SMART CONTRACTS

Ethereum

A simple description: „The World Computer”. Ethereum is a platform at physical level represented in a network of computers that executes programs called smart contracts.

The Ethereum platform enables anyone to build powerful decentralized applications (applications that have centralized code and also decentralized code). While providing high availability, auditability, transparency, and neutrality,it also reduces or eliminates censorship and reduces certain counterparty risks. Everything is enforced by computer code, no human intervention, no corruption, no human feelings and is backed by a large community of unknown (anonymous) parties.

Components of Ethereum blockchain

- A peer-2-peer network of Ethereum clients responsible for propagating transactions and blocks of verified transactions. Part of this network are the miners (special nodes that solve complex mathematical puzzles in order to have the right for adding information into the blockchain).
- Transactions: messages sent throughout this network containing either transfer of ether token between two accounts or executions of smart contracts.
- A set of consensus rules, governing what constitutes a transaction and what makes a valid state transition.
- A state machine (a Turing complete Ethereum Virtual Machine, EVM in a short) that processes transactions according to the consensus rules.
- A database (also called blockchain) which is a chain of cryptographically secured blocks containing transactions.
- A consensus algorithm that decentralizes control over the blockchain, by forcing participants to cooperate in the enforcement of the consensus rules with a game-theoretically sound incentivization scheme to economically secure the state machine. For the moment Ethereum is using Proof of Work algorithm and it is scheduled to switch to Proof of Stake in the next 2 years.
- A set of clients (software that implements the above rules) that are running on different computers around the world and create the Ethereum network.

Smart Contracts

There are 2 types of accounts in Ethereum:

- **Externally Owned Accounts (EOA)**. EOAs are controlled by users, often via software such as a wallet application that is external to the Ethereum platform. Users in the Ethereum network own ether tokens in this type of account. They have a public key (encoded in an Ethereum address) and a private key that is kept secret by the user and used only to sign transactions. EOAs can transfer ether tokens from one address to another and also can run a smart contract. They cannot control the execution of smart contracts, they can only fire it.

- **Smart Contract accounts**. In contrast, contract accounts are controlled by program code (also commonly referred to as smart contracts) that is executed by the Ethereum Virtual Machine. This type of accounts do not have a need for a private key, they do not “sign” transactions and if they have ether tokens in their balance the spending of the tokens is done by the computer and the rules of spending it are described in the smart contract code.

Smart Contract - Definition

“a set of promises, specified in digital form, including protocols within which the parties perform on the other promises” - Nick Szabo in the 1990s

“immutable computer programs that run deterministically in the context of an Ethereum Virtual Machine as part of the Ethereum network protocol” - Andreas Antonopoulos our days

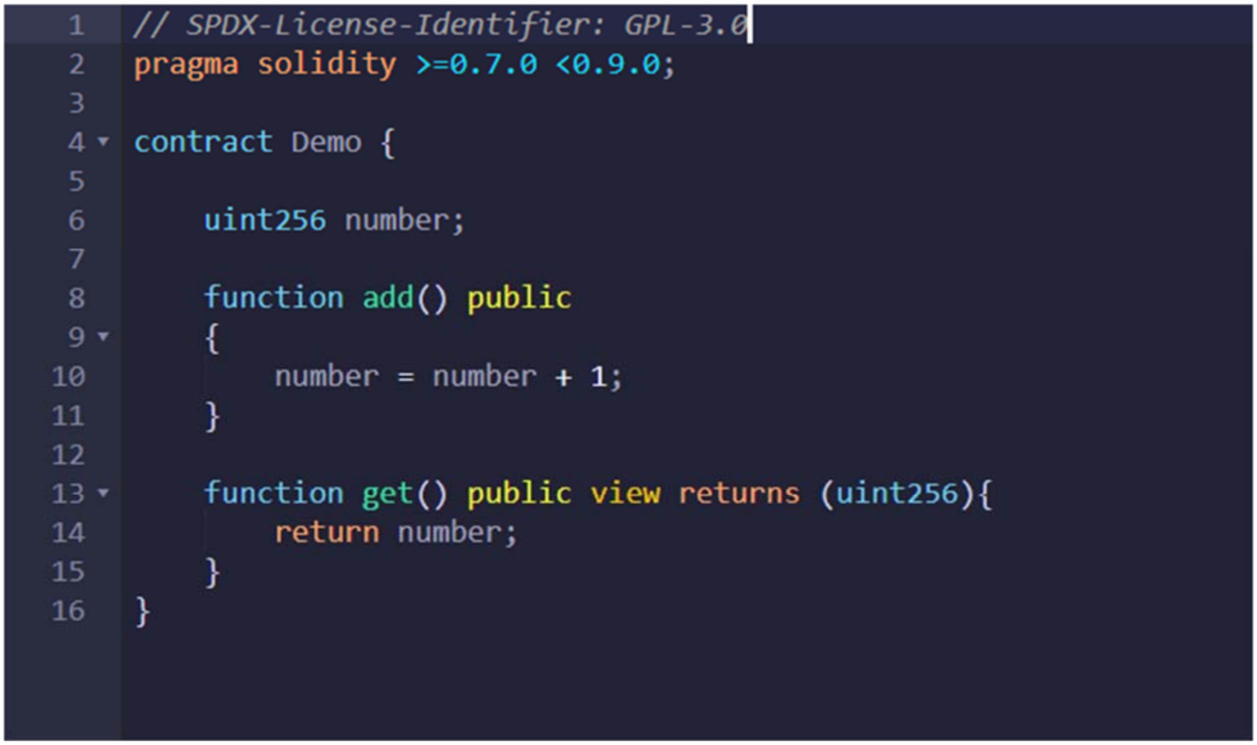
The word “contract” has no legal meaning here, they are simply computer programs. Immutable means in the context of blockchain they can not be changed once written in the blockchain. There are some cases when a smart contract can be changed but it must be defined a specific way and this is transparent to anyone since the blockchain is a public database. By “deterministic” it means that for the same set of input data the outcome will always be the same. This is very important because all the nodes from the network (Decentralized world computer) need to execute the smart contract and verify the output validity. EVM context means a contract can access it’s own data part (state), information about the transaction and information from the block.

Components of a smart contract

- Data part component (state). The state of the smart contract contains information needed for its executions. Every change in the data results in a new state and every state is stored in the blockchain. This way the execution is transparent and anyone can see the execution history. After every execution a snapshot of the smart contract state is created and saved in the blockchain. These snapshots are protected by blockchain’s cryptography and they cannot be altered or deleted.

- Methods component. The second part of the smart contract is a set of methods that are executed by EOA in special transactions or by other smart contracts. There are two kinds of methods: methods that change a smart contract state (add information to the blockchain) and methods used to view a smart contract state. Methods that change the state are executed by all nodes, verified and the execution costs ether tokens. Special nodes (miners) that are allowed to add information to the blockchain are “paid” with these tokens.

Example of a smart contract



```
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.7.0 <0.9.0;

contract Demo {

    uint256 number;

    function add() public
    {
        number = number + 1;
    }

    function get() public view returns (uint256){
        return number;
    }
}
```

Data:

- “uint256 number”

Methods:

- function add() public
- function get() public view returns (uint256)

Method add is runned by every node and it has a cost of Ether tokens, method get can be runned by any node and it only returns (used to view data part of this smart contract) data with no cost.

Every time the method add is executed by an EOA or another smart contract the number value changes and the new value is stored into the blockchain. Running the method several times all the values for the number field are stored and you can see the execution history of the smart contract.

Why use smart contracts and create decentralized apps instead of centralized ones?

- **Speed and no need for a lawyer**: A smart contract can be created by anyone, you don’t need a lawyer licence or a lot of school years to understand the ramifications you just enter some computer rules bases on simple mathematical calculus and logical operands and you have your contract
- **Cost**: To add (deploy) a smart contract into the blockchain the network will take from you a small amount of tokens. As an example, nowadays to deploy a medium size smart contract into the Ethereum blockchain the cost is less than $50.
- Immutable: Once deployed into the blockchain there is virtually no chance for anyone to change it and it’s never lost, you can always find it there.
- **Content (rules) is crystal clear**: Because of the way a smart contract is executed every rule that you write into it can not be interpreted, everything is clear. In traditional contract offen when there was a dispute even a comma in a phare could change it’s meaning
- **Secure**: it is protected by the cryptography of the blockchain and is backed by the entire community that’s running the network, they will all have a copy of it
- **Virtual Presence**: you do not need to physically sign the contract, you don’t even need to know who you are dealing with and you can be safe that the computer is watching over the contract and basically this way you can trust anyone.
- **Enforced by computer**: You don’t need a judge to decide if the rules are met or who’s right and who’s wrong. The computer by using logic and math will enforce the already agreed rules and it’s incorruptible and has no human emotions.

Fields of use for smart contracts

Digital Identity: you can store identities in the blockchain and instead of trusting a government entity like we do today that can be corruptible you can the trust “the world computer”

Financial Security: instead of relaying an investment fund with your assets you can trust a smart contract with clear rules and actions to manage your assets

Trading and payments: you can create smart contracts to help you make cheap payments all over the world and trade assets without being blocked or taxed

Clinical trials: instead of big medical company use you medical data including blood tests or any kind of tests to make money in huge research projects you can decide what to do with your data

Escrow and insurance: any kind of escrow application or insurance application can be created using smart contracts and the response in any case will happen in a blink of an eye instead of spending time in filling unnecessary papers.

Supply chain management: you can track any product from manufacturer to customer and the information will stay in blockchain forever, no one will ever be able to hide anything

Intellectual property: You can protect your intellectual property using smart contract and blockchain and it will be cheaper and faster and no one ever will be able to take your credit for it no matter how much money or power they have.

Conclusion

Smart contracts will change our way of living, we will be able to trust each other even if we never met, we can build the trust ourselves, we will not need lawyers, judges or third parties to settle disputes between us, because there will be none. Using smart contracts we will be able to collaborate far more easily than we are doing right now and things like scamming or tricking between people will cease to exist.

The mass adoption of smart contracts will happen when mankind will be able to create applications with nice interfaces and anyone with an analytical mind will be able to create a smart contract. This kind of application will need to be very easy to use, probably in the future you will be able to describe in words what you need and the application will be able to create a logical diagram of what you need. People need to stay in front of a computer / phone and by using the mouse or fingers to be able to design a smart contract.

The blockchain technology is a very young one, the first implementation happened only 12 years ago and the adoption was slow because of a lot of controversial issues around Bitcoin. The technology itself is a game changer and it is probably the mass adoption of blockchain in our lives and the smart contract will happen in the next 5 to 10 years.