



El futuro digital
es de todos

MinTIC



Blockchain

& analítica de datos
para industrias digitales



Agenda

- Identidad autosoberana
- Despliegue contratos inteligentes.



El futuro digital
es de todos

MinTIC



Identidad digital

- Se puede como un conjunto finito de atributos que permite a una persona, animal, cosa o proceso ser identificado como único y probar su identidad frente a terceros electrónicamente. Nuestra persona digital se compone de varias identidades digitales, estando a su vez cada una de estas identidades representada por uno o varios identificadores y atributos que son únicos en un contexto específico



- La cual implica que cada persona tiene el control total de su propia identidad, gestionando su propia información y relaciones, y siendo independiente de cualquier organización, por lo que nadie puede violar su privacidad ni quitarle su identidad.

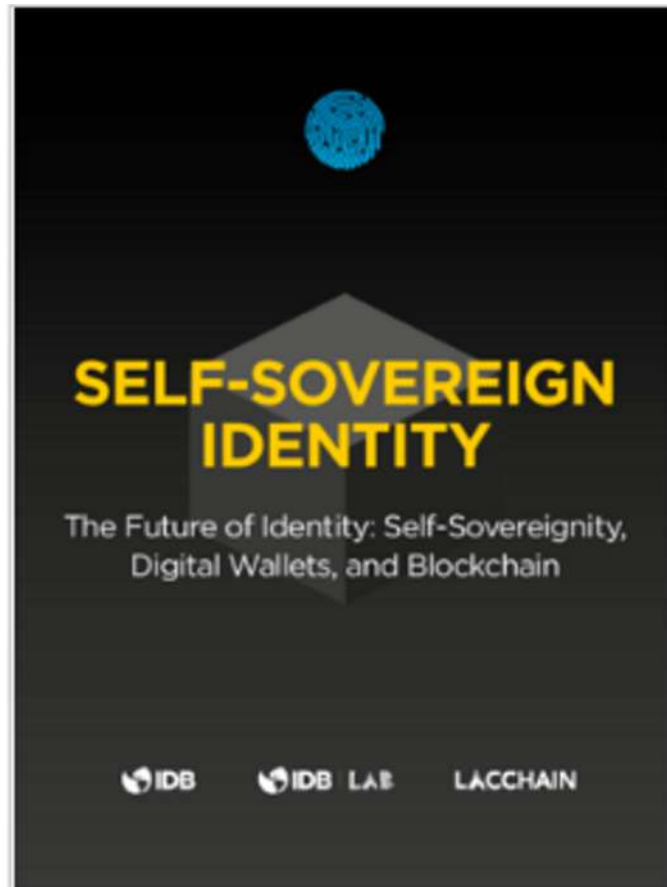
Identidad autosoberana

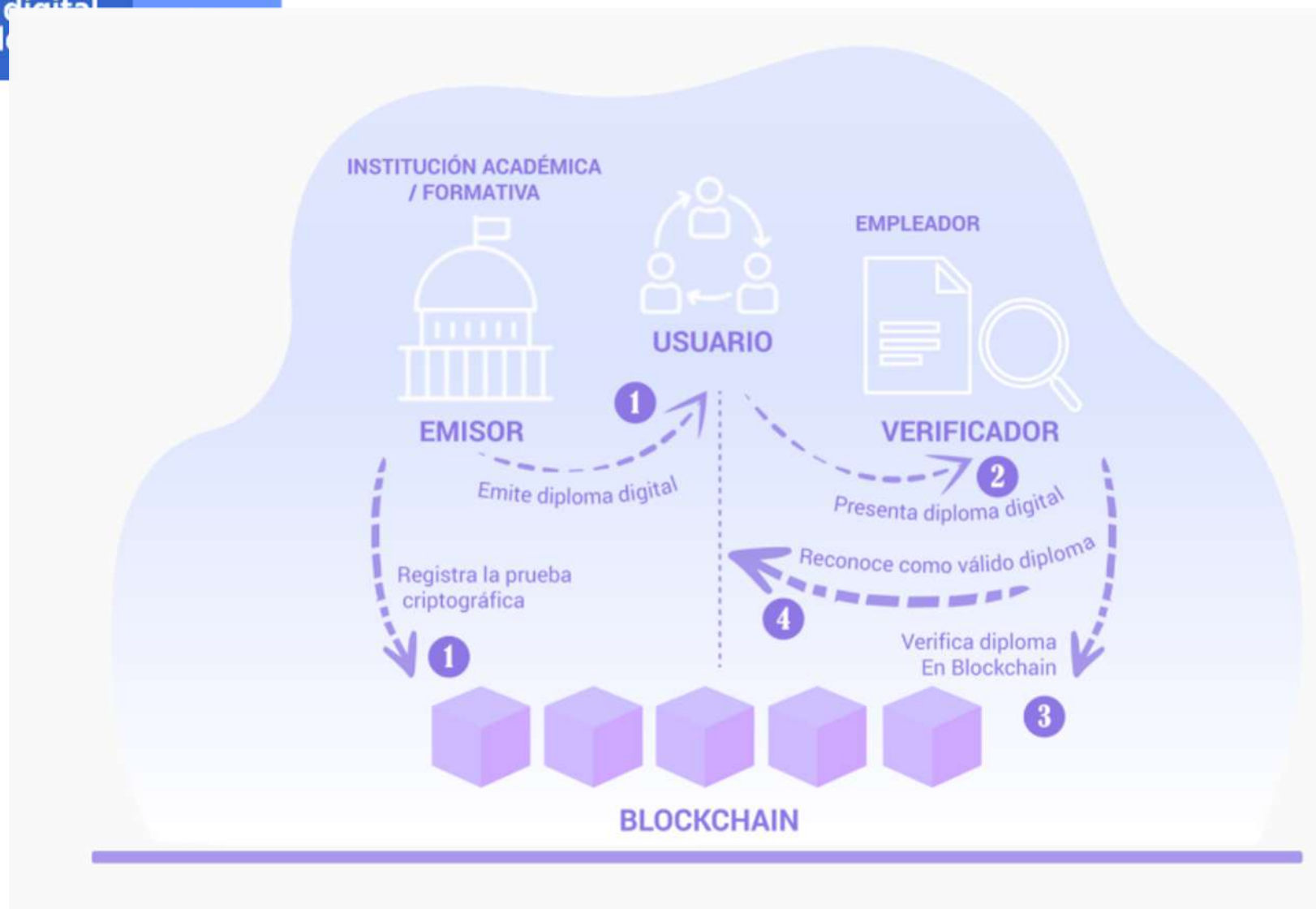




El futuro digital
es de todos

MinTIC





Zero Knowledge Proof

- ¿Es posible demostrar que algo es verdad sin desvelar los datos que lo prueban? Es lo que propone la tecnología 'Zero Knowledge Proof', o Prueba de Conocimiento Cero, una técnica que emplea algoritmos criptográficos para que varias partes puedan verificar la veracidad de una información sin necesidad de compartir los datos que la componen.



'Zero Knowledge' | Ejemplo intuitivo



GANACHE



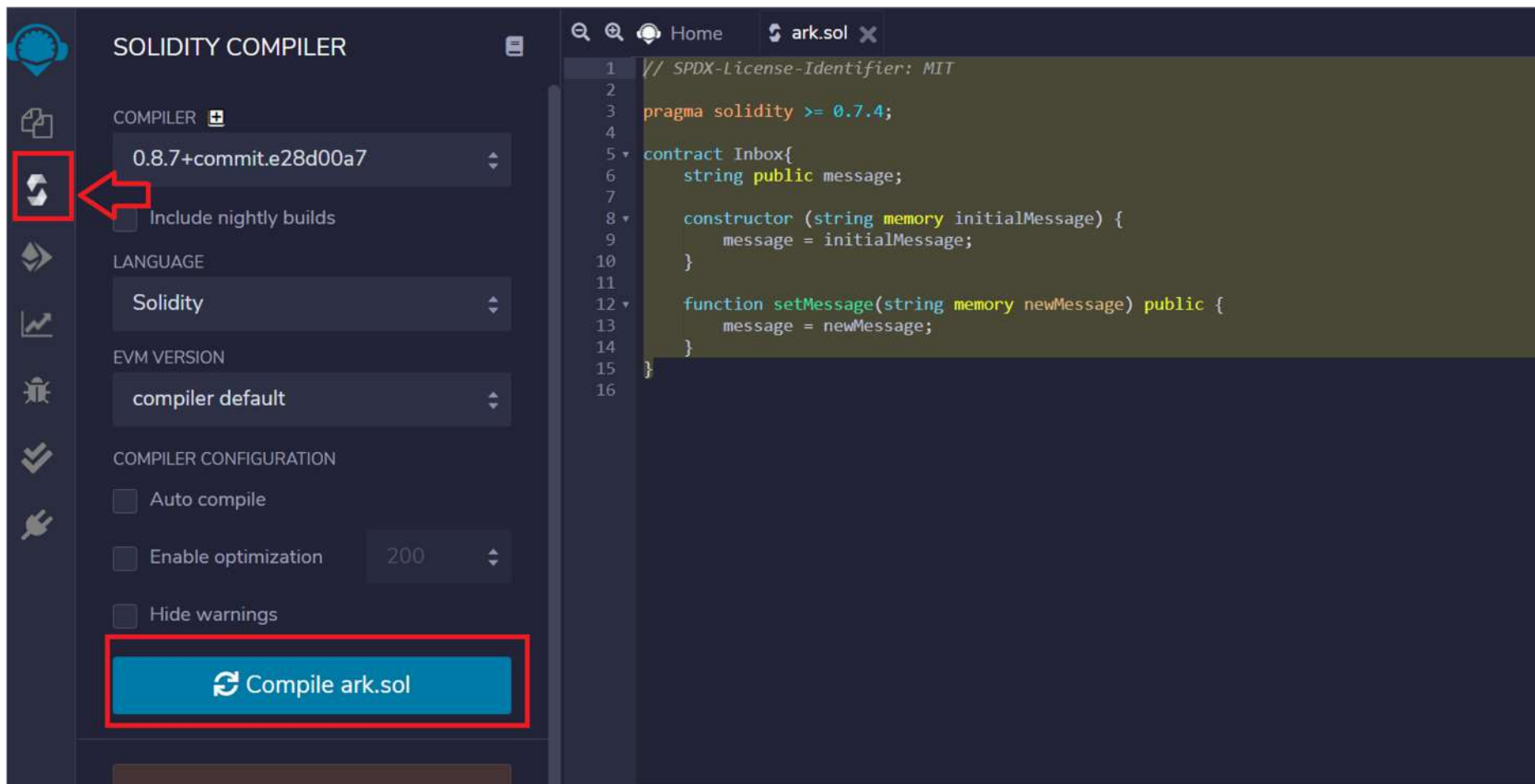
Ganache



PYTHON

- `pip install web3`





The screenshot shows the Solidity Compiler interface. On the left sidebar, the 'Compiler' section is active, showing the version '0.8.7+commit.e28d00a7'. A red box highlights the refresh icon (a circular arrow) next to the version dropdown, with a red arrow pointing to it. Below the version, there are checkboxes for 'Include nightly builds', 'Auto compile', 'Enable optimization' (set to 200), and 'Hide warnings'. At the bottom of the sidebar, a large blue button labeled 'Compile ark.sol' is highlighted with a red rectangle. The main editor area on the right displays the Solidity code for 'ark.sol'.

```
1 // SPDX-License-Identifier: MIT
2
3 pragma solidity >= 0.7.4;
4
5 contract Inbox{
6     string public message;
7
8     constructor (string memory initialMessage) {
9         message = initialMessage;
10    }
11
12    function setMessage(string memory newMessage) public {
13        message = newMessage;
14    }
15 }
16
```

compiler default

COMPILER CONFIGURATION

☐

Auto compile

☐

Enable optimization200

☐

Hide warnings

Compile mintic.sol

CONTRACT

Inbox (mintic.sol)

Publish on Ipfs

Compilation Details

ABI

Bytecode

CONTRACT

Inbox (mintic.sol)

Publish on Ipfs

Compilation Details

Copied

ABI

Bytecode

```
[
  {
    "inputs": [
      {
        "internalType": "string",
        "name": "initialMessage",
        "type": "string"
      }
    ],
    "stateMutability": "nonpayable",
    "type": "constructor"
  },
  {
    "inputs": [],
    "name": "message",
    "outputs": [
      {
        "internalType": "string",
        "name": "",
        "type": "string"
      }
    ],
    "stateMutability": "view",
    "type": "function"
  },
  {
    "inputs": [
      {
        "internalType": "string",
        "name": "newMessage",
        "type": "string"
      }
    ],
    "name": "setMessage",
    "outputs": [],
    "stateMutability": "nonpayable",
    "type": "function"
  }
]
```

Ganache

ACCOUNTS

BLOCKS

TRANSACTIONS

CONTRACTS

EVENTS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK
0

GAS PRICE
20000000000

GAS LIMIT
6721975

HARDFORK
MUIRGLACIER

NETWORK ID
5777

RPC SERVER
HTTP://127.0.0.1:7545

MINING STATUS
AUTOMINING

WORKSPACE
MINTIC_RED

SWITCH

MNEMONIC ?
blush lyrics category found green brisk hold valley test balcony clarify cousin

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS 0x052dCcFA344244453f6C333329d716573F0e01E8	BALANCE 200.00 ETH	TX COUNT 0	INDEX 0	
ADDRESS 0xA88F054c3C74942B00968A5Cc85D6057E9ad9ec8	BALANCE 200.00 ETH	TX COUNT 0	INDEX 1	
ADDRESS 0xb5aE1BFF28Ab16C6F7112d4E0c2c26cdAE957205	BALANCE 200.00 ETH	TX COUNT 0	INDEX 2	
ADDRESS 0x2B97D256a1c410Af17231B077BcCf1FB5EDfD9E5	BALANCE 200.00 ETH	TX COUNT 0	INDEX 3	
ADDRESS 0x60BEA7969E3A0d59fd6a3b0Be7DD2e1364B40aeA	BALANCE 200.00 ETH	TX COUNT 0	INDEX 4	
ADDRESS 0x843B8d01EeD61318eFfA40f96AfCC906E08fF673	BALANCE 200.00 ETH	TX COUNT 0	INDEX 5	
ADDRESS 0x8b2945047c444C036834af30F3Ae1718341f71B1	BALANCE 200.00 ETH	TX COUNT 0	INDEX 6	





El futuro digital
es de todos

MinTIC

Gracias

