

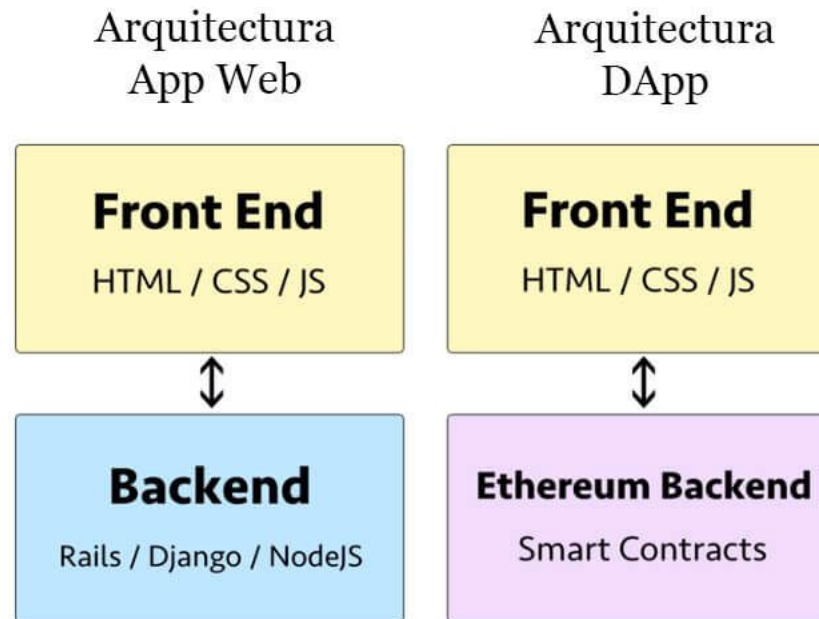
Curso desarrollo Blockchain Ethereum con Solidity

Clase 2

¿Qué es una dApp?

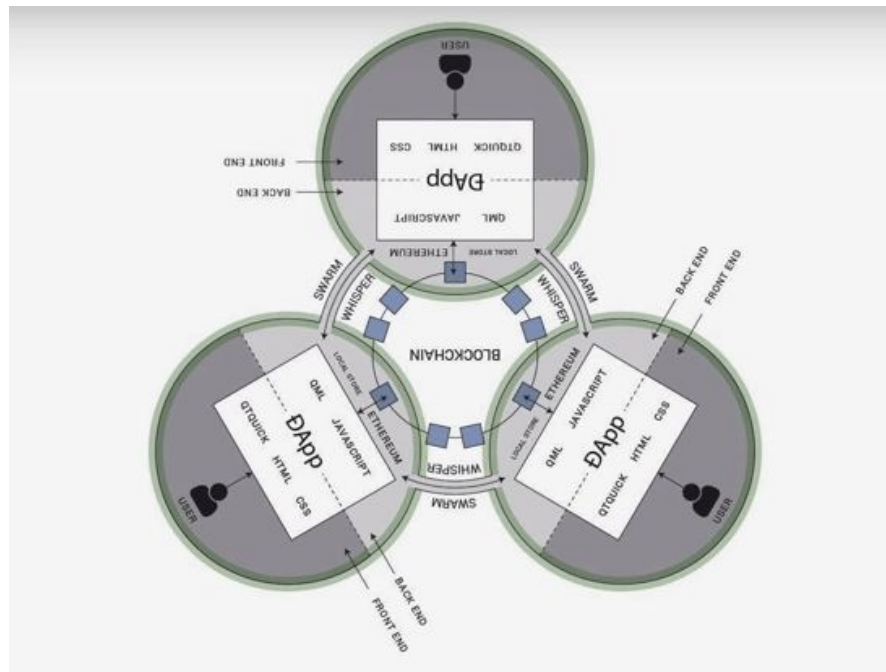
¿Qué es una dApp?

- Una dApp es una aplicación distribuída sobre la Ethereum Blockchain
- Tiene multiples capas y componentes
- No depende de un sistema centralizado sino que depende de la comunidad de usuarios que la utiliza
- Puede ser mobile*
- Puede ser una web*



¿Qué es una dApp?

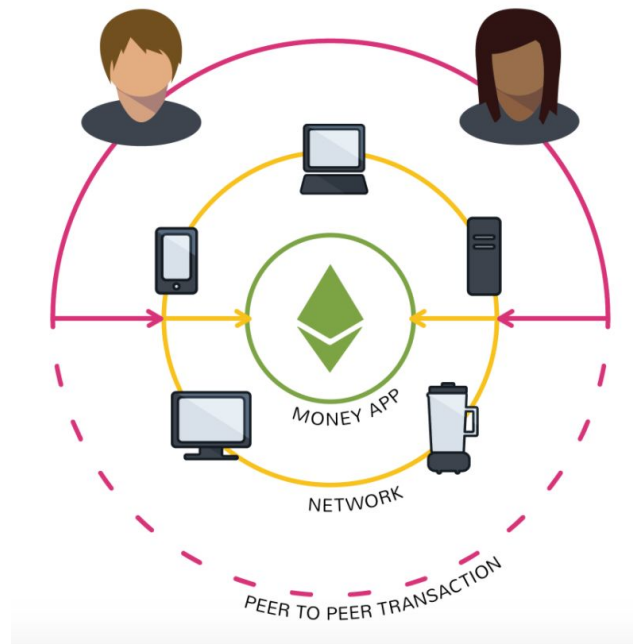
- No es necesario registrarse (como Facebook, Twitter, Google, etc.)
- Remarcadamente superiores para integración de pagos*
- Garantía de datos inmutable, inalterable y completamente accesible**
- Mayor tranquilidad para los usuarios dado que pueden ver el código de la aplicación, verificando así que no existe un proceso oculto embebido



Principios fundamentales para una dApp

Principios fundamentales para una dApp

- Debe ser descentralizada
- Utiliza estándares preestablecidos y mecanismos públicos de consenso
- Se comunica con la blockchain a través de protocolos y estándares pre-establecidos
- Pueden ser clasificadas por su función financiera y/o por su función en base a la Blockchain



Principios fundamentales para una dApp

En base a la función financiera pueden ser categorizadas como

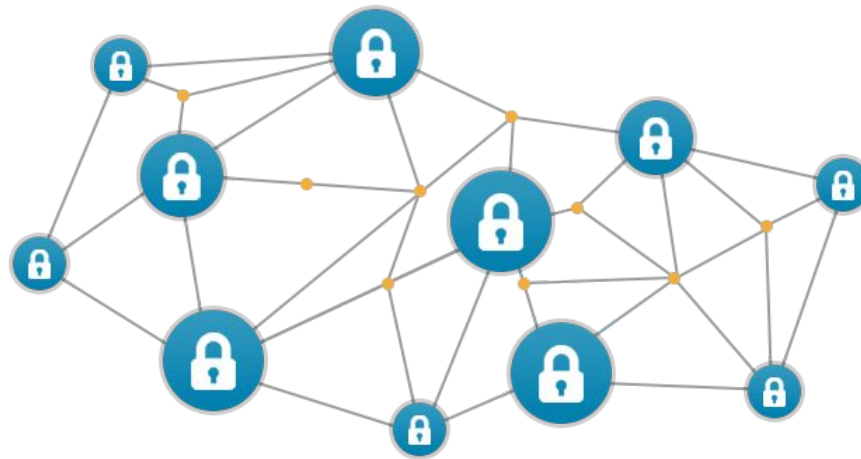
- Puramente financieras: Se ocupan de cuestiones puramente monetarias (ej. Ayudan a los usuarios a administrar su dinero)
- Semi-financieras: Si bien tienen un elemento financiero, se ocupan de cosas como intercambio de dinero por artículos o servicios.
- No financieras: No involucran dinero, claros ejemplos de estas dApps son sistemas de votación, gubernamentales, etc.



Principios fundamentales para una dApp

En base a la función sobre Blockchain pueden ser categorizadas como

- Con blockchain propia: Mantienen su propia cadena, un claro ejemplo es Bitcoin
- Con uso de Blockchain existente: Utilizan una blockchain existente y requieren del uso de tokens*
- Especializadas: Utilizan un mecanismo muy similar a las anteriores pero son específicas para un ítem de acción



CryptoKitties: Una dApp como caso de éxito

CryptoKitties: Una dApp como caso de éxito

Los CriptoKitties han sido un caso de éxito rotundo de este sistema de aplicativos.

- A bajo nivel, se trata de una serie de algoritmos, hashes, lógica y varios miles de líneas de código.
- A nivel visual, son bellos gatitos coleccionables
- Han llegado a valer +U\$100.000

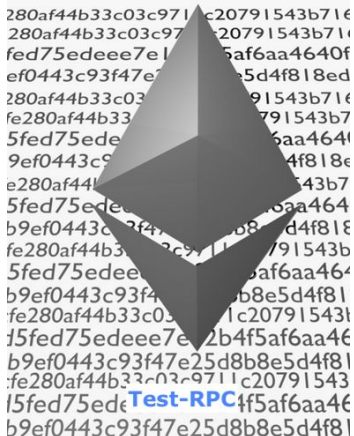


Herramientas

Herramientas

Para desarrollar Dapps existen multiples herramientas como

- Geth
- JSON RPC
- Test RPC
- Truffle
- Remix



GETH

GETH

- Es el nodo que nos provee la fundación Ethereum
- Posee una interfaz completa
- Está desarrollada en GO
- Será la base del navegador MIST*
- Es el principal producto de la etapa Frontier**
- Los binarios estables actualizados pueden ser descargados desde <https://geth.ethereum.org/downloads/>



JSON RPC

JSON RPC

- Permite la comunicación con el nodo que queremos conectar
- Se puede utilizar sobre un nodo local indicando -rpc (usualmente lo abre en el puerto 8045)
- Es una capa de comunicación
- Es agnóstico en cuanto al transporte, ya que los conceptos se pueden usar dentro del mismo proceso, a través de sockets, a través de HTTP o en muchos entornos de envío de mensajes
- Utiliza JSON (RFC 4627) como formato de datos
- Para C++ el default endpoint es: <http://localhost:8080>
- Para Go el endpoint por default es: <http://localhost:8545>



Test RPC

Test RPC

- Es el nodo simulado
- No está realmente conectado a la Blockchain
- Requiere NodeJS
- Es un emulador de blockchain rápido y personalizable
- Permite realizar llamadas a la Blockchain sin los gastos generales de ejecutar un nodo Ethereum real
- Las cuentas pueden ser reutilizadas y/o reestablecidas con una cantidad deseada de Ether SIN necesidad de minar
- El precio del GAS puede ser modificado a gusto
- La velocidad de minado puede ser alterada a conveniencia



```
280af44b33c03c9711c20791543b716
280af44b33c03c9711c20791543b716
fed75edeee7e11c20791543b716
ef0443c93f47e25d8b8e5d4f818ed
280af44b33c03c9711c20791543b716
fe280af44b33c03c9711c20791543b7
5fed75edeee7e11c20791543b7
9ef0443c93f47e25d8b8e5d4f818e
e280af44b33c03c9711c20791543b7
5fed75edeee7e11c20791543b7
b9ef0443c93f47e25d8b8e5d4f818e
fe280af44b33c03c9711c20791543b
5fed75edeee7e11c20791543b
b9ef0443c93f47e25d8b8e5d4f818e
fe280af44b33c03c9711c20791543b
15fed75edeee7e11c20791543b
b9ef0443c93f47e25d8b8e5d4f818e
fe280af44b33c03c9711c20791543b
15fed75edeee7e11c20791543b
b9ef0443c93f47e25d8b8e5d4f818e
```

Truffle

Truffle

Truffle es un entorno de desarrollo, un marco de prueba y un gestor de flujos para Ethereum, que facilita el desarrollo en Ethereum

- Compilación de contrato inteligente incorporada, vinculación, despliegue y gestión del binario
- Automatización del testing de contratos con Mocha y Chai
- Procesos de build configurable con soporte para builds custom
- Implementación de scripts de deploy y migración
- Consola interactiva para comunicación directa con el contrato
- Rebuild instantaneo durante el desarrollo
- Ejecutor de scripts externo que permite ejecución interna en un ambiente controlado por Truffle



Remix

Remix

- Es un compilador que ofrece la Ethereum Foundation
- Tiene una interfaz Web
- Permite configurar la versión de Solidity a utilizar
- Soporta multiples Enviroments
- Permite compilar contratos
- Es posible hacer debugg de lo que está pasando en nuestro contrato
- Brinda multiples cuentas con suficientes Ether para hacer múltiples pruebas



remix

Blockchain explorer

Blockchain explorer

Todas las operaciones, transacciones y balances de la Ethereum Blockchain pueden ser vistos en <https://etherscan.io/>

Block #6680559

Home / Blocks / Block Information

Overview

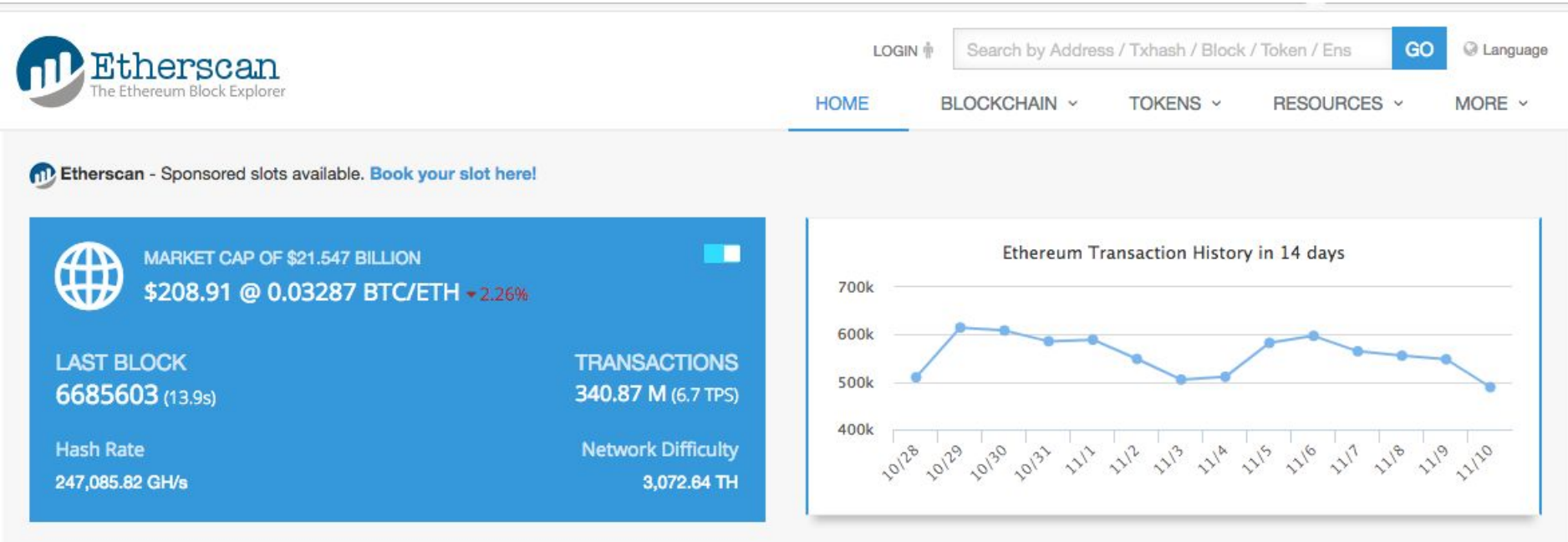
Comments

Block Information

Height:	6680559
TimeStamp:	25 secs ago (Nov-10-2018 08:40:29 PM +UTC)
Transactions:	18 transactions and 14 contract Internal Transactions in this Block
Hash:	0xe25ac72626b1ea0d789ff6390820ded84874af978ce146dd3fda9844b2d2a0f6
Parent Hash:	0xfb02b2456b8fdd93d95635a9c5aea40fd5de00c3f9fdbf52d479270229c131f
Sha3Uncles:	0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347
Mined By:	0x52bc44d5378309ee2abf1539bf71de1b7d7be3b5 (Nanopool) in 5 secs
Difficulty:	3,070,783,879,468,183
Total Difficulty:	7,734,797,263,037,641,036,864
Size:	3777 bytes
Gas Used:	2,183,377 (27.29%)
Gas Limit:	8,000,029
Nonce:	0x2fba6ad4004a29d6
Block Reward:	3.01831775760661058 Ether (3 + 0.01831775760661058)
Uncles Reward:	0
Extra Data:	nanopool.org (Hex:0x6e616e6f706f66c2e6f7267)

Blockchain explorer

- Permite hacer seguimiento de una transacción*
- Posee un directorio de cuentas de Ethereum
- Cuenta con un visualizador de tokens ERC20 y ERC721**
- Provee una API para poder conectarla desde una web/mobile y obtener información específica
- Presenta gráficos de las operaciones realizadas, valor del Ether, etc.
- Soporta el escaneo de operaciones en las testnets de Ropsten, Kovan, Rinkeby y Toba

















Fundamentos de deploy

Fundamentos de deploy

- Tener instalado NodeJS, GET, SOLC
- Compilar el SmartContract (abi & bin)
- Iniciar el nodo de Geth (con rinkeby por ejemplo)
- También es posible hacer deploy desde Remix

creation of EjemploEducacionIT pending...

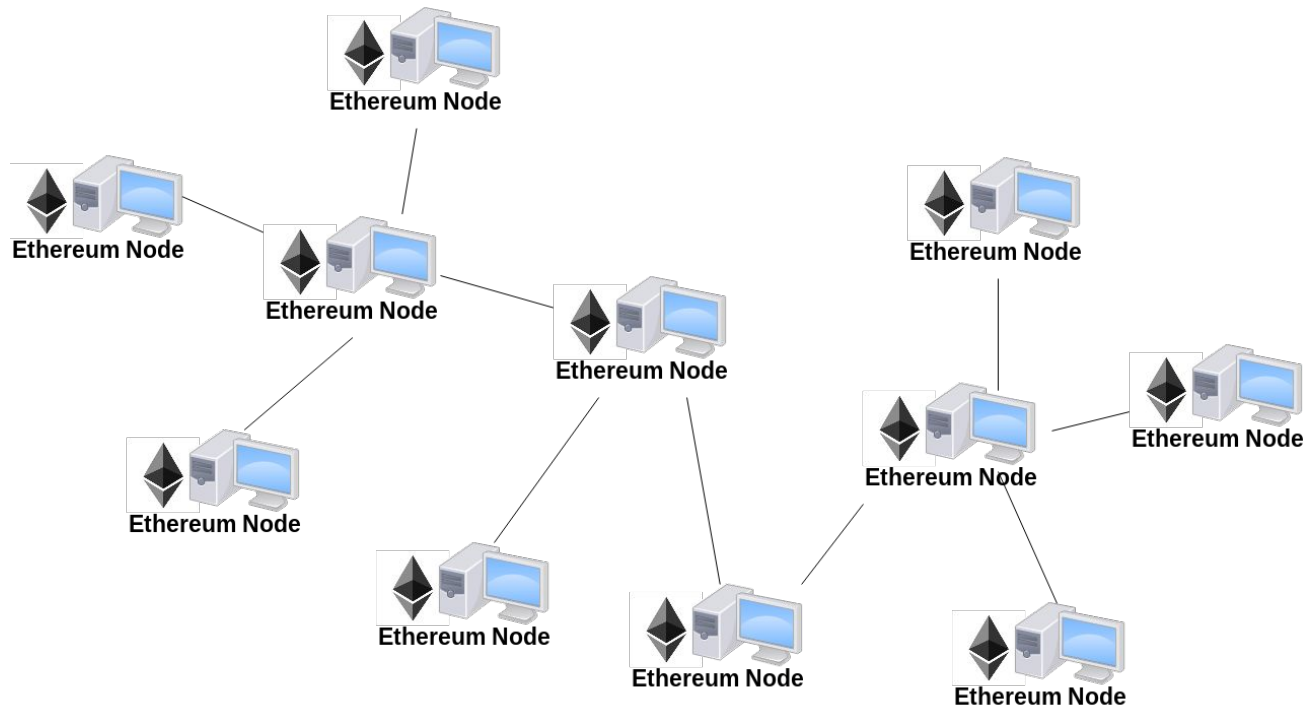
✓ [vm] from:0xca3...a733c to:EjemploEducacionIT.(constructor) value:0 wei data:0x608...00000 logs:0 hash:0xb38...389b9

status	0x1 Transaction mined and execution succeed
transaction hash	0xb385c36f358d5c60b2ef478bad302b9a9cad227bf8f18a1205f6f0cf37f389b9 
contract address	0x692a70d2e424a56d2c6c27aa97d1a86395877b3a 
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c 
to	EjemploEducacionIT.(constructor) 
gas	3000000 gas 
transaction cost	214526 gas 
execution cost	116746 gas 
hash	0xb385c36f358d5c60b2ef478bad302b9a9cad227bf8f18a1205f6f0cf37f389b9 
input	0x608...00000 
decoded input	{ "string initialMessage": "Curso de Blockchain" } 
decoded output	- 
logs	[]  
value	0 wei 

Testnets

Testnets

- Son redes utilizadas para simular el comportamiento completo de la Ethereum Blockchain*
- Pueden correr en un equipo local
- Ether preminados
- Ether ilimitados**
- Cada nodo contiene una copia completa de la blockchain de Ethereum
- Ethereum cuenta con 3 redes para el desarrollador (para poder probar todo lo necesario)



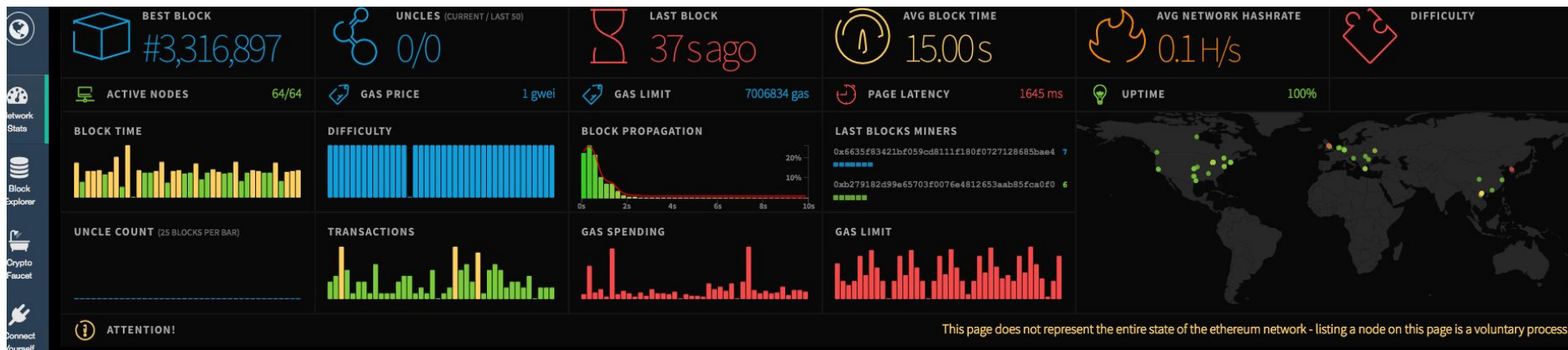
Testnets



KOVAN Testnet

- Vigente desde Marzo de 2017
- PoA testnet
- Identificador de la red: 42
- Block time: 4 segundos
- Explorer <https://kovan.etherscan.io/>
- Github <https://github.com/kovan-testnet/proposal>

Testnets



Rinkeby Testnet

- Vigencia desde Abril de 2017
- PoA testnet
- Identificador de la red: 4
- Block time: 15 seconds
- Explorer <https://rinkeby.etherscan.io/>
- Github <https://github.com/ethereum/EIPs/issues/225>
- Sitio Web: <https://www.rinkeby.io>

Testnets



Ropsten Testnet

- Vigente desde Noviembre de 2016
- PoW testnet
- Identificador de la red: 3
- Block time*: < 30 segundos
- Explorer <https://ropsten.etherscan.io/>
- Github <https://github.com/ethereum/ropsten>

Introducción a Solidity

Introducción a Solidity

- Es mundialmente conocido como el lenguaje de programación con el que se programan los contratos inteligentes de Ethereum
- Es un lenguaje de scripting tipado estáticamente que hace el proceso de verificar y hacer cumplir las restricciones en tiempo de compilación en lugar de en tiempo de ejecución
- Solidity es un lenguaje Turing Complete
- Es un lenguaje orientado a objetos
- Está diseñado para correr específicamente sobre la Ethereum Blockchain*
- Cuenta con un IDE oficial llamado Remix



SOLIDITY

Introducción a Solidity

A screenshot of a code editor window titled 'browser/educacionItContract.sol'. The editor shows Solidity code for a contract named 'EjemploEducacionIT'. The code includes a pragma statement for Solidity version 0.4.17, an import statement for 'jds.sol', a comment '//EducacionIT 2018 -', a constructor that takes a 'name' string and sets 'owner' to it, and a 'getHelloWorldMessage()' function that returns the string 'Hello World!'. The left sidebar shows a file explorer with 'browser' containing 'jds.sol' and 'educacionItContract.sol', and 'config'.

Este es un ejemplo de un contrato sumamente sencillo hecho en solidity versión 0.4.17

Introducción a Solidity

Del contrato anterior, cada línea tiene su explicación

- **Pragma** solidity permite indicar la versión de Solidity a utilizar
- **Contract** es una palabra reservada que indica el inicio de la definición de un contrato
- **Public** es un modificador de acceso que le da visibilidad fuera del contrato
- **Function** es una palabra reservada para indicar el inicio de definición de una función
- **Returns** indica que la función retornará algún valor
- La asignación en Solidity es de derecha a izquierda

