DAAR | Blockchain & Smart contracts

Guillaume Hivert | hivert.is.coming@gmail.com | @ghivert

We’ll talk about blockhains and smart contracts.

Smart Contracts? Blockchain? Do you have an example?

Some use cases

- Transfer of money without third-party
- Create digital private property
- Used in digital art
- Create decentralised finance

What is a blockchain?

- A blockchain is a service providing **truth**
- A blockchain is a **database** (or a ledger)
- It ensures **everyone will have the exact same info** anywhere in the world
- In a **decentralized** way
- It will be the backbone of our applications
- It **resists to censorship**
- It is unbreakable

Some chronology

- Created in 2009 (11 years ago)
- Bitcoin was the first cryptocurrency
- A lot of cryptos has been created
- First try of smart contracts in 2015
- Ethereum in 2015

A blockchain is made of nodes, wallets and transactions

- Everybody are verifying transactions through nodes
- We have a **wallet** to identify us (thanks to RSA)
- Every interactions with the blockchain are made through transactions, with inputs and outputs
- It heavily uses Game Theory
- We can transfer wealth
- We can transfer **data,** why not program it?

Let’s build some Dapp

- Ensuring unicity of dematerialized things
- Ensuring truth
- Decentralizing information
- Handling transactions between people
- Identifying someone

Why a Smart Contract?

- Automatically follow rules of a contract between two stakeholders
- Tamper proof
- Unbreakable
- Decentralized
- Uncensorship
- Replaces backends
- Provides trust

A programmable blockchain, with smart contracts

A smart contract is a software ensuring rules will always be correct. It resembles a backend. It has entry points and outputs.

It is compound of:

- Data
- Functions
- Triggers
- Events

An idea? Train booking software

Train booking software

- Order your train ticket
- The order go into a contract
- For every ride, the data are recorded to the contract
- The contract ensures everything will follow the rules
- If a train is late, the contract will automatically refund the customers

Wild Smart contracts appeared!!!

Developers use Bitcoin! It is not super effective...

Bitcoin allow 80 bytes of free data in every transaction.

1 action = 1 transaction

Follow rules according to new transactions

(Script, MiniScript, Colored Coins)

Can we do better ? Fully hosted directly on blockchain

We need :

- a language
- a VM

=> Ethereum

Here comes a new challenger ! Ethereum

- A language : Solidity
- A VM : EVM
- A full blockchain with wallets with plenty of nodes
- An interop way with JavaScript

What about opponents?

- Tezos
- Cardano
- Solana

But Ethereum is:

- 7 years old
- Robust

How does it work?

1. Write your contract in Solidity.
2. Compile to EVM bytecode and ABI.
3. Push the bytecode to Ethereum.
4. Ethereum will instantiate Smart Contract at an address.
5. Use ABI to interact with contract.
6. Every interaction is made of a transaction.

Solidity key points

- Inspired by C++ and JavaScript
- Typed language
- Object Oriented
- Package managers
- Huge community usage

We code contracts

- A contract has data and functions that modifies data.
- A contract has pure functions to read data on the blockchain.
- The contract has conditions and entrypoints to interact from the outside world.
- The contract has private and public functions.

How is Solidity looking?

```
pragma solidity 0.6.6;

contract Greeter {
  string private message;

  function setMessage(
    string memory _message
  ) public {
    message = _message;
  }

  function greet()
  public view returns(string memory) {
    return message;
  }
}
```

/!\ Other languages can compile to EVM bytecode.

What about Dapps?

A DApp

A Dapp is an application using the blockchain as a backend.

It connects to a Smart Contract and interact directly with the blockchain.

It’s made up of a frontend in JavaScript and a backend as a Smart Contract.

How does a DApp interact with users?

1. It has the smart contract address
2. It creates a new transaction
3. The user signs the transaction with her wallet
4. The front send the transaction.
5. The blockchain execute the smart contract code.
6. The blockchain hooks the front.

An example? Let’s take a live example

Remarks

- While we are targeting Ethereum, Tezos or Cardano, the concept are the same on other blockchains.

Thank you for your attention