declaration of Digital Economic Development, Belarus became the first country to officially enter into smart contracts.

REFERENCES

- https://searchcompliance.techtarget.com/definition/smart-contract
- https://www.ibm.com/topics/smart-contracts
- https://corpgov.law.harvard.edu/2018/page/51/
- https://medium.com/youngwonks/what-is-a-smart-contract-d80789593208
- https://medium.com/@asper9/smart-contracts-a194da695a68