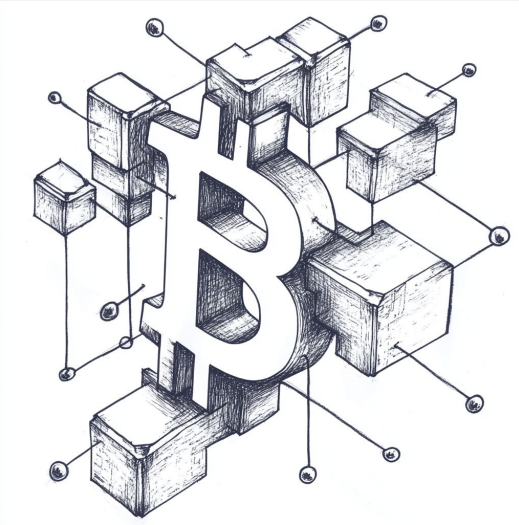
Smart Contracts, Ethereum, EVM



Alejandro Narancio
ale.narancio@gmail.com
@anarancio

Smart contracts

Smart contracts - Características

Origen

Smart contracts - Características

Origen

Elimina intermediarios

Smart contracts - Características

Origen

Elimina intermediarios

Distribuidos & Descentralizados

Smart contracts - Características

Origen

Elimina intermediarios

Distribuidos & Descentralizados

Autonomos

Smart contracts - Características

Origen

Elimina intermediarios

Distribuidos & Descentralizados

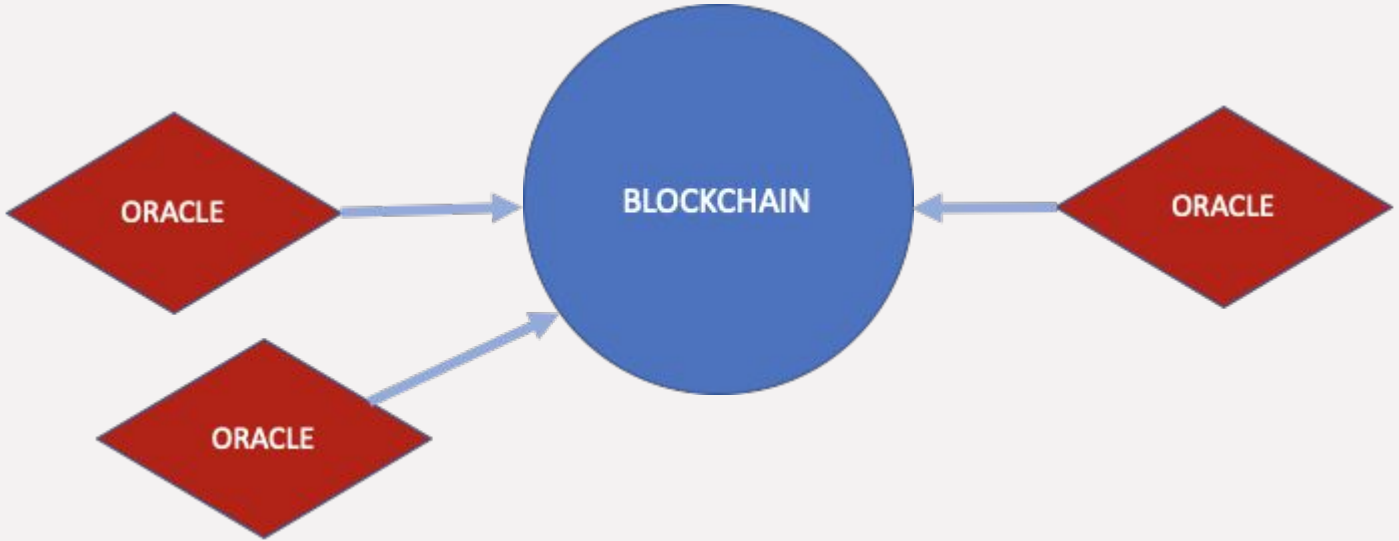
Autonomos

Inmutables

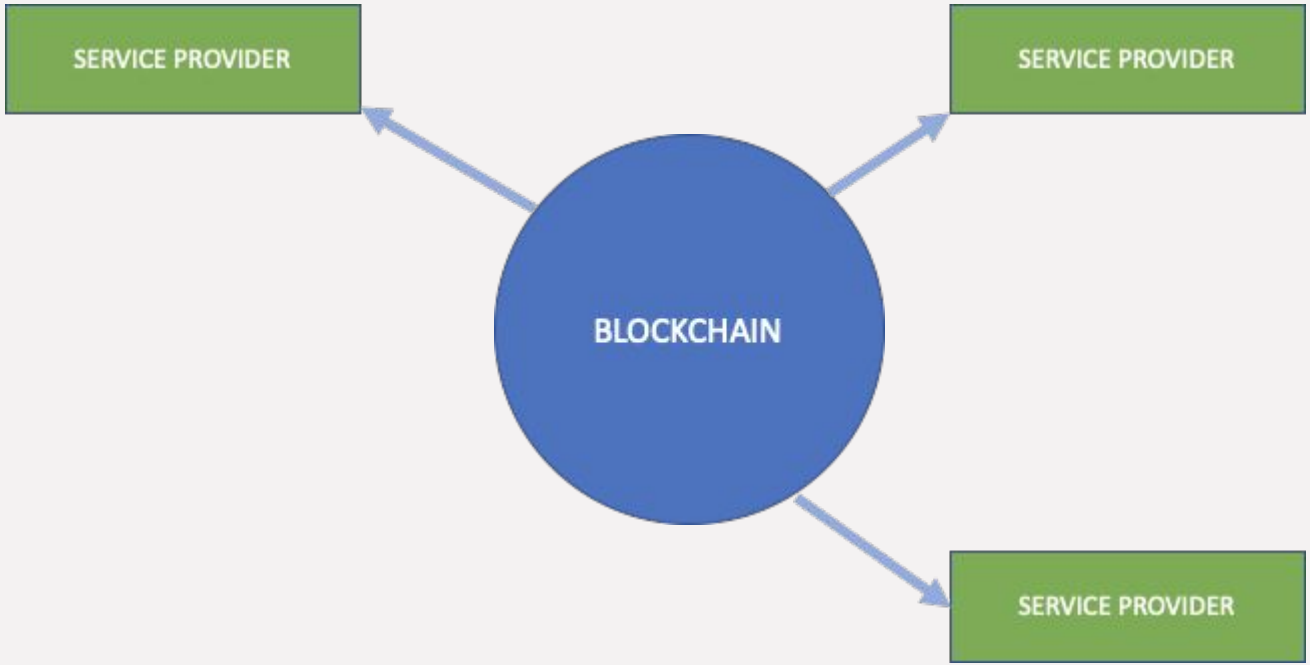
Smart contracts - Plataformas

Smart contracts - Integración con sistemas externos

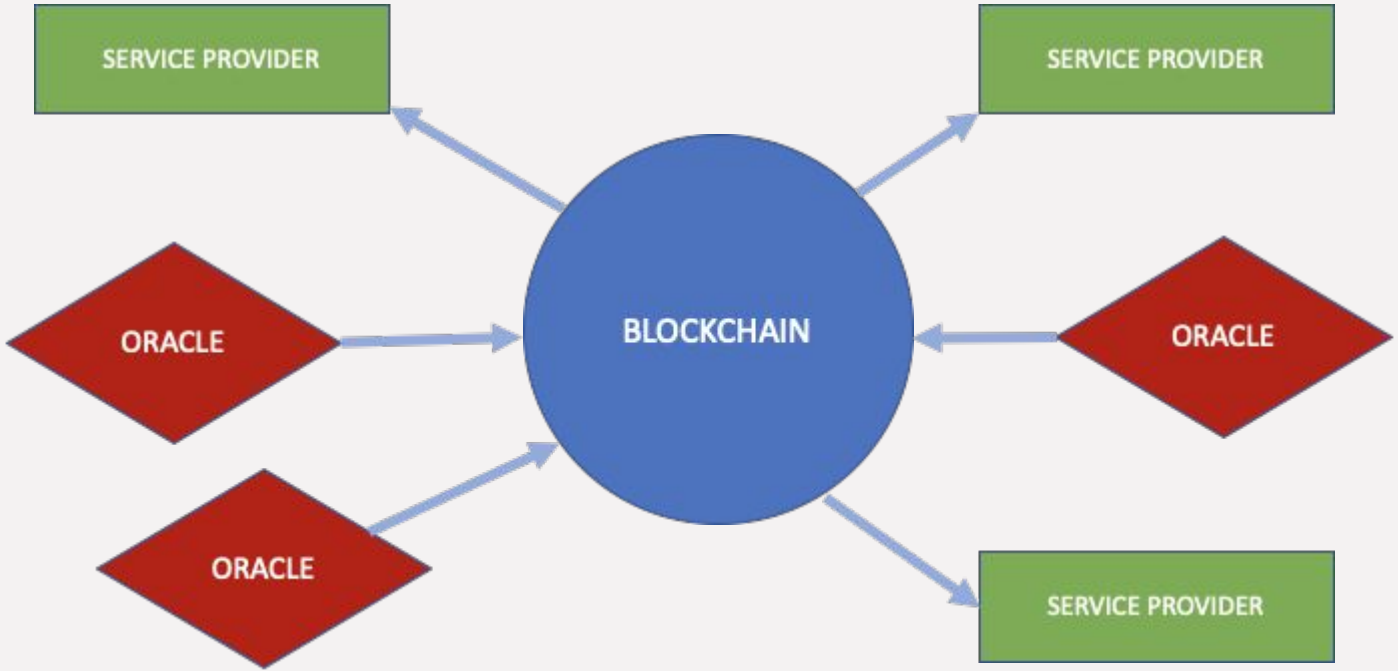
Smart contracts - Integración con sistemas externos



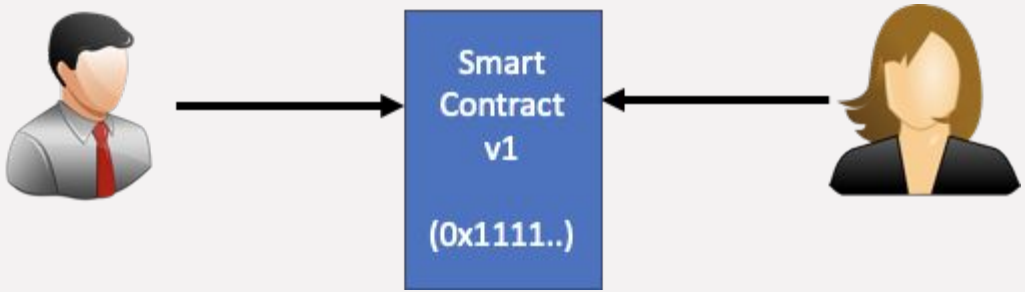
Smart contracts - Integración con sistemas externos



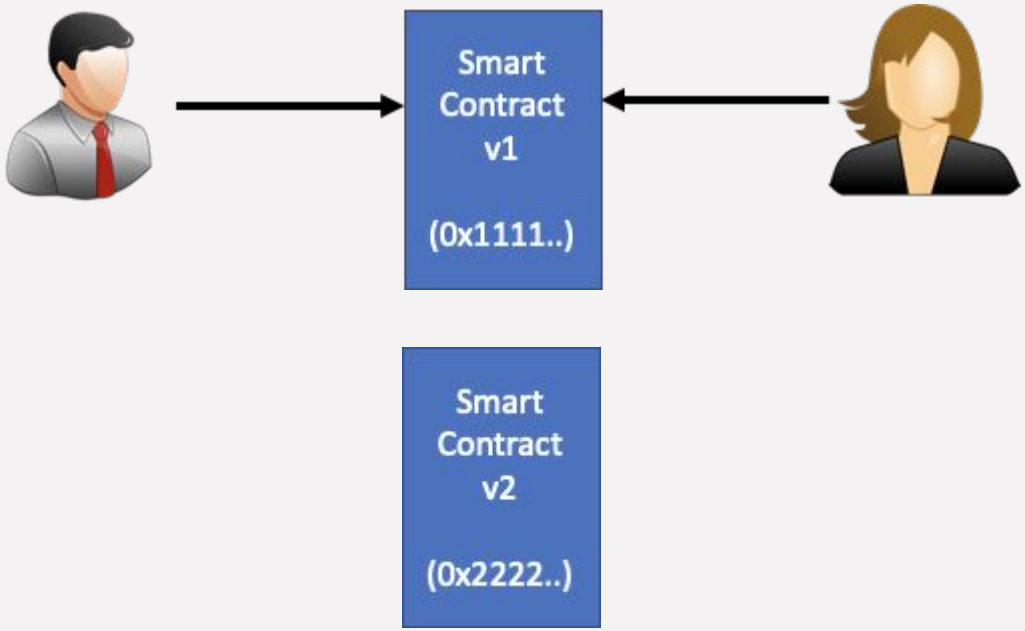
Smart contracts - Integración con sistemas externos



Smart contracts - “Problemas” de la inmutabilidad

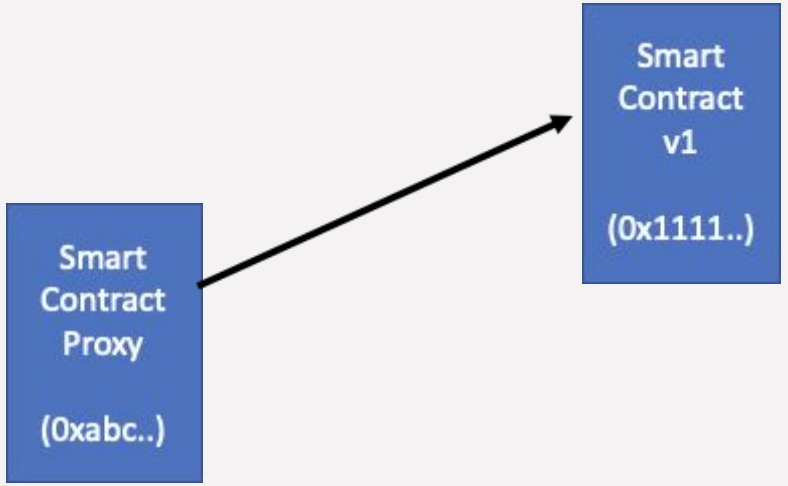


Smart contracts - “Problemas” de la inmutabilidad

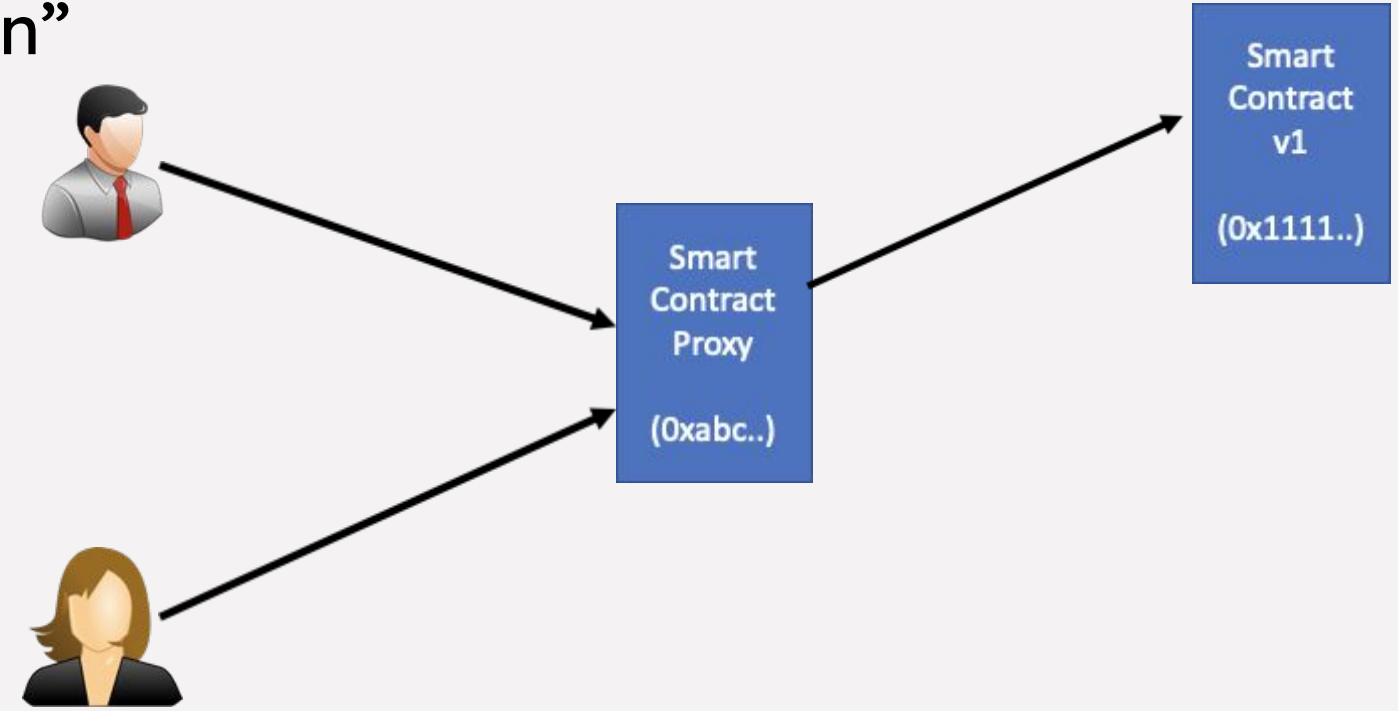


Smart contracts - “Problemas” de la inmutabilidad - “Solución”

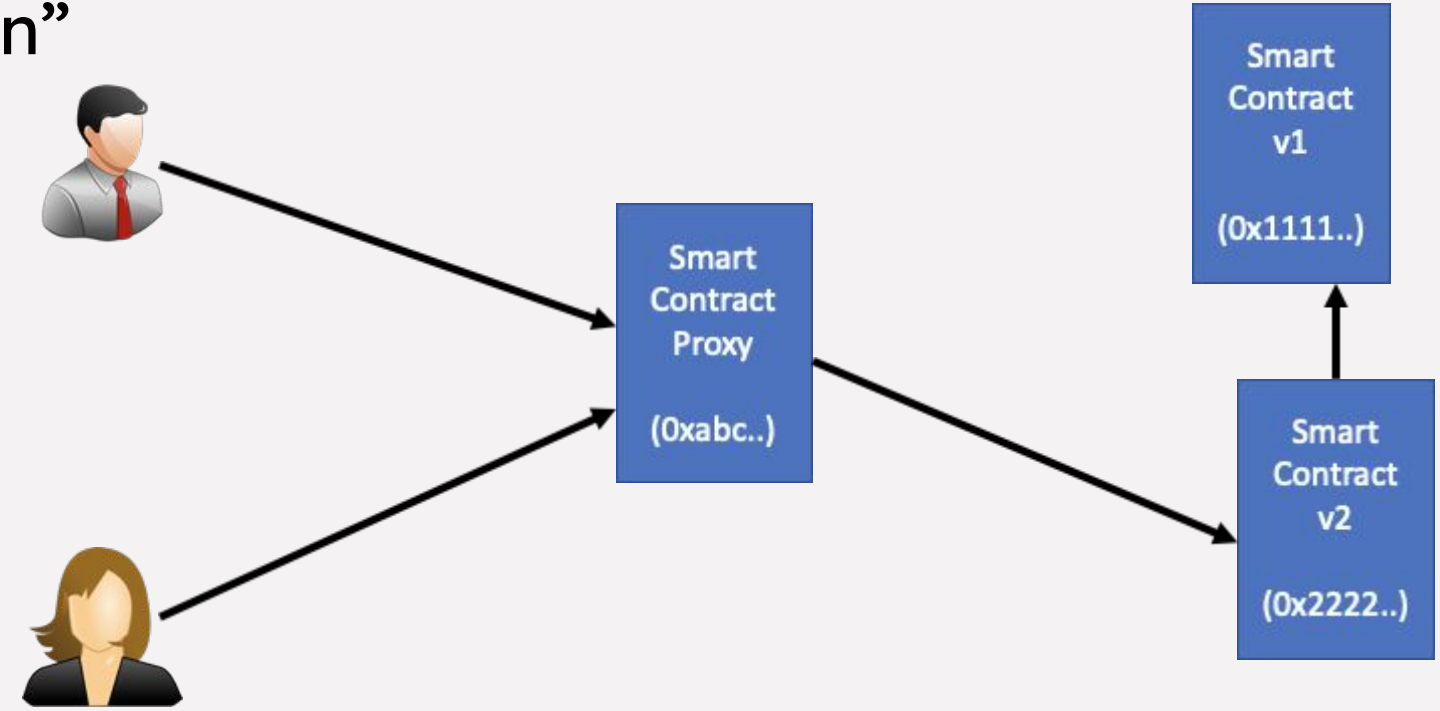
Smart contracts - “Problemas” de la inmutabilidad - “Solución”



Smart contracts - “Problemas” de la inmutabilidad - “Solución”



Smart contracts - “Problemas” de la inmutabilidad - “Solución”



Ethereum & EVM

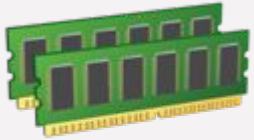
Problemas en el language Script de Bitcoin para escribir Smart Contracts

Problemas en el language Script de Bitcoin para escribir Smart Contracts

No Turing Complete

Problemas en el language Script de Bitcoin para escribir Smart Contracts

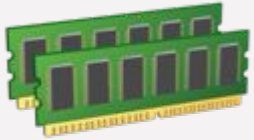
No Turing Complete



Pocos Recursos

Problemas en el language Script de Bitcoin para escribir Smart Contracts

No Turing Complete

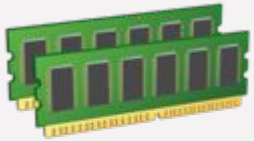


Pocos Recursos

Sin memoria persistente

Problemas en el language Script de Bitcoin para escribir Smart Contracts

No Turing Complete



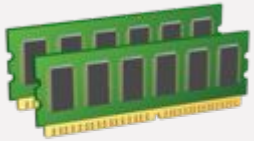
Pocos Recursos

Sin memoria persistente

Contexto limitado

Problemas en el language Script de Bitcoin para escribir Smart Contracts

No Turing Complete



Pocos Recursos

Sin memoria persistente

Contexto limitado

Muchos OP CODES deshabilitados

EVM - Conceptos básicos

EVM = Ethereum Virtual Machine

EVM - Conceptos básicos

EVM = Ethereum Virtual Machine

Soporte de lenguaje Turing complete

EVM - Conceptos básicos

EVM = Ethereum Virtual Machine

Soporte de lenguaje Turing complete

Dos tipos de cuentas: EOA y Contratos

EVM - Conceptos básicos

EVM = Ethereum Virtual Machine

Soporte de lenguaje Turing complete

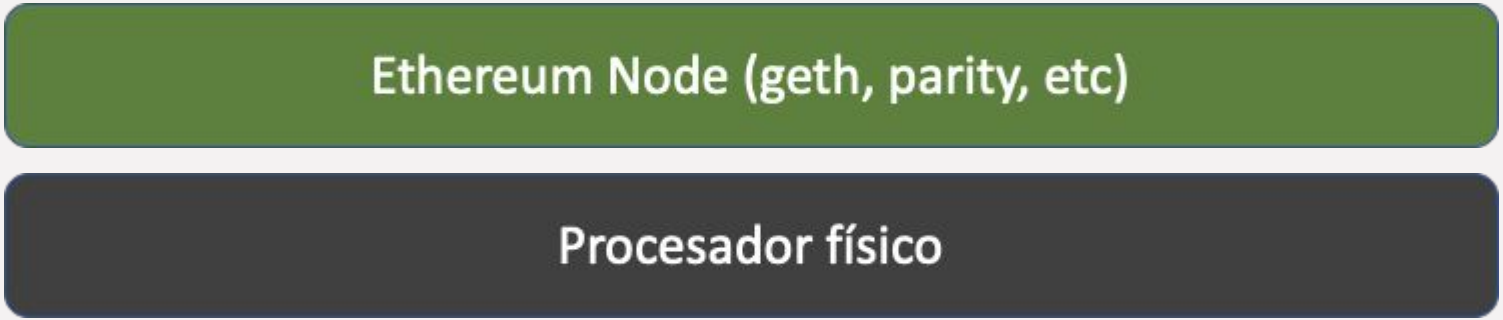
Dos tipos de cuentas: EOA y Contratos

Todas las operaciones que ejecuta un contrato se ejecutan en todos los nodos del sistema

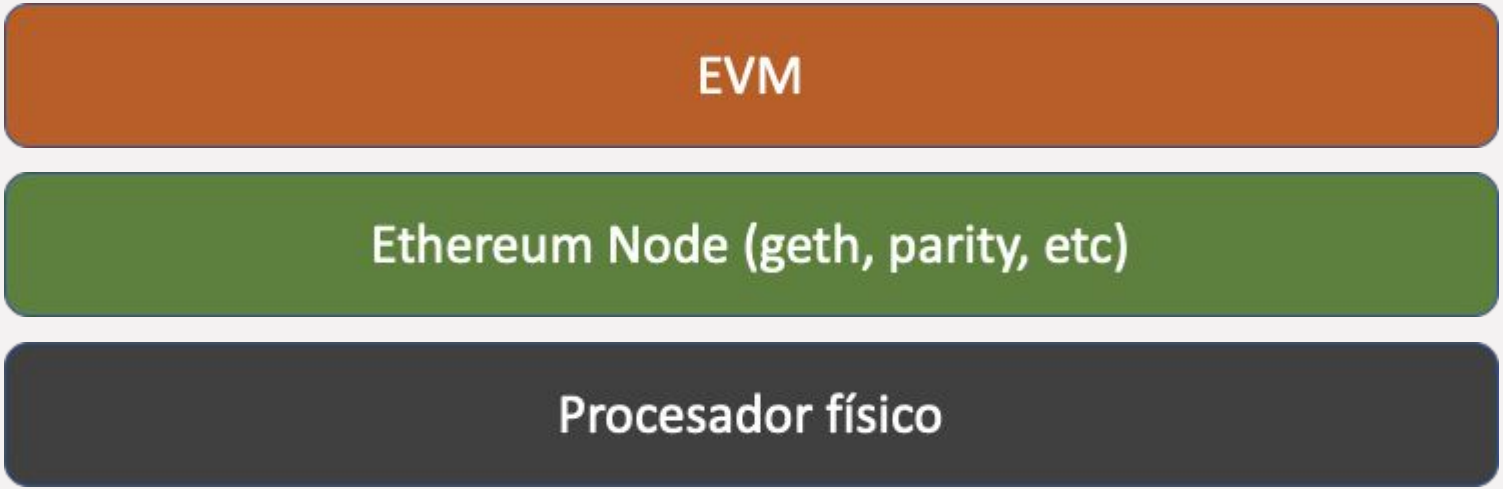
EVM - Layers

EVM - Layers

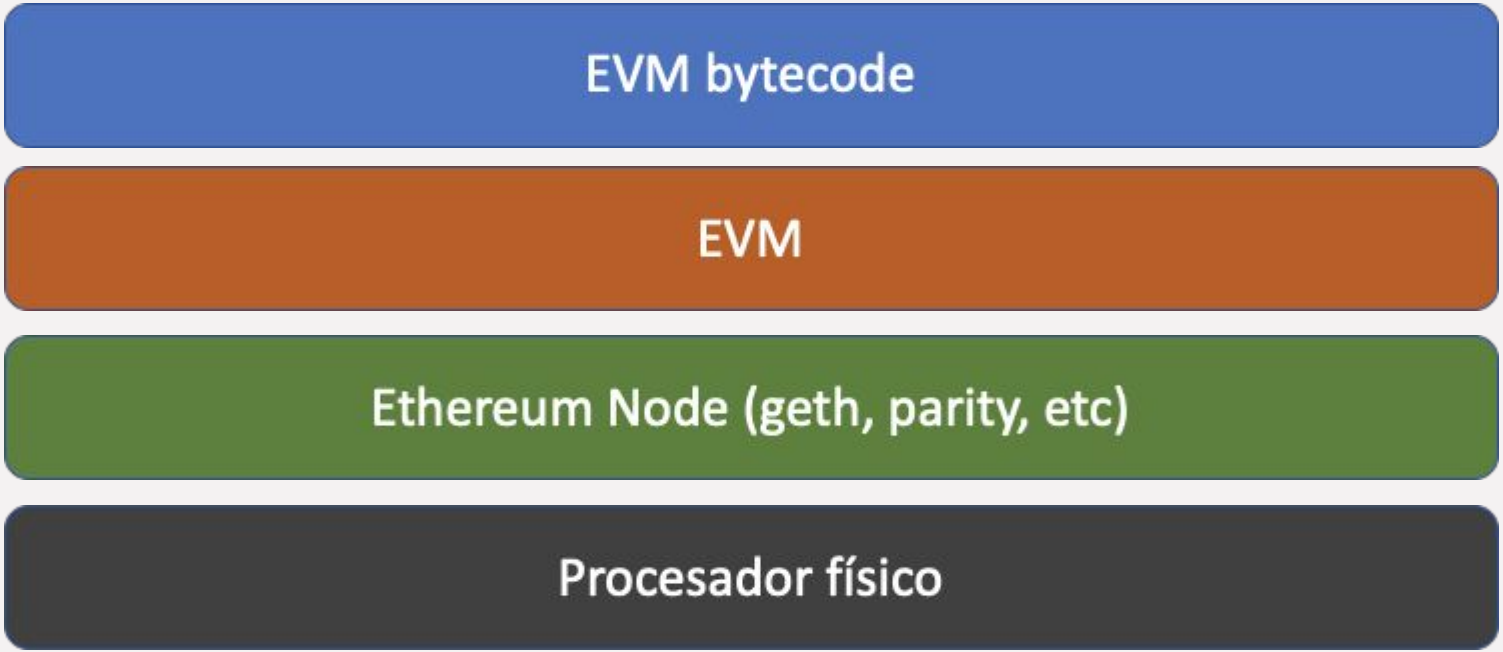
EVM - Layers



EVM - Layers

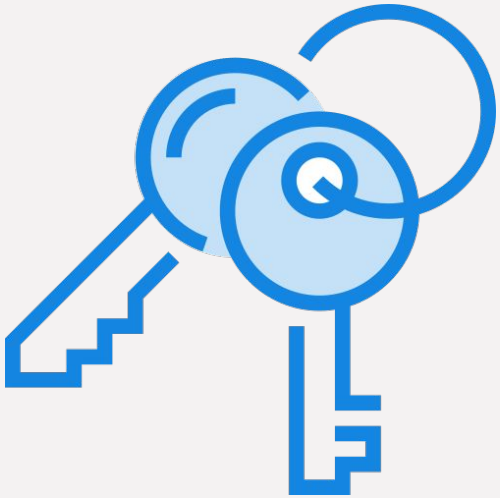


EVM - Layers


EVM bytecode
EVM
Ethereum Node (geth, parity, etc)
Procesador físico

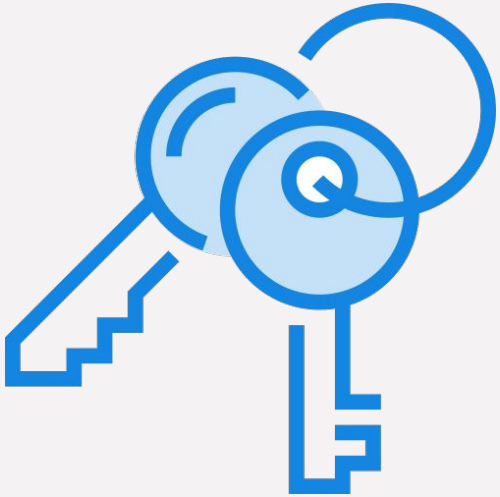
EVM - Tipos de cuentas

EVM - Tipos de cuentas

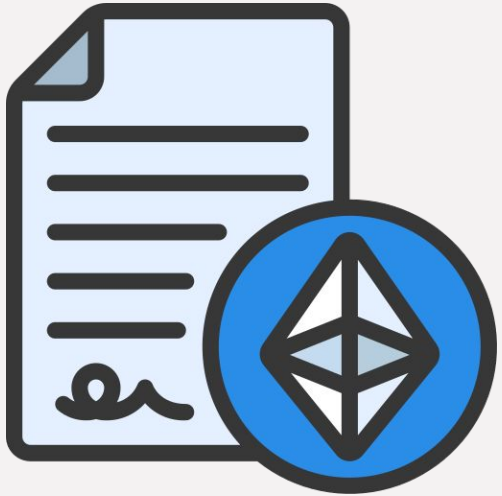


EOA
(External Owned Account)

EVM - Tipos de cuentas



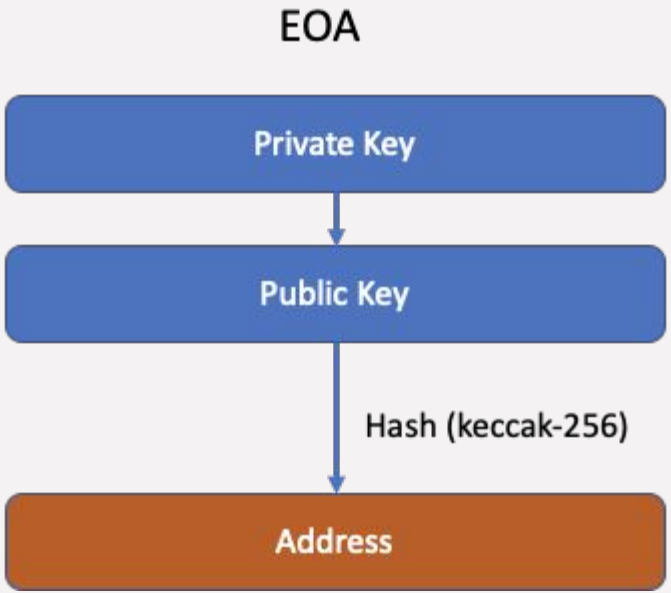
EOA (External Owned Account)



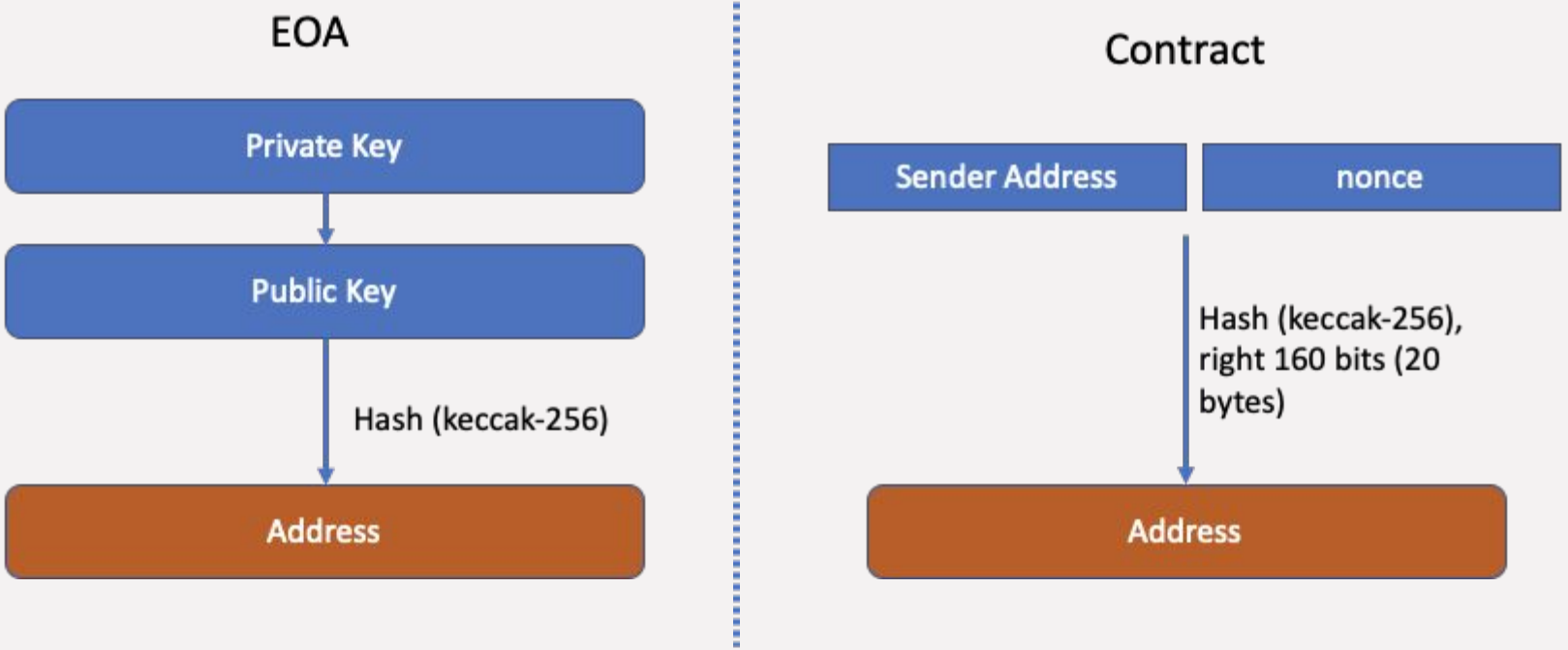
Contratos

EVM - Tipos de cuentas - Cómo se generan las cuentas?

EVM - Tipos de cuentas - Cómo se generan las cuentas?



EVM - Tipos de cuentas - Cómo se generan las cuentas?



EVM - Bytecode y ABI

EVM - Bytecode y ABI

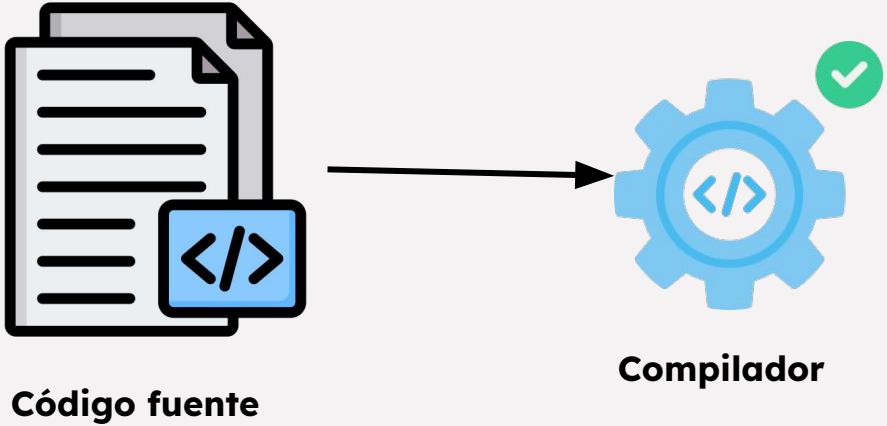
Código fuente

EVM - Bytecode y ABI

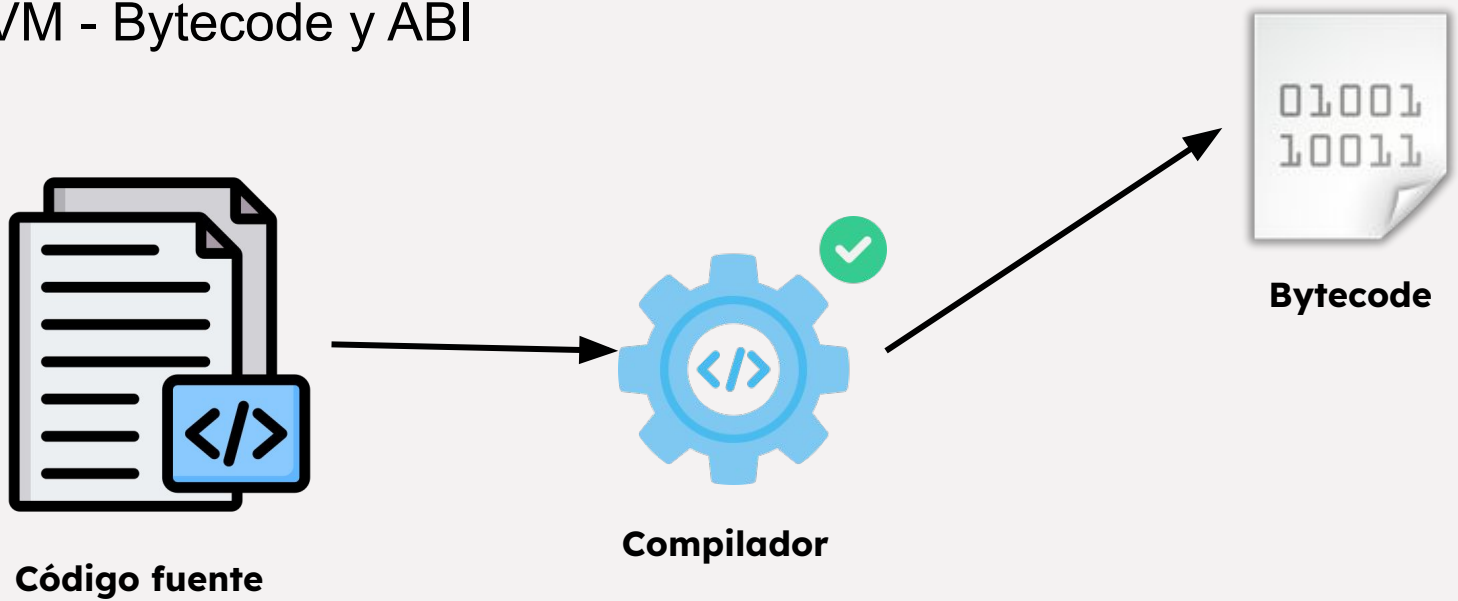
Código fuente

```
8  contract HelloWorld {
9      string private greeting;
10
11     /**
12      * @dev Constructor sets the initial greeting
13      * @param _greeting Initial greeting message
14      */
15     constructor(string memory _greeting) {
16         greeting = _greeting;
17     }
18
19     /**
20      * @dev Returns the current greeting
21      * @return Current greeting message
22      */
23     function getGreeting() public view returns (string memory) {
24         return greeting;
25     }
26
27     /**
28      * @dev Updates the greeting message
29      * @param _greeting New greeting message
30      */
31     function setGreeting(string memory _greeting) public {
32         greeting = _greeting;
33     }
34 }
```

EVM - Bytecode y ABI

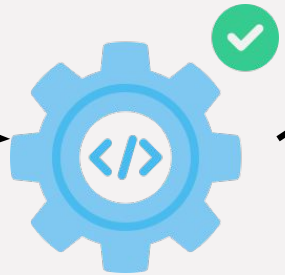


EVM - Bytecode y ABI



EVM - Bytecode y ABI

Código fuente

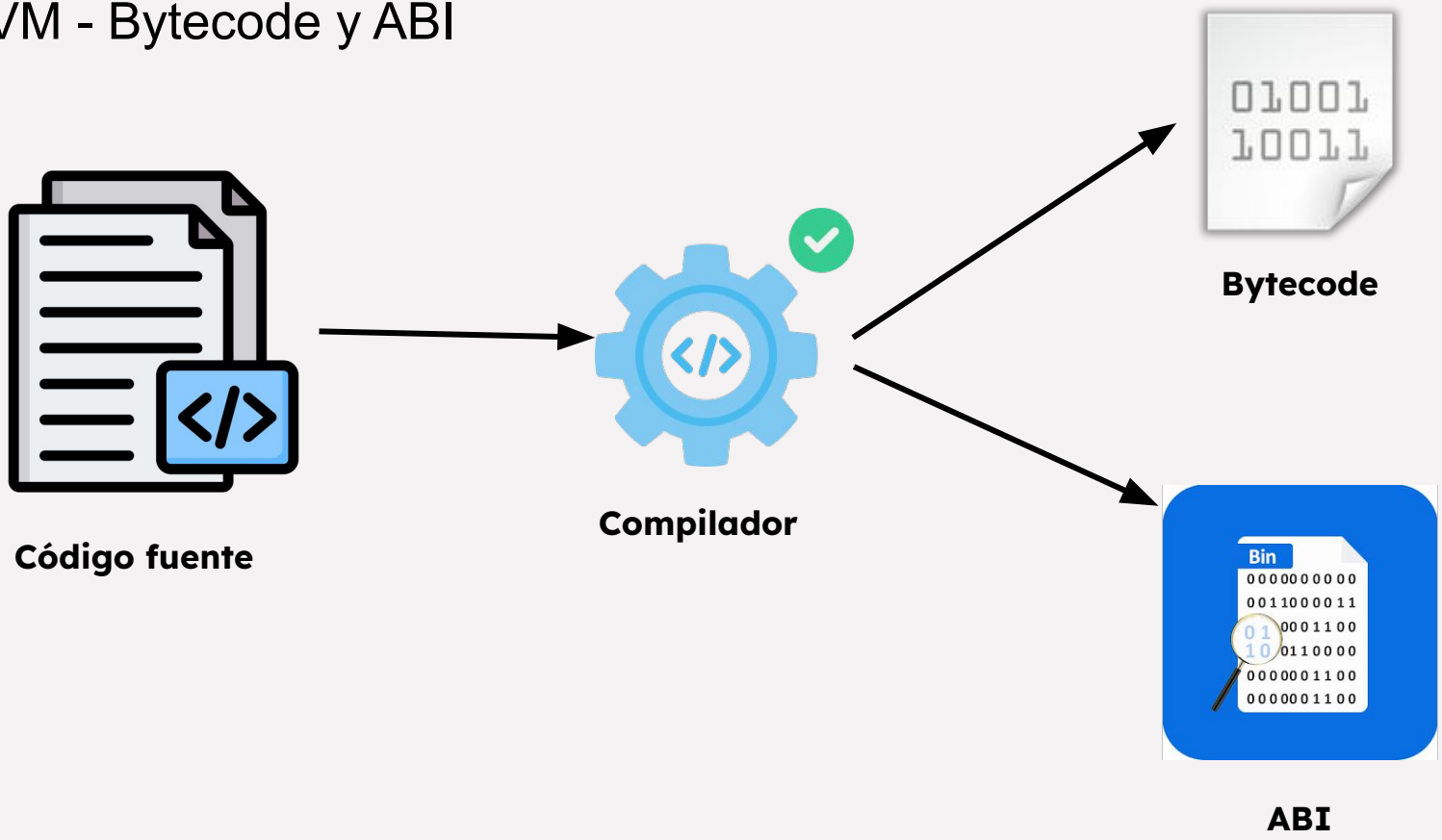


Compilador

Bytecode

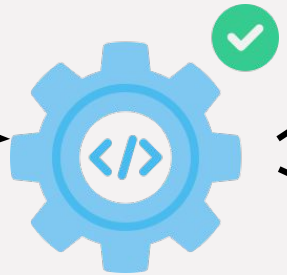

```
"bytecode":
"0x6080604052348015610010576000080fd5b50604051610b84380380610b8483398181016040528101906100329190610 1bd565b806000908161004191906104275650b50506104f9565b6000604051905090565b600080fd5b600080fd5b600080fd5b600080fd5b6000601f19601f830116905091905050565b7f4e487b7100000000000000000000000000000000000000000000000000000000600052604160045260246000fd5b6100af82610066565b810181811067ffffffffffffffff82111715610 0ce576100cd610077565b5b80604052505050565b60006100e1610048565b90506100ed82826100a6565b9190505065b600067ffffffffffffffff82111561010d5761010c610077565b5b6101168261006656 5b905060208101905091905050565b60005b838110156101415780820151818401526020810190506101265656b60008484015250505050565b600061016061015b846100f2565b6100d7565b90508281526020810184848401111561017c5761017b610061565b5b61018784828561012356 5b509392505050565b60008261f8301126101a4576101a361005c565b5b81516101b484826020860161014d565b91505092915050565b60006020828403121561 01d3576101d2610052565b5b600082015167ffffffffffffffff8111156101f1576101f0610057565b5b6101fd8482850161018f565b91505092915050565b600081519050919050565b7f4e487b7100000000000000000000000000000000000000000000000000000000600052602260045260246000fd5b60006002820490506001821680610257 607f821691505b6020821081036102 6b5761026a610211565b5b5091905056 5b600081905081600052602060002090509190505065b60006020601f8301049050919050565b600082821b905092915050565b6000600883026102d37fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff82610296565b6102dd8683610296565b9550801984169350808616841792505050939250505056 5b600081905091905056 5b600081905091905056 5b600061032461031f61031a846102f5565b6102ff565b6102f5565b9050919050565b600081905091905056 5b61033e83610309565b61035261034a8261032b565b8484546102a3565b825550505050565b600090565b61036761035a565b61037281848461033556 5b505050565b5b8
```

EVM - Bytecode y ABI



EVM - Bytecode y ABI

Código fuente



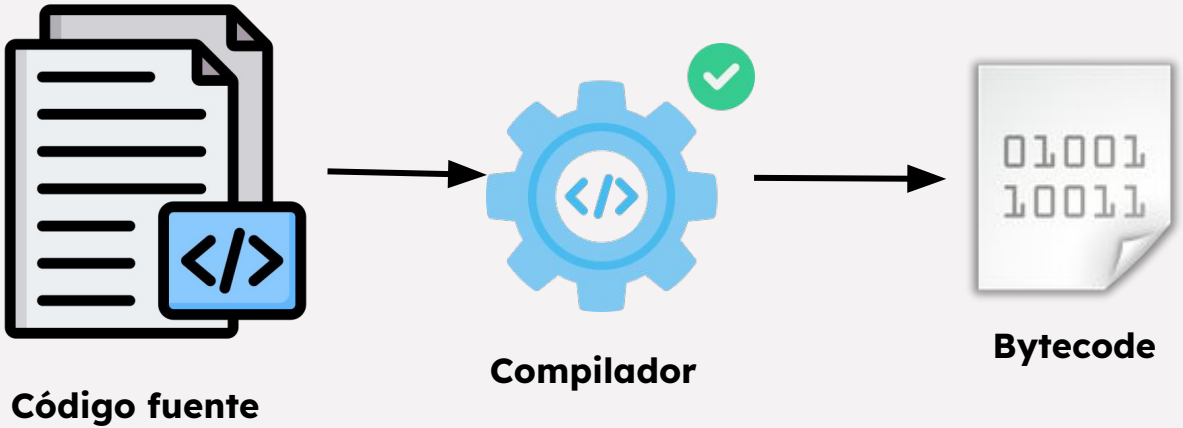
Compilador

Byte

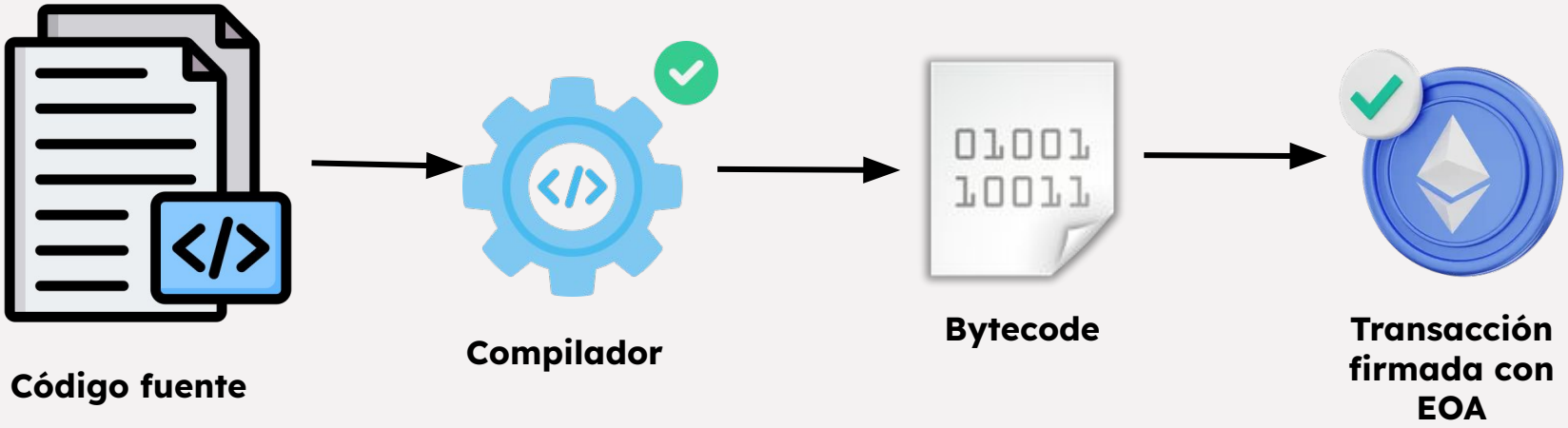
ABI

EVM - Deploy

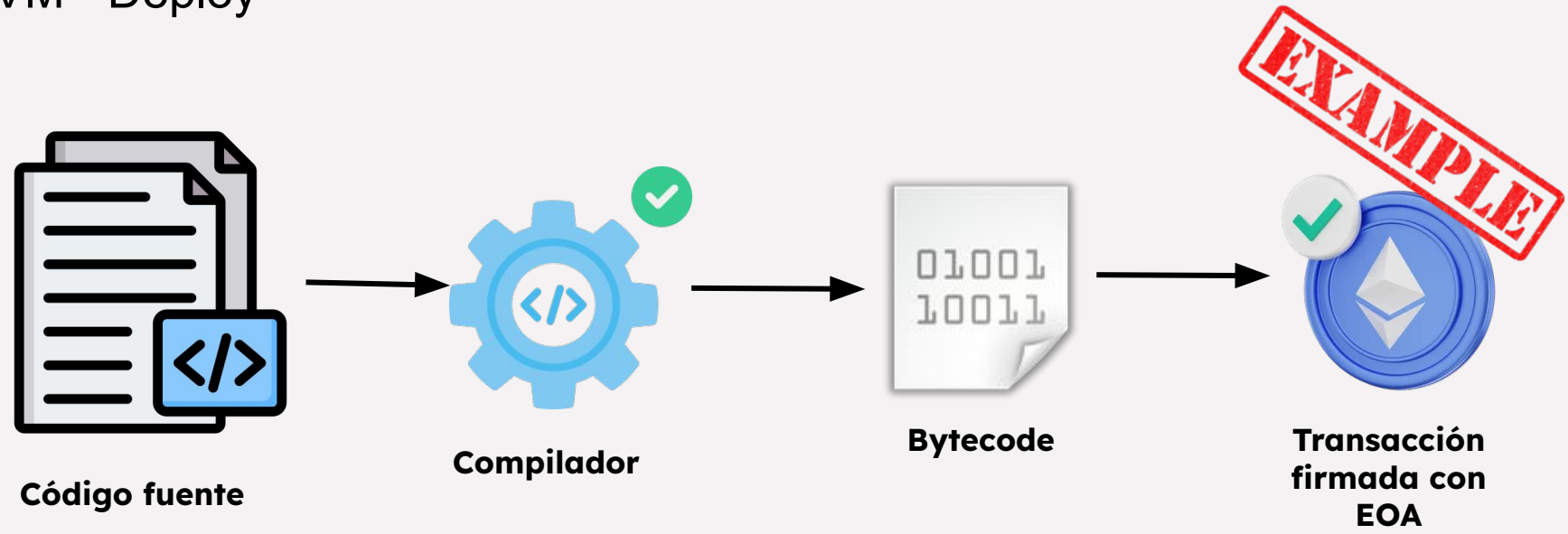
EVM - Deploy



EVM - Deploy


01001
10011
Código fuente
Compilador
Bytecode
Transacción firmada con EOA

EVM - Deploy

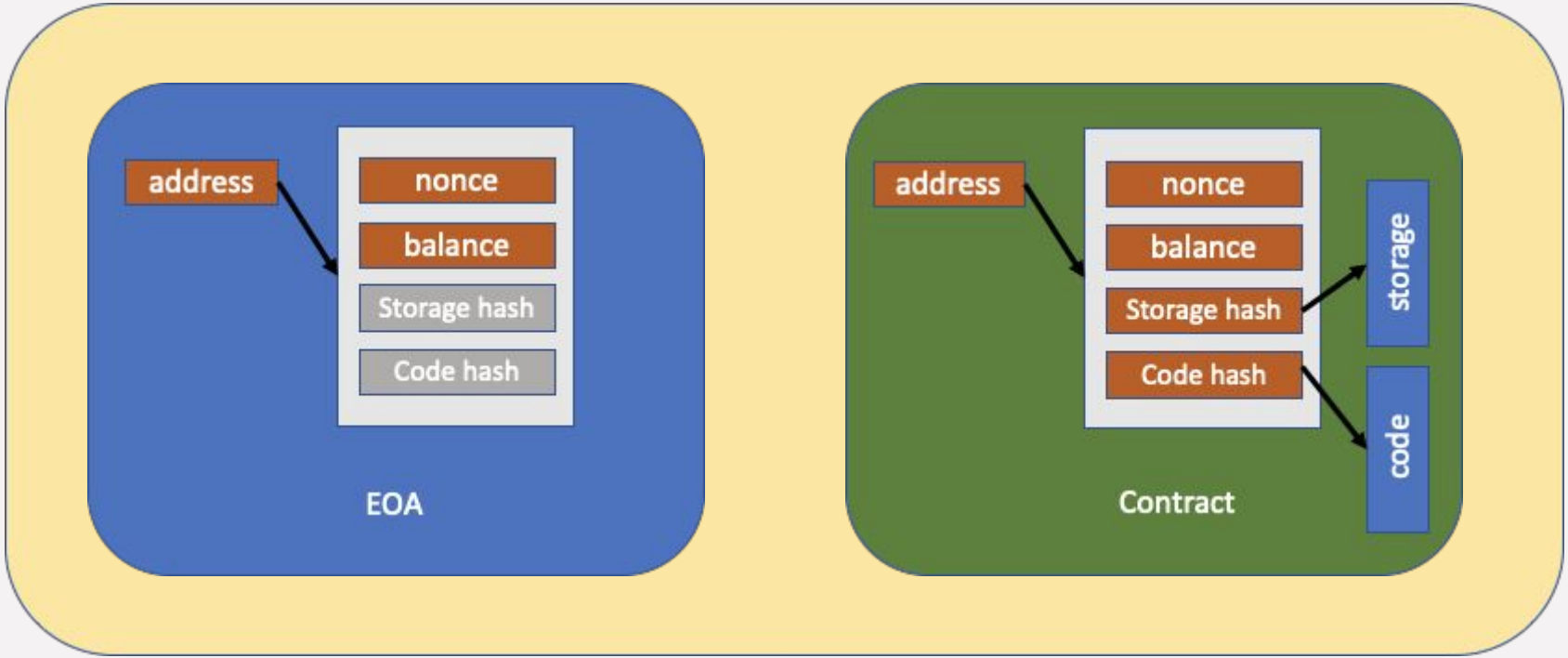


https://drive.google.com/file/d/1sevzrtX9rUtwS_3XCevnpqyDqZBQ6kRw/view?usp=drive_link

EVM - World State

EVM - World State

EVM - World State



EVM - Gas

EVM - Gas

Utilizado para pagar los costos de la red
Se utilizan para pagar los costos de transacción

EVM - Gas

Utilizado para pagar los costos de la red
Se utilizan para pagar los costos de transacción

A nivel de transacción
Gas price, Gas limit, Gas usado

EVM - Gas

Utilizado para pagar los costos de la red
Se utilizan para pagar los costos de transacción

A nivel de transacción
Gas price, Gas limit, Gas usado

A nivel de bloque
Gas limit, Gas usado

EVM - Gas

Utilizado para pagar los costos de la red
Se utilizan para pagar los costos de transacción

A nivel de transacción
Gas price, Gas limit, Gas usado

A nivel de bloque
Gas limit, Gas usado

En el London Fork (ERC-1559) se cambió el esquema
Se agrego la quema de tokens según la congestión de la red

EVM - Gas

Utilizado para pagar los costos de la red
Se utilizan para pagar los costos de transacción

A nivel de transacción
Gas price, Gas limit, Gas usado

A nivel de bloque
Gas limit, Gas usado

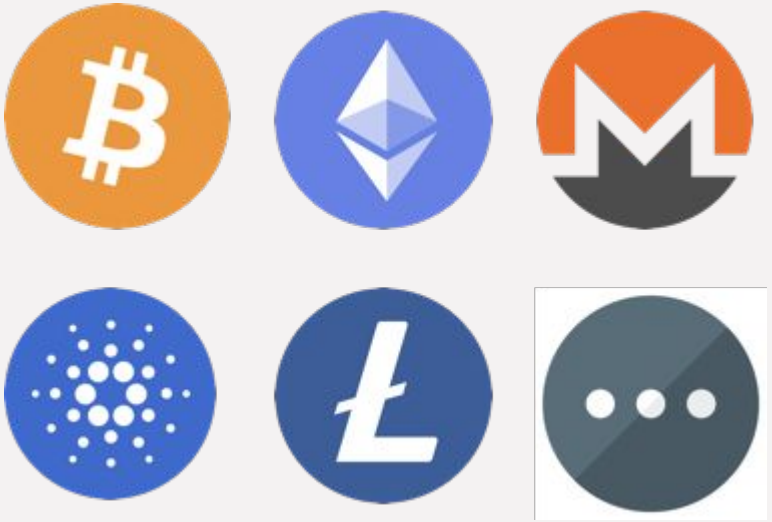
En el London Fork (ERC-1559) se cambió el esquema
Se agrego la quema de tokens según la congestión de la red

Ethereum - Tokens

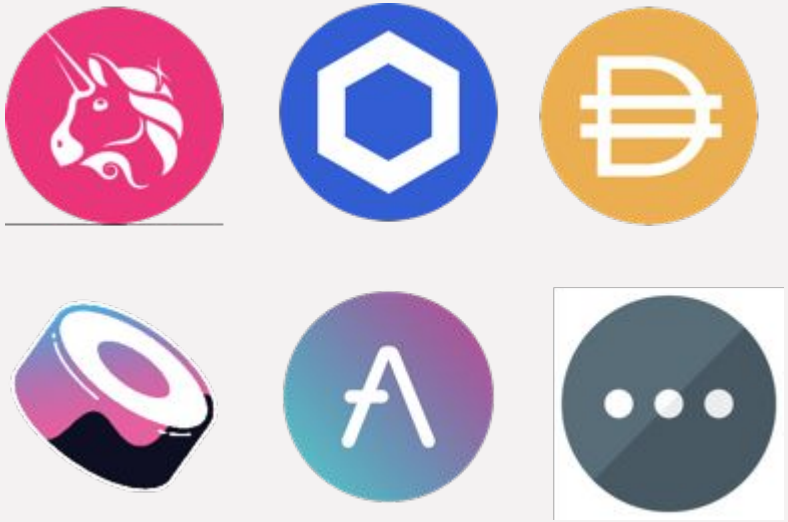
Ethereum - Tokens

Ethereum - Tokens

NATIVAS



PROYECTOS



Ethereum - Tokens

Fungible

No Fungible

Ethereum - Tokens

Ethereum - Tokens

ICO (Initial Coin Offering)
Utilizado para financiar proyectos

Ethereum - Tokens

ICO (Initial Coin Offering)
Utilizado para financiar proyectos

ERC20
Fungible, supply fijo

Ethereum - Tokens

ICO (Initial Coin Offering)
Utilizado para financiar proyectos

ERC20
Fungible, supply fijo

ERC721
No fungible

Ethereum - Tokens

ICO (Initial Coin Offering)
Utilizado para financiar proyectos

ERC20
Fungible, supply fijo

ERC721
No fungible

ERC621
ERC20 con soporte variable de supply (mint y burn)