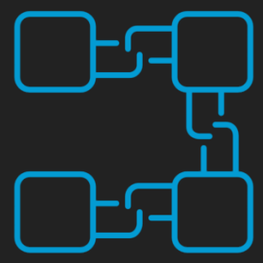


Blockchain

GRAIN CHAIN

MANUEL DE JESUS TOALA PEREZ

AGENDA

- Que es blockchain
- Características
- Tipos de blockchain
- Ventajas y desventajas
- Smart Contracts
- Ejemplos de aplicación

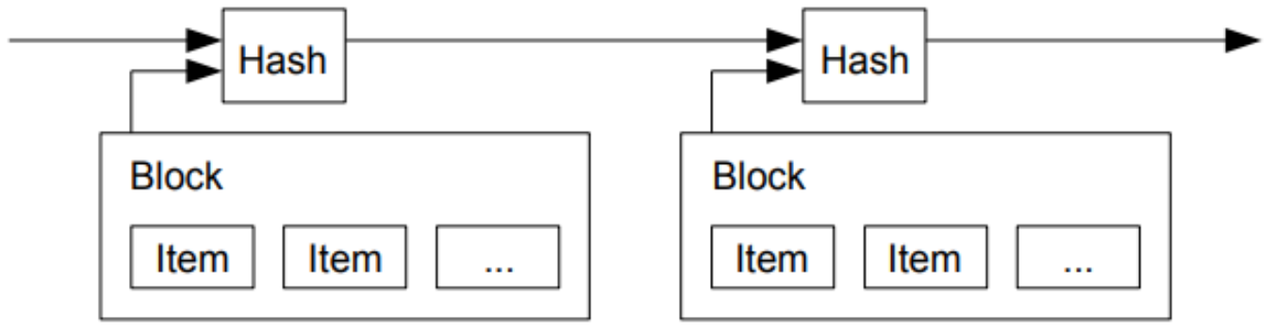
ORIGEN BLOCKCHAIN

- 1991. Stuart Haber y W. Scott Stornetta
  - Bloques y Marcas de Tiempo
- 1992. Bayer, Haber and Stornetta
  - Merkie Tree
- 2008 Satoshi Nakamoto
  - Se Publica en Octubre "Bitcoin: A Peer-to-Peer Electronic Cash System"
- 2009 Satoshi Nakamoto
  - Publica la versión 0.1 de bitcoin

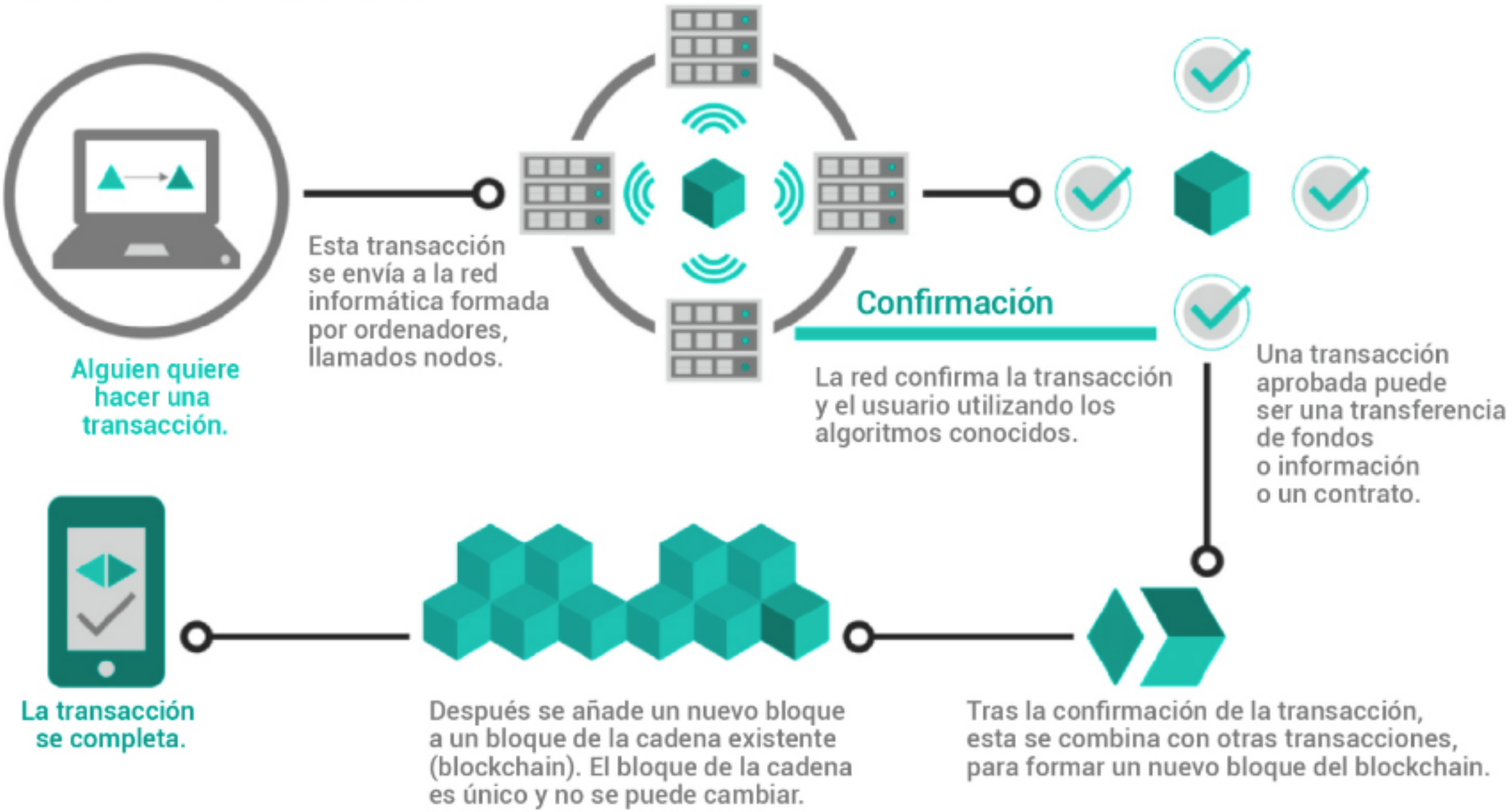
QUE ES BLOCKCHAIN

Una cadena de bloques (block chain), también conocida como libro de contabilidad distribuido (distributed ledger), es una base de datos distribuida que registra bloques de información y los entrelaza para facilitar la recuperación de la información y la verificación de que ésta no ha sido cambiada.

- Trazabilidad
- Inmutabilidad
- Mecanismo de consenso
- Transparencia
- Smart Contracts



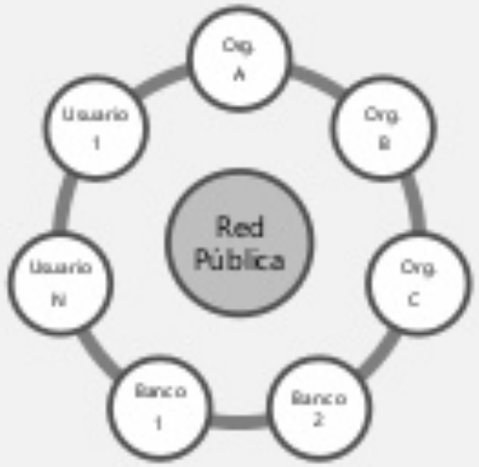
¿Por qué blockchain es tan segura?



- Cada nodo de la red almacena una copia exacta de la cadena
- Registro consensuado
- Cada bloque está matemáticamente vinculado

Tipos de blockchain

Blockchain Público



Muchos, **participantes desconocidos**

Anónimos o seudo-anónimos

Todos los participantes **pueden leer y escribir**

Consenso basado en **Pruebas de Trabajo**

Blockchain Empresarial

Privado

Consorcio

Solo participantes aprobados

Usuarios con **identidades conocidas**

La autorización es requerida para escribir, leer y participar en la confirmación de las transacciones

Múltiple **algoritmos para el consenso**

Nombre	Acrónimo	Año	*Blockchain*	Consenso	Tiempo bloque	Confirmación	Privacidad	Max tps[5]	Máximo monedas	Criptografía POW	Consumo Energía
Bitcoin	BTC	2009	Público	POW	10 minutos	1 hora	Media-baja	3-7	21 millones	SHA256	Muy alto
Ether	ETH	2015	Público (propio)	POW	14 segundos	3 minutos	Media-baja	15	18 millones por año	ethcash	Alto
Bitcoin Cash	BCH	2017	Público (parte de *bitcoin*)	POW	variable (18minutos media)	2 horas	Media-baja	28	21 millones	SHA256	Alto
Ripple	XRC	2012	Privado (Ripplenet)	Ripple	4 segundos	4 segundos	Buena (privado)	1500	100 millones	-	muy bajo
Litecoin	LTC	2011	Público (basado en *bitcoin*)	POW	2.5 minutos	15 minutos	Media-baja	28	84 millones	Scrypt	Alto
Dash	DASH	2014	Público (basado en *bitcoin*)	POW + POS (service)	2.5 minutos	minutos (opc. instantáneo)	Alta (opcional)	1500-3500	19 millones	other	muy alto
Bitconnect	BCC	2016	Público (propio)	POS + POS (stake)	minutos	minutos	Media-baja		28 millones	?	Alto
Antshares/NEO	NEO	2016	Público (propio)	dBTF	segundos	segundos	Media-baja	1000	100 millones	NeoQS	Alto
NEM	XEM	2015	Público (propio)	POI	1 minuto	minutos	Media-baja	>100	9000 millones	-	Bajo

SMART CONTRACT

1. Es un programa informático

2. Ejecuta acuerdo entre 2 o más partes

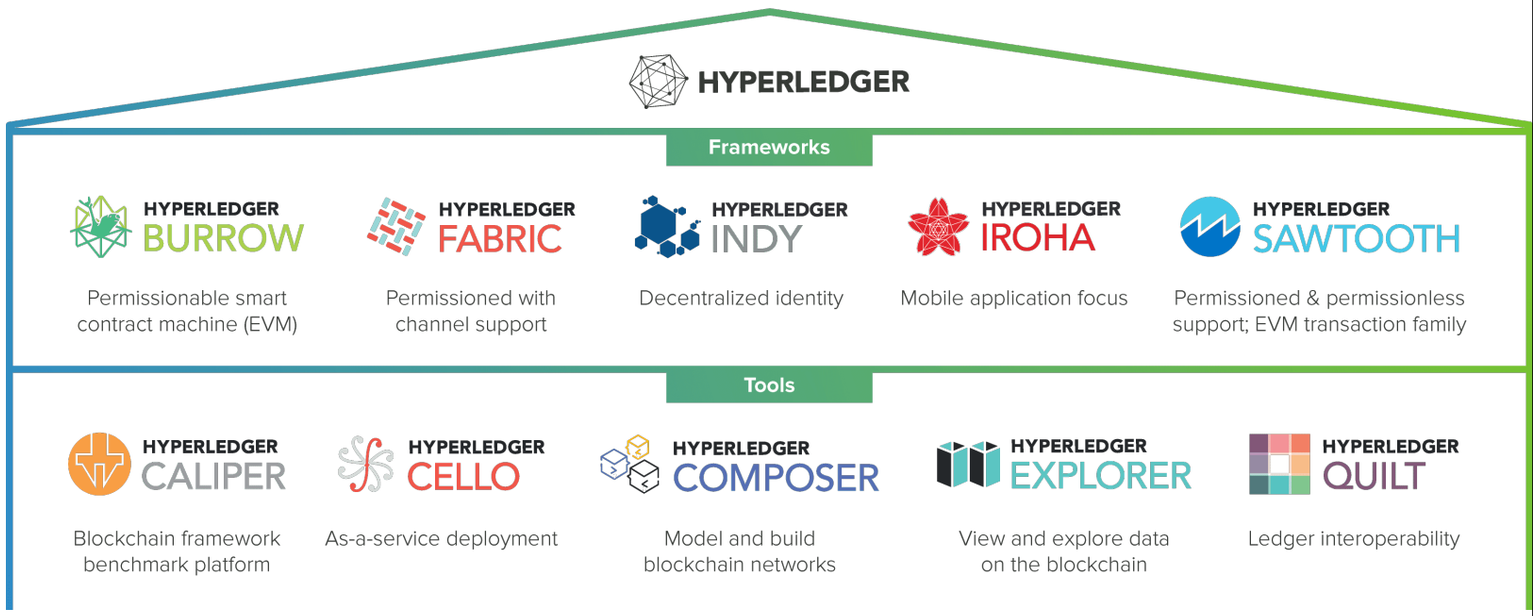
3. Se ejecuta en un sistema no controlado por ninguna de las mismas

4. Cuando se cumple una condición pre-programada, el programa ejecuta la cláusula contractual correspondiente

TIPOS DE SMART CONTRACT

ethereum

HYPERLEDGER



Origen. 2014 por Vitalik Buterin.

- Plataforma Open Source
- Smart Contracts
- Moneda Ether
- Gas para poder ejecutar nuestros contratos

ETHEREUM

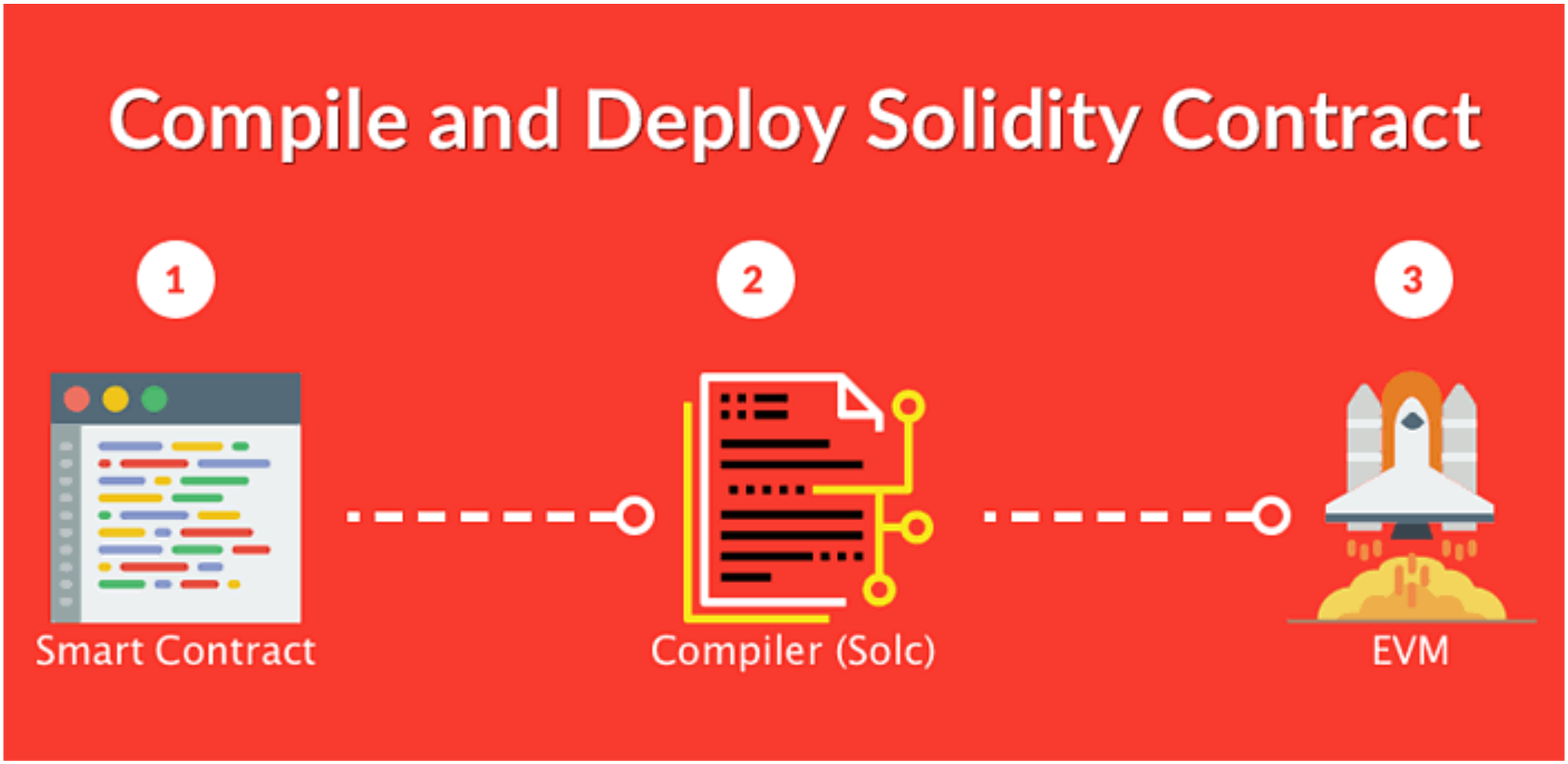
Ethereum virtual machine(EVM)

- 1 de Marzo tenemos 27,500 nodos en el main ethereum network
- Implementaciones
  - Go
  - Python
  - JavaScript
  - Ruby
  - Rust

Que tiene la EVM

- Es determinista
- Es terminable
- Esta aislado

TEXTO


Compile and Deploy Solidity Contract
1
2
3
Smart Contract
Compiler (Solc)
EVM

LOS LENGUAJES DE LOS SMART CONTRACT EN ETHEREUM

- Solidity
- Serpent - Deprecado
- LLL (Lisp)
- Mutan(go) deprecado
- Viper (python) - En desarrollo

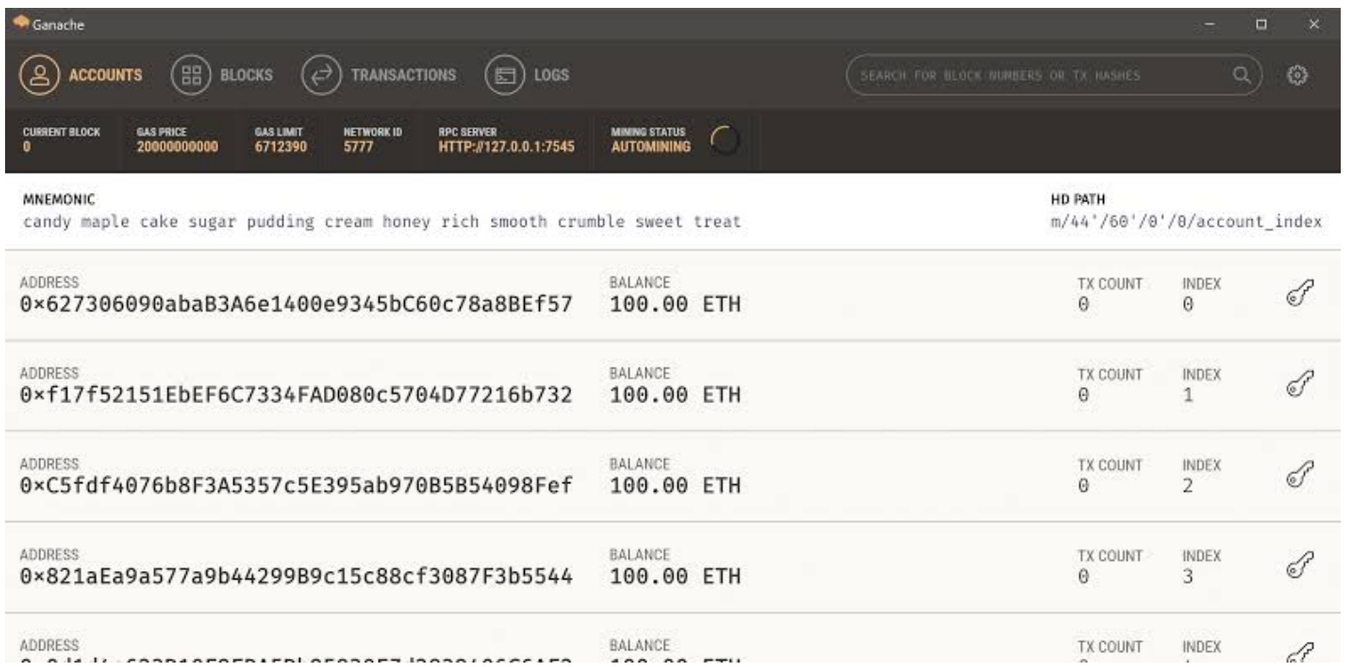
POR DÓNDE COMIENZO

openzeppelin

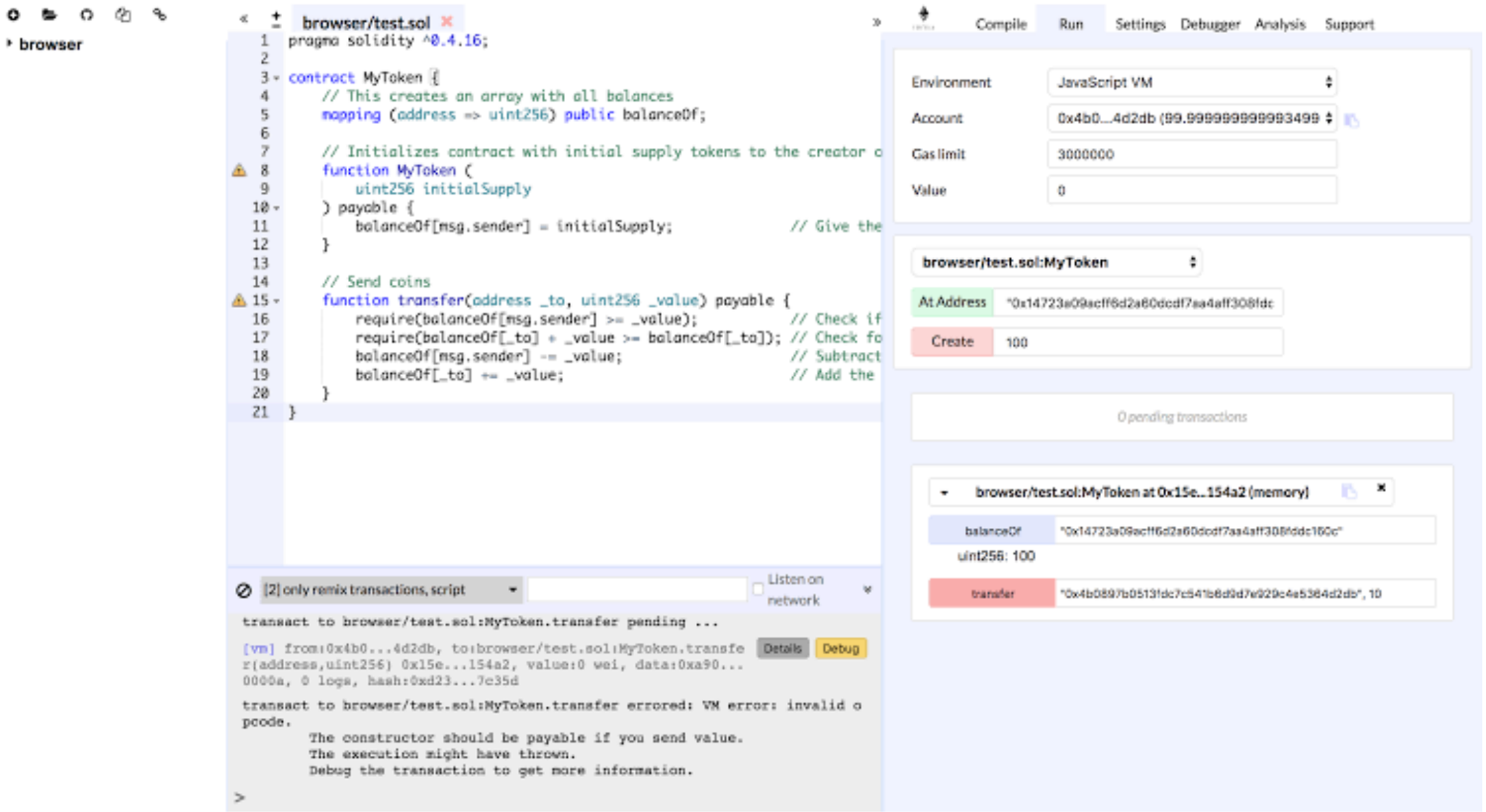
TRUFFLE

drizzle

METAMASK



REMIX IDE


browser
browser/test.sol
pragma solidity ^0.4.16;
contract MyToken {
// This creates an array with all balances
mapping (address => uint256) public balanceOf;
// Initializes contract with initial supply tokens to the creator o
function MyToken (
uint256 initialSupply
) payable {
balanceOf[msg.sender] = initialSupply; // Give the
}
// Send coins
function transfer(address _to, uint256 _value) payable {
require(balanceOf[msg.sender] >= _value); // Check if
require(balanceOf[_to] + _value >= balanceOf[_to]); // Check fo
balanceOf[msg.sender] -= _value; // Subtract
balanceOf[_to] += _value; // Add the
}
}
Compile
Run
Settings
Debugger
Analysis
Support
Environment
JavaScript VM
Account
0x4b0...4d2db (99.99999999993499
Gas limit
3000000
Value
0
browser/test.sol:MyToken
At Address
0x14723a09acff6d2a60dcdf7aa4aff308fdc
Create
100
0 pending transactions
browser/test.sol:MyToken at 0x15e...154a2 (memory)
balanceOf
"0x14723a09acff6d2a60dcdf7aa4aff308fddc160c"
uint256: 100
transfer
"0x4b0897b0513fdc7c541b6d9d7e929c4e5364d2db", 10
[2] only remix transactions, script
Listen on network
transact to browser/test.sol:MyToken.transfer pending ...
[vm] from:0x4b0...4d2db, to:browser/test.sol:MyToken.transfe
r(address,uint256) 0x15e...154a2, value:0 wei, data:0xa90...
0000a, 0 logs, hash:0xd23...7c35d
Details
Debug
transact to browser/test.sol:MyToken.transfer errored: VM error: invalid o
pcode.
The constructor should be payable if you send value.
The execution might have thrown.
Debug the transaction to get more information.
>

Transformación Digital de Blockchain

Transformación de Blockchain

Tecnología

Seguridad cibernética
Protección contra el ataque DDoS, el sistema de registros evita la piratería.

Internet de las Cosas
Implementación de sistemas IdC dentro de industrias, aplicaciones IdC para transacciones.

Almacenamiento en la nube
Seguridad adicional con redes descentralizadas, bajos costos de transacción, espacio no utilizado.

Gestion de energia
Energía de bajo costo, transferencias de energía de punto a punto, medición de servicios públicos.

Inteligencia artificial
Mejora de la implementación, automatización y seguridad de la tecnología de inteligencia artificial.

Medios de comunicación

Publicidad
Publicidad y marketing de bajo costo, sin intermediarios.

Gaming
Las plataformas de juego descentralizadas, permiten a los jugadores intercambiar artículos de los juegos.

Ley y Crimen

Policía / ley
Preservación de evidencia, cero datos falsificados, sellos de tiempo, cadena de hechos.

Rastreo de armas
Rastreo de los criminales y preservar la propiedad de la posesión de armas.

Transporte

Negocios de transporte
Acceso a los datos del viaje y seguimiento de la ruta.

Automotriz
Seguimiento de vehículos, gestión de la cadena de suministro, producción e historial de ventas.

Transporte público
Pagos precisos, viajes compartidos, simplificación de viajes.

Entretenimiento

Industria del entretenimiento
Derechos de propiedad, derechos de autor, sistema de contrato inteligente para la compensación del artista.

Industria de la música
No hay descargas ilegales, canales adecuado para compensar a los artistas.

Contratos

Herencias
Validez de los testamentos y sistemas de contratos inteligentes para asegurar la herencia.

Propiedad y Terreno
Información de la propiedad, transparencia en el pago, cambios de propiedad.

Contratos legales
Preservación de documentación legal y contratos. Los contrato inteligente definen las reglas de os contratos.

Finanzas

Finanzas
Mayor eficiencia y seguridad en el sistema bancario y en las transacciones de dinero.

Protección financiera
Preservación de contratos de seguro, validacion del acuerdo y procesos de transacción.

Interfaz bancaria
Más precisión, mejor interfaz, seguridad en las transacciones.

Derechos humanos y contribuciones

Derecho a la información
Verificación de identificaciones, historial de empleados, proceso de pago.

Servicios gubernamentales

Gobierno
Sistema de votación ~~transparente~~, minimización del fraude, derechos ciudadanos.

Viajes
Información de viajes, información de abordaje, identificación de pasajeros.

Contribuciones
Mantener la integridad de la donación, garantizar canales de recaudación seguros.

Organizacion voluntaria
Seguimiento de todas las donaciones y garantizar la integridad, reduce la complejidad de los procesos.

Salud
Gestión de la base de datos de pacientes, gestión de la cadena de suministro de medicamentos, transacciones de honorarios médicos, privacidad.

Educación
Canal didáctico adecuado, digitalización, información académica.

GRACIAS

TEXTO

Bibliografía

[1] Satoshi Nakamoto,(2008 Oct.). Accessed 2017, Bitcoin: A Peer-to-Peer Electronic Cash System. [Online], Available: https://bitcoin.org/bitcoin.pdf

[2] Adam Back,(2002 Ago) Accessed 2017, Hashcash - A Denial of Service Counter-Measure. [Online], http://www.hashcash.org/papers/hashcash.pdf

[3] Wei Dai,(1998) Accessed 2017, B-money. [Online], http://www.weidai.com/bmoney.txt

[4] Hal Finney,(2004) Accessed 2017, RPOW - Reusable Proofs of Work. [Online], http://nakamotoinstitute.org/finney/rpow/index.html

[5] Nick Szabo,(2005) Accessed 2017,Bit gold. [Online], https://unenumerated.blogspot.lu/2005/12/bit-gold.html [6] -,(2010) Accessed 2017, Bitcoin Wiki, [Online],https://en.bitcoin.it/wiki

[7] Joseph Bonneau ,(2015) Accessed 2017, How long does it take for a Bitcoin transaction to be confirmed?. [Online], https://coincenter.org/entry/how-long-does-it-take-for-a-bitcoin-transaction-to-be-confirmed

[8] -,(2017 Dic), Legality of bitcoin per country or territory. [Online], https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory

[9] Identity2020 Systems,Accessed 2017, Why digital identity?. [Online], http://id2020.org/digital-identity-1 [10] -,Accessed 2017, Cryptocurrency Market Capitalizations,[Online],https://coinmarketcap.com/coins/

[11] Vitalik Buterin,Last Modified 2017 Sep. Accessed 2017, Ethereum white paper. [Online], https://github.com/ethereum/wiki/wiki/White-Paper